ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BAJO LA NORMA ISO/IEC 27001:2013, EN UNA INSTITUCIÓN FINANCIERA ECUATORIANA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

ROSALES BRAVO PAUL FERNANDO

paul_rosales_1@hotmail.com

SUÁREZ LEÓN MERY PAULINA

paupausl@yahoo.es

DIRECTOR: MSc. ING. JUAN HERRERA

juan.herrera@leveltech.com.ec

QUITO, MAYO DEL 2015

DECLARACIÓN

Nosotros, Paul Fernando Rosales Bravo y Mery Paulina Suárez León, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes 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.

_____	_____
Paul Fernando	**Mery Paulina**
Rosales Bravo	**Suárez León**

CERTIFICACION

Certifico que el presente trabajo fue desarrollado por Paul Fernando Rosales Bravo y Mery Paulina Suárez León, bajo mi supervisión.

_____

MSc. Juan Herrera
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Al culminar tal vez uno de los retos más complicados que he tenido en mi vida, es justo dar las gracias a un sin número de personas que de una u otra forma han contribuido para que hoy culminar mi carrera sea una realidad.

A Dios por darme todo lo que tengo. A mis queridos padres por darme la vida, la educación y los valores que han regido mi vida, a mis hermanos por su cariño.

A mis familiares por todo su apoyo. A los profesores del colegio y universidad que supieron compartir su conocimiento y su experiencia. A mi compañera y amiga Paulina por su amistad y por ayudarme a culminar este reto.

A usted, Ing. Juan Herrera por el apoyo, la dirección, la guía y los consejos que nos brindó y que poco a poco hicieron que vayamos avanzando para cumplir el objetivo final.

A mi querida esposa Janeth por ser una mujer en todo el sentido de la palabra, por su cariño, paciencia y apoyo en todo este tiempo y finalmente a la luz de mi vida, mi hija Micaela fuente de inspiración y amor que alegra día a día mi vida.

Gracias

Paul

AGRADECIMIENTOS

Agradezco al Señor por permitirme estar aquí y darme la oportunidad de cumplir un objetivo más.

A mis padres, por su ejemplo, al demostrarme cada día que no hay otro camino para la felicidad que el trabajo honesto. Por su tesón y apoyo incondicional en los tiempos difíciles.

A mis amigos y hermanos, porque tengo la certeza que siempre han estado ahí, por su cariño incondicional.

A Paúl y su familia, mi compañero de tesis y amigo, por el apoyo brindado en todo momento, contra todo pronóstico lo logramos…

Al Ing. MSc. Juan Herrera, quién desde un inicio nos apoyó incondicionalmente y nos dio la libertad para desarrollar nuestro tema de tesis, contando siempre con sus acertadas sugerencias y lineamientos.

A todo el cuerpo docente de la Escuela Politécnica Nacional quienes nos han guiado con el ejemplo en nuestro camino hacia la excelencia profesional.

Paulina

DEDICATORIA

Este trabajo está dedicado a las personas que de una u otra manera me apoyaron para que culmine mi tesis.

A dios, a mi madre, mi padre, mis hermanos, mis familiares, a mi esposa y mi hija.

Gracias a ustedes siempre.

Paul

DEDICATORIA

A mi madre, porque ha trabajado con ahínco para apoyarme en mis estudios. Que este logro sea el testimonio de tu esfuerzo, gracias mamá.

A mis hijos, Mateo y Romina, mi razón de ser, quiénes son luz en todo momento y logran que siempre me sienta bendecida y agradecida con Dios.

Paulina

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

El presente proyecto de titulación diseña un Plan para implementar un Sistema de Gestión de Seguridad en una institución financiera ecuatoriana basado en el estándar ISO 27001:2013 y la regulación vigente para este tipo de empresa.

El Plan establece el alcance del Sistema que se desea implementar, esto se realiza en términos de la naturaleza del negocio, locación, activos de información, aspectos legales y tecnología de la institución evaluada.

Determinado el alcance, seleccionaremos el tipo de controles requeridos y se establecerá la política de seguridad que servirá de marco referencial para el cumplimiento de los objetivos institucionales y regulatorios, basados en una estrategia de evaluación, control y mitigación del riesgo.

DESCRIPCION DEL DOCUMENTO

El presente proyecto de titulación se encuentra estructurado de la siguiente manera:

El capítulo 1: “Diagnóstico de la Seguridad de la Información” permite conocer la organización que será evaluada, cuales son los objetivos institucionales, establece un mapa conceptual de su infraestructura tecnológica y sus necesidades en relación a la seguridad de la información, mediante un análisis inicial con la herramienta MSAT, con el objetivo de establecer los alcances y límites del Sistema de Gestión de Seguridad que se desea implementar.

En el capítulo 2: “Planificación del Sistema de Seguridad de la Información” se establece la metodología para la evaluación de riesgos apropiada para el SGSI y la razón de ser del negocio, en este proyecto nos hemos basado en la metodología establecida en la NIST 800-30, se realiza el análisis y evaluación de riesgo, acorde a las amenazas y vulnerabilidades identificadas para la institución financiera, los riesgos levantados servirán de insumo para determinar los requerimientos de seguridad de la organización y escoger los controles de seguridad requeridos acorde al estándar ISO 27001:2013.

Para el capítulo 3: “Determinación de las estrategias de Implementación del Plan de Seguridad” se evalúan y determinan los requerimientos legales y

organizacionales que se encuentra supeditada la institución financiera y nos permita alinear los alcances y límites del Sistema de Gestión de Seguridad a nivel de negocio, con lo cual se constituye la Política de Seguridad que regirá a la institución, en nuestro caso se evalúa la política que actualmente ya mantiene la organización con el objeto de establecer sugerencias para su actualización. Cerrando el capítulo se emite el enunciado de aplicabilidad en el cual se instituye los objetivos de control y controles seleccionados y los motivos para su elección; así como la verificación de cuales ya se encuentran implantados y por último definir la exclusión de controles en caso aplicase.
En el capítulo 4 se emiten las conclusiones y recomendaciones del proyecto acorde al proceso y metodología utilizada en este proyecto.

DESCRIPCION DEL PROBLEMA

El cumplir con normas de Seguridad de la Información ha tomado mucha fuerza en estos últimos años debido a su carácter obligatorio para las entidades bancarias de acuerdo a las resoluciones emitidas por la Superintendencia de Bancos y Compañías (SBS), entre las principales tenemos JB-2005-834, JB-2012-2148 y JB-2014-3066, al momento todas estas se encuentran consolidadas en la Norma de Riesgo Operativo, la cual regula a este tipo instituciones, así como la necesidad de garantizar al cliente seguridad en su información y evitar eventos que pongan en riesgo su patrimonio.

La empresa a ser evaluada debe garantizar la confidencialidad, integridad y disponibilidad de sus activos y la de sus clientes; acorde a la normativa vigente la misma que está alineada a estándares de Seguridad como la 27001, al ser una institución nueva, requiere establecer lineamientos internos para cumplir ese objetivo junto a un plan estratégico del área de Seguridad y alineado a los objetivos institucionales.

Bajo lo expuesto, es necesaria la implementación de un Sistema de Gestión de Seguridad que asegure la información de la institución financiera y de sus clientes, y este en cumplimiento a la regulación vigente. Adicionalmente con

el objeto de conocer los nuevos controles establecidos en temas del estándar 27001, este proyecto utilizará la nueva versión 27001:2013.

OBJETIVOS

Objetivo General

- Planificar un Sistema de Gestión de Seguridad de la Información en una institución financiera ecuatoriana bajo las normativas de la ISO/IEC 27001:2013.

Objetivos Específicos

- Diagnóstico de la situación actual de la Seguridad de la Información en una institución financiera ecuatoriana.
- Planificación del Sistema de Gestión de Seguridad de la Información.
- Determinación de las estrategias de implementación del Plan para el Sistema de Gestión de Seguridad de la Información.
- Establecer recomendaciones y conclusiones.

ALCANCE

El proyecto de titulación tiene como objetivo inicial realizar un análisis de deficiencias sobre el nivel de seguridad actual de una institución financiera ecuatoriana basada en la evaluación de la documentación proporcionada por la empresa, para posteriormente determinar los riesgos de los sistemas de información y el estado de seguridad frente al estándar ISO 27001:2013, con base en estos resultados identificar los controles de seguridad más apropiados para la institución acorde a las necesidades de negocio, finalmente se establecen las conclusiones y recomendaciones para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), mediante la generación del plan de acción respectivo.
La implementación no será parte del proyecto de titulación.

CAPITULO 1: DIAGNOSTICO DE LA SEGURIDAD DE LA INFORMACION

1.1 RECONOCIMIENTO DE LA EMPRESA

Establecida como una institución pública con autonomía administrativa, técnica y financiera, con finalidad social y de servicio público y domicilio principal en la ciudad de Quito, Distrito Metropolitano, tiene como principal servicio la entrega de préstamos hipotecarios, los mismos que inician bajo un proceso inicial de precalificación mediante el acceso a internet.
La empresa está formada por 600 empleados aproximadamente y tiene presencia a nivel nacional. Mantiene como clientes al total de afiliados y jubilados[1], lo que da un total aproximado de 3 millones de clientes.

1.1.1 GENERALIDADES DE LA EMPRESA.

1.1.1.1 Historia de la Empresa

La Constitución de la República del Ecuador en su artículo 372, establece la instauración de una entidad financiera responsable de canalizar sus inversiones y administrar los fondos previsionales públicos, inversiones privativas y no privativas; y, que su gestión se sujetará a los principios de seguridad, solvencia, eficiencia, rentabilidad y al control del órgano competente.

Acorde a este mandato constitucional, fue aprobada la creación de la institución financiera mediante ley publicada en el Registro Oficial No. 587 del lunes 11 de mayo de 2009.

La institución financiera abrió las puertas el 18 de Octubre del año 2010.

[1] Por motivos de confidencialidad de la información se reserva el nombre de la empresa.

Actualmente se encuentra en un proceso de migración de sus procesos operativos y tecnológicos para su principal producto que es los préstamos hipotecarios, los mismos que estaban a cargo de una empresa privada. Desde Febrero del 2014 la institución toma el proceso de préstamos hipotecarios bajo su administración como fase inicial para productos específicos.

1.1.1.2 Servicios de la Institución Financiera

En la institución financiera pueden identificarse dos servicios preponderantes:

Servicio de Préstamos

Acorde a la ley, sus funciones más preponderantes es brindar los distintos servicios financieros como créditos hipotecarios, prendarios y quirografarios, así como también, operaciones de redescuento de cartera hipotecaria de instituciones financieras y otros servicios financieros a favor de clientes mediante operaciones directas o a través del sistema financiero nacional.

Servicio de Inversiones

Otra función de la institución financiera son las inversiones, que se encaminan a través de los instrumentos que ofrece el mercado de valores para el financiamiento a largo plazo de proyectos públicos y privados, productivos y de infraestructura que generen rentabilidad financiera, valor agregado y nuevas fuentes de empleo, así como también inversiones en títulos de renta fija o variable a través de del mercado primario y secundario.

1.1.1.2.1 Servicios de Préstamos

Préstamos Hipotecarios: La institución financiera ofrece préstamos hipotecarios para la adquisición de bienes inmuebles, como unidades de vivienda, construcción, remodelación, ampliación y/o mejoramiento de las mismas, terrenos, oficinas, locales comerciales o consultorios; así como

también sustitución de créditos hipotecarios para viviendas otorgadas por otras instituciones financieras del país.

Préstamos Quirografarios: La institución financiera ofrece créditos quirografarios, dependiendo de su capacidad de pago, se puede solicitar un monto de hasta 80 salarios básicos unificados del trabajador en general (USD 27.200).

Préstamos Prendarios: La institución financiera concede créditos inmediatos con dinero en efectivo, recibiendo como garantía joyas de oro.

1.1.1.2.2 Servicios de Inversiones

Se brinda asesoría e información a empresas privadas, en materia de finanzas, valores, estructuración de portafolios de valores, negociación de paquetes accionarios, adquisiciones, fusiones, escisiones y otras operaciones del mercado de valores para sí o para emisores relacionados con su actividad.

Estos servicios especializados que involucran movilización de recursos de capital y deuda, tienen como objetivo el apoyo y desarrollo del sector empresarial y la consecución de nuevos proyectos de inversión que generen empleo y valor agregado.

Inversiones en el mercado de valores: Las inversiones a través del Mercado de Valores consisten en la adquisición de recursos en títulos valores de renta fija y renta variable de empresas del sector público y privado, que ofrezcan expectativas de seguridad, liquidez y rendimiento.

Dichas inversiones proveen la inversión en bonos del estado, obligaciones de corto, mediano y largo plazo de empresas, valores representativos de titularización de activos; valores de participación, reportes bursátiles y acciones; como una alternativa que ofrece la institución financiera para el financiamiento de corto, mediano y largo plazo; con el fin de impulsar el

desarrollo del país a través de instrumentos que generen rentabilidad.

Las inversiones bursátiles podrán efectuarse en títulos valores en el mercado primario y secundario, los cuales podrán negociarse a través de las Bolsas de Valores.

1.1.2 MISION, VISION Y OBJETIVOS DE LA EMPRESA

1.1.2.1 Misión

"Administrar, de manera eficiente, los recursos provisionales de los asegurados generando operaciones financieras con retorno social y económico adecuado, que contribuyan a impulsar la producción, creen valor agregado y garanticen nuevas fuentes de empleo."[2]

1.1.2.2 Visión

"Ser la institución Financiera Pública reconocida por la excelencia en la generación de rendimientos y servicios financieros para beneficio de los clientes, la integridad de su gente y su contribución al desarrollo nacional."[1]

1.1.2.3 Valores, políticas y objetivos

Valores

"Compromiso institucional.
Vocación de servicio a los asegurados.
Integridad.
Liderazgo de los mandos medios.
Orientación a resultados.
Mejoramiento continuo." [3]

[2] Documento interno de la institución Financiera.
[3] Documento interno de la institución Financiera

Políticas Generales

“Garantizar el uso eficiente de los fondos previsionales bajo principios de seguridad, solvencia, eficiencia, rentabilidad y responsabilidad en función de los estándares del mercado.
Asegurar la diversificación de las operaciones financieras; y, canalizar los fondos previsionales hacia la inversión productiva.

Propender a la universalización de las operaciones financieras expandiendo su cobertura a nivel nacional, procurando compatibilidad entre los fondos previsionales y el volumen de crédito e inversión otorgados.
Promover condiciones competitivas dentro del mercado financiero nacional.
Garantizar transparencia y eficiencia en la gestión de la institución financiera, incorporando mecanismos de evaluación y rendición de cuentas, respetando la aplicación de normas, manuales y resoluciones.
Fomentar la observancia plena del Código de ética en los diferentes procesos y en la gestión del negocio de la institución financiera.
Instrumentar mecanismos que permitan mitigar el riesgo en las operaciones de crédito e inversión.
Incorporar como parte de la cultura de la institución financiera la administración integral de riesgos y la política de mejoramiento continuo para la calidad.” [3]

Objetivos

“Establecer mecanismos de financiamiento que posibiliten satisfacer las necesidades de crédito de los asegurados e impulsen el desarrollo del Sector Productivo.
Orientar los fondos previsionales hacia inversiones rentables de corto, mediano y largo plazo que propicien el desarrollo de la economía.
Fortalecer la autonomía técnica, administrativa y financiera de la institución financiera dentro del marco regulatorio a fin de proteger e incrementar los fondos previsionales, fomentando una cultura orientada al servicio a los asegurados y al mejoramiento continuo.

Desarrollar, mejorar e implementar nuevos productos y servicios financieros para los asegurados bajo condiciones de seguridad, confianza y rentabilidad.
Implementar una estructura organizacional flexible con adecuados estándares de calidad, en función de las necesidades de los procesos de negocio, de apoyo, de control y agregado de valor.

Implementar los procesos operacionales de la institución financiera en base a sistemas tecnológicos, de información y comunicación de punta acorde a la realidad de la institución financiera.
Alcanzar la mejor rentabilidad posible del portafolio de inversiones acorde a la curva de rendimiento por calificación de riesgo y plazo." [4]

1.1.3 ESTRUCTURA ORGANIZACIONAL DE LA EMPRESA

Al ser un organismo estatal se encuentra bajo la autoridad de un Directorio el cual está integrado por:

- El presidente del Consejo Directivo
- Un Delegado del Ejecutivo
- Un representante de los afiliados
- Un representante de los jubilados

Dentro de su proceso funcional la institución financiera se encuentra establecido en el siguiente orden de gobernabilidad:

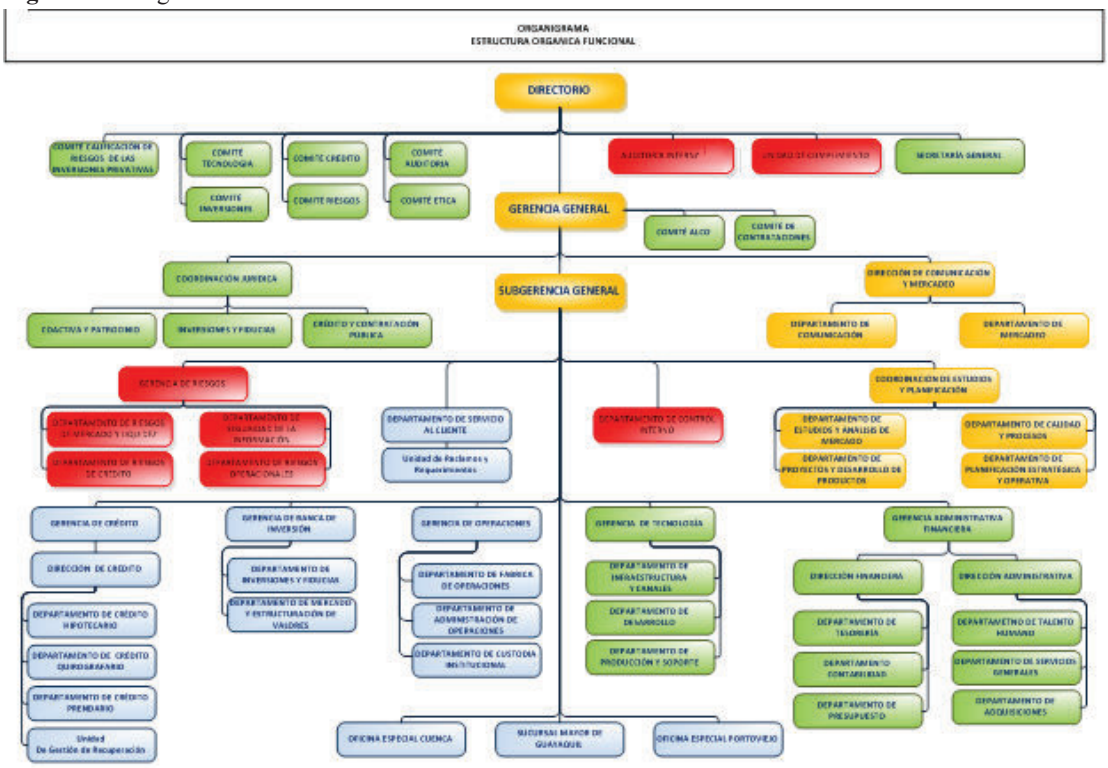
- Gerente General
- Subgerente General
- Gerencias de negocio
- Jefes Departamentales
- Analistas Séniores – Junior
- Técnicos
- Asistentes Administrativos
- Otros

[4] Documento de la institución financiera

1.1.3.1 Organigrama

La estructura de la institución financiera se puede apreciar en la Figura 1-1

Figura 1-1: Orgánico Funcional Institución Financiera



Fuente: Los autores.

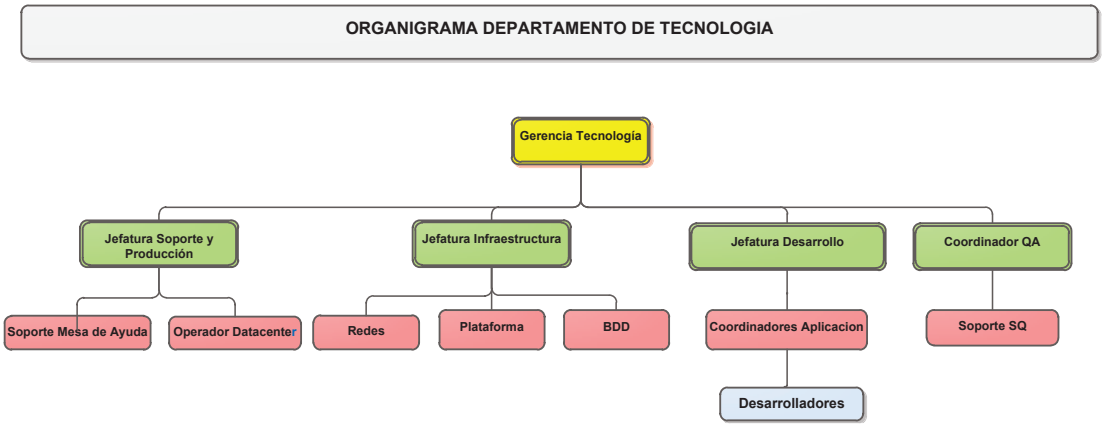
1.2 ANÁLISIS DE LA SITUACIÓN INFORMÁTICA

El análisis de la situación consiste en realizar en primer lugar un inventario del sistema de información, en particular de la siguiente información:

- Personas y funciones
- Materiales, servidores y los servicios que éstos brindan
- Esquematización de la red (esquema de direcciones, topologías físicas y lógicas, etc.)
- Lista de los nombres de dominio de la empresa.
- Infraestructura de la comunicación (enrutadores, conmutadores, etc.)
- Información

En la Figura 1-2 podemos apreciar la estructura funcional del departamento de tecnología de la Institución Financiera.

Figura 1-2: Orgánico Funcional Departamento Tecnología



Fuente: Los autores.

1.2.1 APLICACIONES

Las aplicaciones son programas desarrollados para solucionar y automatizar procesos específicos, a continuación se detalla aquellos aplicativos que dan viabilidad a los servicios y productos que brinda a la institución financiera, estos se encuentran en servicios de Hosting[5] y Housing[6] principalmente.

Aplicativos para el Servicio de Préstamos Quirografarios e Hipotecarios

1.2.1.1 Sistema de Préstamos Quirografarios.

Descripción:

Aplicativo encargado de manejar el servicio de préstamos quirografarios el mismo que permite la administración, seguimiento y operación de las transacciones, así como un seguimiento de la transacción desde sus inicios, en la tabla 1-1 se aprecia la descripción del sistema.

Modo de acceso: Web

[5] Espacio físico dentro de un centro de datos que se alquila o vende generalmente a empresas grandes para que estas coloquen ahí sus propios servidores aprovechando así la infraestructura.
[6] Alquiler o venta de un espacio de almacenamiento dentro de un servidor de una empresa generalmente para una empresa de internet

Tabla 1-1: Descripción del Sistema de Préstamos Quirografarios

Ubicación
Proveedor Hosting

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Préstamos Quirografarios	Software para concesión de préstamos Quirografarios	Red Hat 5.5	Oracle	Java

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli1IP	122 GB	27 GB	Activo

Usuarios
Funcionarios y Clientes

Fuente: Los autores

1.2.1.2 Sistema de Préstamos Hipotecarios

Descripción:

El Aplicativo permite la administración, seguimiento y operación de las transacciones hipotecarias, en la tabla 1-2 se verifica sus componentes.

Modo de acceso: Web

Tabla 1-2: Descripción del Sistema de Préstamos Hipotecarios

Ubicación
Proveedor Hosting

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Préstamos Hipotecarios	Software para concesión de préstamos hipotecarios	Red Hat 5.5	Oracle	Java

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli2IP	114 GB	20 GB	Activo

Usuarios
Funcionarios y Clientes

Fuente: Los autores

1.2.1.3 Sistema de Gestión de Procesos.

Descripción:

Es un Administrador de Procesos de Negocio que implementa un conjunto de servicios y herramientas que facilitan la administración de procesos de negocio (análisis, definición, ejecución, monitoreo y control de los procesos). Además contempla el soporte para interacción humana e integración de los flujos con aplicaciones o sistemas externos. Actualmente es utilizada para todo el flujo requerido para la aprobación de préstamos hipotecarios.

Funciona en ambiente Web, en la tabla 1-3 se muestra como está conformado en sus distintos componentes.

Modo de acceso:

Web

Tabla 1-3: Descripción del Sistema de gestión de procesos.

Ubicación
Proveedor Hosting

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema de Gestión de Proyectos	Sistema de Gestión de Proyectos	WINDOWS 2008 R2	SQL SERVER 2008 R2	ASP.net

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli3IP	100,99 GB	4096 MB	Activo

Usuarios
Funcionarios y usuarios externos

Fuente: Los autores

1.2.1.4 Sistema de Gestión de Administración Financiera

Descripción:

Es un sistema de información que permite a las instituciones financieras ofrecer a sus clientes el acceso a productos, como son en este caso manejo

de créditos hipotecarios ajustándose a las reglas del negocio de la institución así como a las exigencias y regulaciones de los organismos de control financiero, por lo cual se constituye en una herramienta para responder rápidamente a las necesidades de crédito y condiciones del mercado, y a la capacidad y planificación de pago de los clientes. En la tabla 1-4 podemos ver la descripción del sistema.

Modo de acceso:

Cliente /Servidor, modo consola AS400

Tabla 1-4: Descripción del Sistema Gestión de Administración Financiera.

Ubicación
Proveedor Hosting

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema de Gestión Administración Financiera	Sistema de Gestión Administración Financiera	IBMi	Librerías IBMi/DB2*	RPG

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli4IP	Microsoft Windows Server 2008	16 GB	Activo

Usuarios
Funcionarios de las áreas de Operaciones, Crédito y Tesorería principalmente

Fuente: Los autores

1.2.1.5 Sistema Manejador de Contenido Empresarial

Descripción:

Es un software orientado a resolver las necesidades de los clientes bajo el concepto de Enterprise Content Management (ECM) para que las empresas puedan administrar cualquier tipo de documento electrónico, para que este sea almacenado, administrado y consultado. En el caso de la institución financiera, permite visualizar y distribuir toda la documentación requerida y generada dentro del proceso de crédito hipotecario por sus distintos actores.

La descripción del sistema lo tenemos en la tabla 1-5.

Modo de acceso:

Cliente /Servidor y Web

Tabla 1-5: Descripción del Sistema Manejador de contenido empresarial

Ubicación
Proveedor Hosting

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema Manejador de contenido empresarial	Sistema Manejador de contenido empresarial	WINDOWS 2008 R2	SQL SERVER 2008 R2	C#

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli5IP	Microsoft Windows Server 2008 R2 (64-bit)	6 GB	Activo

Usuarios
Funcionarios y usuarios externos

Fuente: Los Autores

1.2.1.6 CRM

Descripción:

Se utiliza para consulta de créditos y administración de préstamos hipotecarios y quirografarios.

Actualmente el sistema toma la información de las bases de datos de los aplicativos de préstamos hipotecarios, préstamos quirografarios e historia laboral, ver descripción en la tabla 1-6.

Modo de acceso:

Cliente /Servidor, modo consola AS400.

Tabla 1-6: Descripción del Sistema para manejo gerencial de créditos

Ubicación
Proveedor Hosting

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Software para manejo gerencial de créditos	Software para manejo gerencial de créditos	Red Hat	Oracle	java

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli6IP	164 GB	3 GB	Activo

Usuarios
Funcionarios de áreas de Crédito y Operaciones

Fuente: Los autores

1.2.1.7 Sistema de Flujos de Trabajo

Descripción:

Se utiliza actualmente para el manejo del flujo operativo de préstamos hipotecarios. En la tabla 1-7 se aprecia los componentes del sistema.

Modo de acceso: Web

Tabla 1-7: Descripción del Sistema de Flujo de Trabajo

Ubicación
Entidad Financiera / Proveedor

Software				
Nombre	**Descripción**	**SO**	**Base de Datos**	**Lenguaje Programación**
Sistema de Flujo de trabajo	Sistema de Flujo de trabajo	Red Hat 5.5	MySQL 5.5	Visual Basic 3.0

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli7IP	100 GB	3GB	Activo

Usuarios
Funcionarios y proveedor

Fuente: Los autores.

1.2.1.8 Sistema de Inversiones

Descripción:

Sistema que se utiliza para el proceso administrativo y de consultas en materia de inversiones, en la tabla 1-8 esta descrito los componentes que forman parte del mismo.

Modo de acceso:

Cliente - Servidor

Tabla 1-8: Descripción del Sistema de inversiones

Ubicación
Proveedor

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Aplicación para inversiones	Aplicativo para inversiones	Windows Server 2008	ORACLE	C#

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli8IP	1 TB	16 GB	Activo

Usuarios
Funcionarios área Inversiones, Operaciones, Riesgos

Fuente: Los autores

1.2.1.9 Sistema de Préstamos Prendarios

Descripción:

Aplicativo utilizado para dar el servicio de préstamos prendarios, mantiene toda la funcionalidad de este producto. Debido a que es necesario su uso a nivel nacional y la dificultad geográfica para su soporte, al momento se mantiene consolidado en un servidor y los usuarios del aplicativo se conectan mediante un terminal server, en la tabla 1-9 de indica cómo está estructurado.

Modo de acceso:

Cliente /Servidor

Tabla 1-9: Descripción del Sistema de Préstamos Prendarios

Ubicación
Entidad Financiera / Proveedor

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema de préstamos Prendarios.	Sistema de Préstamos Prendarios	Red Hat 5.8 x86_64	ORACLE 11.2 Enterprise Edition	Visual Basic

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli9IP	2.55 TB	49152 MB	Activo

Usuarios
Funcionarios del área de Crédito y Operaciones

Fuente: Los Autores

1.2.1.10 Aplicativo Contable, Talento Humano y Activos Fijos

Descripción:

Es un aplicativo que maneja varios módulos de servicios, en los que se encuentra el proceso de Talento Humano, Administración de Activos y Contabilidad. El módulo de Talento Humano permite manejar todo el ciclo de vida del empleado, desde el reclutamiento, selección, plan de carrera, información histórica, administración, rol de pagos, administración de tiempo. Sin embargo al momento la institución financiera maneja un proceso paralelo con el nuevo Software de Talento Humano y trabajan paralelamente ambos aplicativos hasta que se migre totalmente al nuevo sistema, ver tabla 1-10.

Modo de acceso:

Cliente /Servidor

Tabla 1-10: Descripción del Aplicativo contable, talento humano y activos fijos.

Ubicación
Proveedor

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Aplicativo contable, talento humano y activos fijos.	Aplicativo contable, talento humano y activos fijos.	Red Hat 5.8 x86_64	ORACLE 11.2 Enterprise Edition	C#

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli10IP	2.55 TB	49152 MB	Activo

Usuarios
Funcionarios principalmente de las áreas de Talento Humano y Contabilidad

Fuente: Los autores

1.2.1.11 Software de Talento Humano

Descripción:

El nuevo aplicativo de Talento Humano reemplazará al aplicativo anterior, el que controla procesos de nómina, control de asistencia y gestión humana. Verificar la tabla 1-11 donde están los componentes del sistema.

Modo de acceso: Cliente /Servidor

Tabla 1-11: Descripción del Sistema de Talento Humano

Ubicación
Proveedor

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Software de Talento Humano	Software de administración del talento humano	Red Hat 5.8 x86_64	ORACLE 11.2 Enterprise Edition	C#

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli11IP	2.75 TB	49 GB	Activo

Usuarios
12 usuarios principalmente del área de Talento Humano

Fuente: Los autores

1.2.1.12 Aplicativo para Gestión de Riesgo Operacional

Descripción:

Aplicativo utilizado para la gestión de Riesgo Operacional a nivel institucional. En la tabla 1-12 se tiene el resumen de los componentes del sistema

Modo de acceso:

Cliente /Servidor

Tabla 1-12: Descripción del Sistema de Gestión de Riesgo Operacional

Ubicación
Institución Financiera

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Aplicativo Gestión Riesgo Operacional	Aplicativo Gestión Riesgo Operacional	WINDOWS 2008 R2	SQL SERVER 2008 R3	java

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli12IP	54.00 GB	54.00 GB	4096 MB

Usuarios
Funcionarios de todas las áreas del banco

Fuente: Los autores

1.2.1.13 Sistema de Gestión Contable.

Descripción:

El módulo de acceso al aplicativo utilizado para la gestión contable interna de la institución financiera, ver la tabla 1-13 la descripción del sistema.

Modo de acceso:

Cliente /Servidor

Tabla 1-13: Descripción del Sistema de Gestión Contable

Ubicación
Institución Financiera

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema de Gestión Contable	Sistema de Gestión contable	Windows Server 2008 R2	SQL SERVER	C#

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli13IP	450 GB	16 GB	Activo

Usuarios
Funcionarios área Financiera Administrativa

Fuente: Los autores

1.2.1.14 Sistema de Gestión de Fideicomisos

Descripción:

Este aplicativo contempla una sola solución global, utiliza una modularidad y funcionalidad ad-hoc, utilizada para fideicomisos y fondos de inversión. En la tabla 1-14 se puede observar los componentes que lo conforman.

Modo de acceso: Cliente /Servidor

Tabla 1-14: Descripción de Gestión de Fideicomisos.

Ubicación
Institución Financiera

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema de gestión de Fideicomisos	Aplicativo de manejo de fondos	Windows 2003 Standard	Sistema Archivos	Power Builder

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli14IP	92 GB	2 GB	Activo

Usuarios
Funcionario principalmente área de Inversiones, Operaciones y Riesgos

Fuente: Los autores

1.2.1.15 Sistema Monitor Transaccional

Descripción:

Proporciona una solución completa para el control de las transacciones crediticias mediante un patrón de las actividades financieras, la configuración del perfil del cliente, así como la verificación de las listas de la OFAC[7]. En la tabla 1-15 se muestra los componentes que lo conforman, ubicación y usuarios.

Modo de acceso: Cliente /Servidor

Tabla 1-15: Descripción del Sistema Monitor Transaccional

Ubicación
Institución Financiera

Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema Monitor Transaccional	Sistema de Gestión crediticia	Windows Server 2008	Windows	java

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli15IP	1 TB	16 GB	Activo

Usuarios
Funcionarios principalmente áreas de Cumplimiento y Crédito

Fuente: Los autores

1.2.1.16 Sistema de verificación de listas de control

Descripción:

Permite la detección en tiempo real en la verificación de identidad, cubre el 100% de las listas de sanciones a nivel mundial, así como las listas nacionales de UIF [8] . El resumen de componentes están en la tabla 1-16.

---

[7] Oficina de control de Activos Extranjeros de Estados Unidos: Es una oficina del Departamento del Tesoro de los Estados Unidos que identifica países, terroristas y narcotraficantes sancionables de acuerdo con las leyes de EEUU. Emite la lista OFAC también conocida como lista Clinton

8 Unidad de Inteligencia Financiera, anteriormente conocida como CONSEP

Modo de acceso: Cliente /Servidor

Tabla 1-16: Descripción del Sistema verificación de listas de control.

Ubicación				
Institución Financiera				
Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema de verificación de listas de control.	Evaluación de listas de control	Windows Server 2008 R2	16 GB	RPG

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli16IP	1 TB	16 GB	Activo

Usuarios
Funcionarios que pertenecen al área de Cumplimiento

Fuente: Los autores

1.2.1.17 Sistema para Control de Riesgos

Descripción:

Sistema de revisión de listas de control, la descripción detallada del sistema lo podemos verificar en la tabla 1-17.

Modo de acceso: Cliente /Servidor

Tabla 1-17: Descripción del Sistema de control de riesgos

Ubicación				
Institución Financiera				
Software				
Nombre	**Descripción**	**Sistema Operativo**	**Base de Datos**	**Lenguaje Programación**
Sistema de control de riesgos	Aplicativo para la gestión de riesgo Operativo	WINDOWS 2008 R2	SQL SERVER 2008 R2	java

Hardware			
Nombre	**Espacio Disco**	**Memoria**	**Estado**
SrvUIOProApli17IP	16384 MB	2.12 TB	Activo

Usuarios
Funcionarios de todas las áreas

Fuente: Los autores

1.2.2 REDES

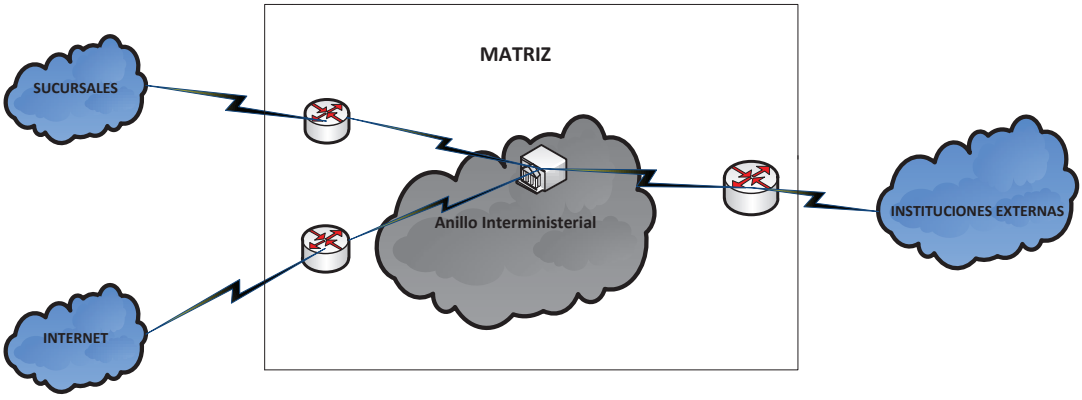
1.2.2.1 Enlaces WAN

Actualmente la institución financiera se encuentra conectada tal como se muestra en la figura 1-3:

Anillo Interministerial: El cual le permite acceder a información del Registro Civil y Presidencia.

Instituciones Externas: Son las empresas y proveedores que le dan acceso a información para sus procesos de negocio, entre ellos se encuentra: la Bolsa de Valores de Quito (BVQ), Superintendencia de Seguros (SBS), CreditReport (Equifax), Banco Central del Ecuador (BCE), Municipio del Distrito Metropolitano de Quito (MDMQ), entre los más principales.

Figura 1-3: Esquema WAN de la institución Financiera.



Fuente: Los autores.

Sucursales y Agencias: Las sucursales y agencias, permiten a los clientes acceder a los servicios de préstamos hipotecarios y quirografarios. Se mantiene como sucursal mayor en Guayaquil y agencias en Cuenca, Portoviejo y Quito Sur.

Los anchos de banda de los enlaces se describen en la tabla 1-18:

Tabla 1-18: Anchos de banda de los enlaces de Institución Financiera

DESCRIPCION	ANCHO DE BANDA (BW)
CONCENTRADOR Datos	40 Mbps
CONCENTRADOR Internet	20 Mbps
INSTITUCIONES EXTERNAS	
Edificio Matriz	70 Mbps
Proveedor 1	10 Mbps
Edifico Sucursal	3 Mbps
Buro de Crédito	2 Mbps
Municipio de Quito	1 Mbps
Proveedor 2	1 Mbps
Bolsa Valores Quito	512 Kbps
Superintendencia SBS	512 Kbps
Banco Central del Ecuador	512 Kbps
SUCURSALES – AGENCIAS	
Guayaquil	5 Mbps
Portoviejo	1 Mbps
Cuenca	1 Mbps
Quito	1 Mbps

Fuente: Los autores

1.2.3 SERVICIOS

1.2.3.1 Correo

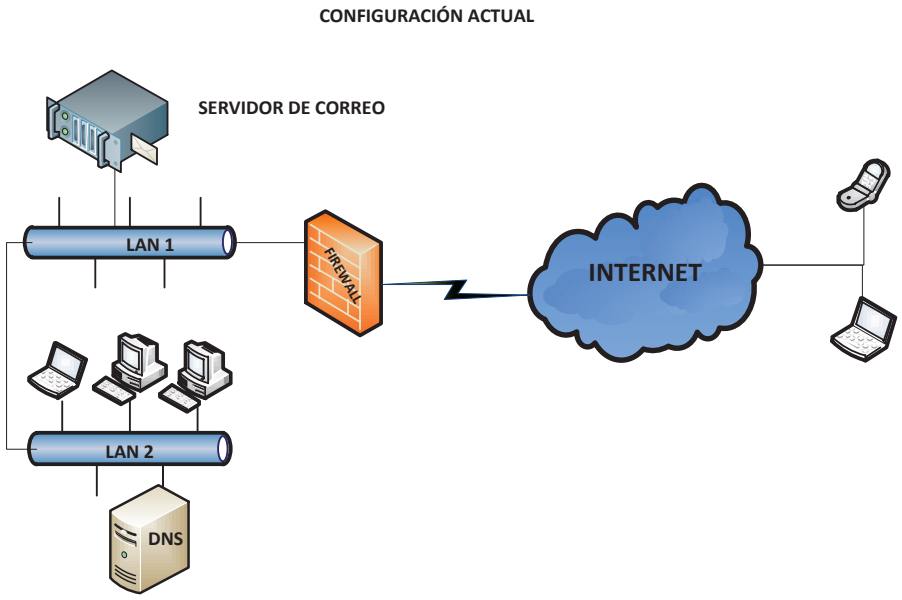
El servicio de correo que maneja la institución financiera es visualizado a través de Zimbra[9], los usuarios se conectan directamente al servidor que maneja la información consolidada de todos los clientes internos.

Al momento mantiene un proceso paralelo de manejo de correos a través del Outlook de Microsoft Office, sin embargo por el número de manejo de licencias de esta herramienta, la misma se encuentra utilizada por un grupo pequeño del personal.

[9] Aplicación que permite la recepción y envió de correo electrónico

El esquema actual del servicio de correo está representado en la Figura 1-4.

Figura 1-4: Esquema del servicio de correo de la Institución Financiera.



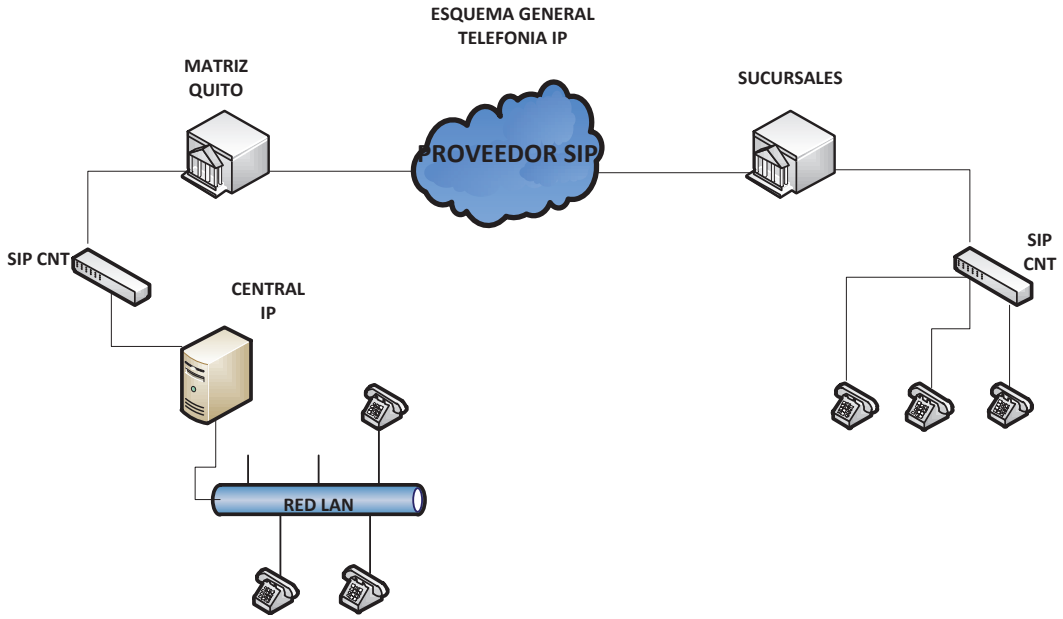
Fuente: Los autores

1.2.3.2 Telefonía IP

La institución financiera utiliza telefonía de voz sobre IP, que permite mantener en una misma red la comunicación de voz y datos, al momento se la utiliza a nivel nacional, sin embargo en agencias pequeñas y áreas específicas aún mantiene telefonía análoga.

El Esquema de telefonía IP con la que cuenta la Institución Financiera se la puede ver en la Figura 1-5.

Figura 1-5: Estructura de Telefonía IP



Fuente: Los autores

1.2.3.4 Red Inalámbrica

Este servicio se encuentra disponible en el edificio Matriz de Quito, lo que genera una ventaja en la movilidad de los equipos portátiles dentro del edificio por lo que es necesario mayor seguridad para evitar a los intrusos, para lo cual existe una Network Access Control (NAC).

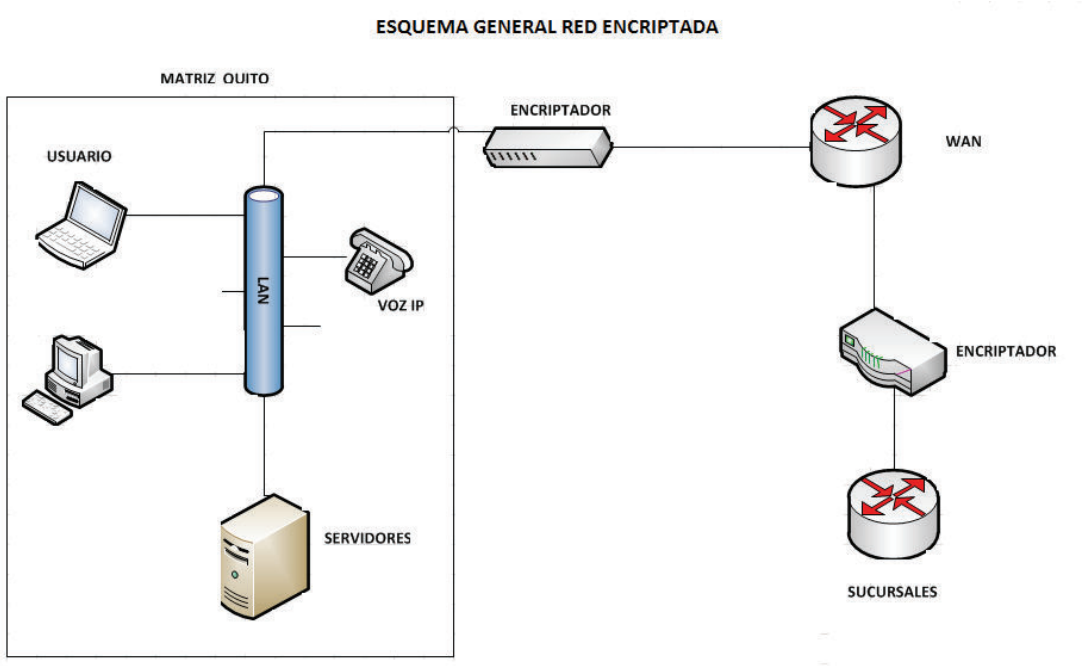
1.2.3.5 Seguridad de la Red

Para la protección de los datos en tránsito, se mantiene la encriptación de hardware a nivel de los enrutadores, se adjunta un diagrama sobre las redes externas con las que se mantiene implementado este control. Existen otras entidades con las que se tiene conexión y se realiza la encriptación mediante

software, existen otras entidades que al momento no tienen este control incluido.

En la Figura 1-6 podemos apreciar la topografía de la red.

Figura 1-6: Topología de la red.



Fuente: Los autores

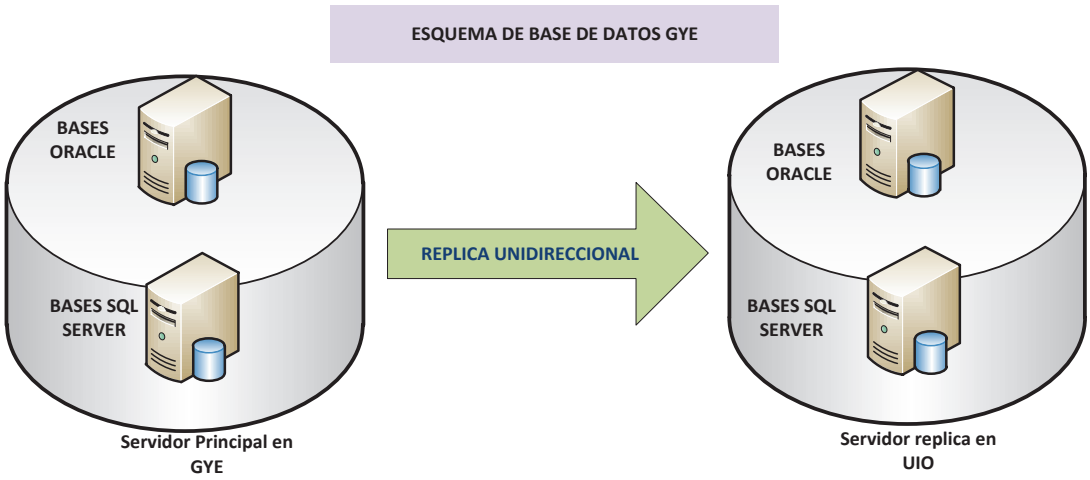
1.2.4 BASES DE DATOS

1.2.4.1 Esquema de Distribución Actual

La institución financiera mantiene la administración de las bases de datos de los aplicativos en su sitio principal y en el alterno, la información es extraída de las BDD del proveedor, procesada y almacenada en las bases locales y el resultado del proceso es devuelto a las BDD del proveedor.

En la figura 1-7 de describe el esquema de replicación de las BDD desde la ciudad de Guayaquil hacia las BDD replica en la ciudad de Quito.

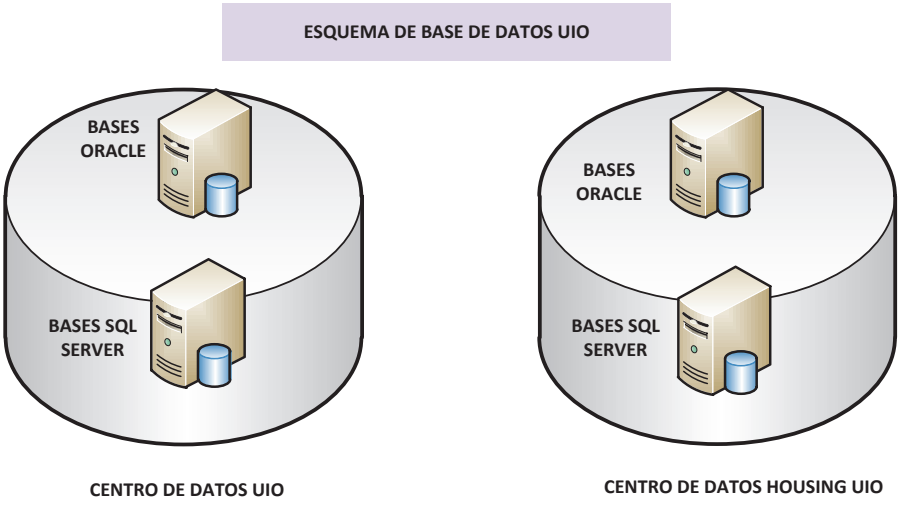
Figura 1-7: Esquema de Bases de Datos Principal (GYE).



Fuente: Los autores

En la figura 1-8 de muestra la distribución de las BDD de la ciudad de Quito que están tanto en la institución financiera como en el Housing contratado.

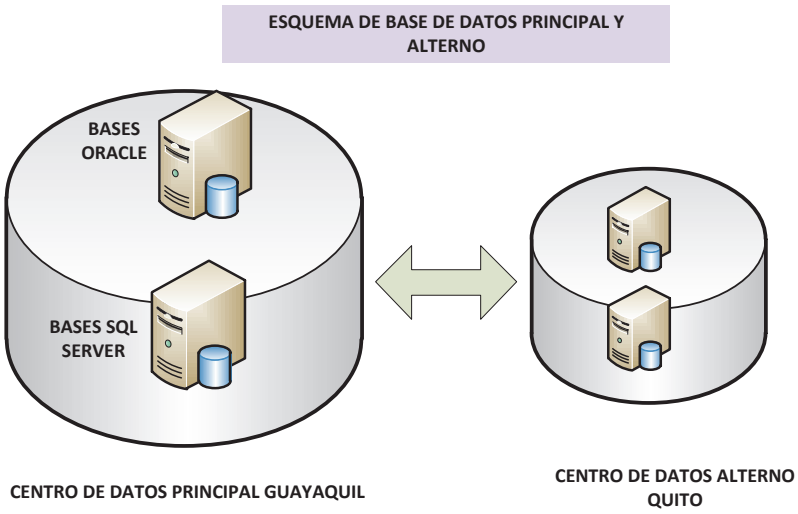
Figura 1-8: Esquema de Bases de Datos Principal (UIO).



Fuente: Los autores

En la figura 1-9 se presenta el esquema de las bases de datos del sitio principal y alterno de la institución financiera que esta implementándose.

Figura 1-9: Esquema de Bases de Datos Principal y Alterno



Fuente: Los autores

1.2.5 RESUMEN DE LA INFRAESTRUCTURA TECNOLOGICA

En la tabla 1-19 se presenta un resumen de las aplicaciones, servidores y principales servicios con los que cuenta la Institución Financiera.

Tabla 1-19: Resumen de la Infraestructura Tecnológica

N	Aplicación / Servicio	Servidor	Ubicación	Funcionarios	Clientes	Otros (Proveedor)
1	Sistema de Préstamos Quirografarios	Red Hat Enterprise Linux 5 (64-bit)	Proveedor Hosting	X	X	
2	Sistema de Préstamos Hipotecarios	Red Hat Enterprise Linux 5 (64-bit)	Proveedor Hosting	X	X	
3	Sistema de Gestión de Procesos	Microsoft Windows Server 2008 R2 (64-bit)	Proveedor Hosting	X	X	
4	Sistema De Gestión de Administración Financiera	Microsoft Windows Server 2008 R2 (64-bit)	Proveedor Hosting	X		
5	Sistema Administrador de contenido Empresarial	Microsoft Windows Server 2008 R2 (64-bit)	Proveedor Hosting	X		
6	CRM	Microsoft Windows Server 2008 R2 (64-bit)	Proveedor Hosting	X		

N	Aplicación / Servicio	Servidor	Ubicación	Funcionarios	Clientes	Otros (Proveedor)
7	Sistema de Flujo de Trabajo.	Microsoft Windows Server 2008 R2 (64-bit)	Entidad Financiera / Proveedor Hosting	X		X
8	Sistema de Inversiones	Microsoft Windows Server 2008 R2 (64-bit)	Proveedor Hosting	X		X
9	Sistema de Préstamos Prendarios	Microsoft Windows Server 2008 R2 (64-bit)	Entidad Financiera	X		
10	Sistema Contable, Talento Humano y Activos Fijos	Microsoft Windows Server 2008 R2 (64-bit)	Proveedor Hosting	X		
11	Software de Talento Humano	Red Hat Enterprise Linux 6 (64-bit)	Proveedor Hosting	X		
13	Sistema de Gestión Contable	Microsoft Windows Server 2008 R2 (64-bit)	Institución Financiera	X		
14	Sistema de Gestión de Fideicomisos	Microsoft Windows Server 2003 Standard (32-bit)	Institución Financiera	X		
15	Sistema Monitor Transaccional	Microsoft Windows Server 2008 R2 (64-bit)	Institución Financiera	X		
16	Sistema de verificación de listas de control	Microsoft Windows Server 2008 R2 (64-bit)	Institución Financiera	X		
17	Sistema para control de Riesgos	Microsoft Windows Server 2008 R2 (64-bit)	Institución Financiera	X		
18	ZIMBRA / Correo	MX-5	Institución Financiera	X		
19	DHCP/DNS	DNS	Institución Financiera	X		
20	Internet	PROXY	Institución Financiera	X		
21	Páginas Web Institución Financiera	WEB	Institución Financiera	X		
22	Telefonía IP	MasterBOx	Institución Financiera	X		

Fuente: Los autores

1.3 ANÁLISIS DE LOS REQUERIMIENTOS DE SEGURIDAD

1.3.1 EVALUACIÓN DE LA SITUACION ACTUAL

Para la evaluación inicial del estado actual de la institución financiera se utilizará la herramienta Microsoft Security Assessment Tool (MSAT)[10] la cual ofrece información y recomendaciones para la seguridad de la información en empresas con menos de 1.000 empleados.

[10] http://www.microsoft.com/es-es/download/confirmation.aspx?id=12273

El proceso de evaluación se basa en una encuesta que consta de más de 200 preguntas con respecto a infraestructura, aplicaciones, operaciones y personas. Las preguntas y respuestas se encuentran asociadas a las recomendaciones que derivan de procedimientos establecidos y aceptados, así como a estándares como ISO 17799[11] y NIST-800[12].

Perfil de riesgos para la empresa (BRP[13]): Medida del riesgo al que está expuesto una empresa, según el entorno empresarial y el sector en que compite.

La puntuación del BRP va de 0 a 100. Una puntuación más alta significa un riesgo posible aumentado al que está expuesta su empresa en esta área de análisis. Es importante tener en cuenta que una puntuación de 0 no es posible; dedicarse a una actividad comercial siempre implica un nivel de riesgo. También es importante comprender que hay riesgos comerciales que no se pueden mitigar directamente.

Índice de defensa en profundidad (DiDI[14]): Medida de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una empresa.

Este índice también tiene una puntuación de 0 a 100. Una puntuación más alta significa un entorno donde han tomado más medidas para implementar estrategias de defensa en profundidad en el área de análisis específica. *La puntuación del índice de defensa en profundidad no indica la eficacia general de la seguridad ni siquiera la cantidad de recursos para la misma, sino que cuantifica la estrategia global que se utiliza para defender el entorno*.

AoAs[15]: Áreas de análisis que son la infraestructura, las aplicaciones, operaciones, y la gente.

---

11 Norma internacional que ofrece recomendaciones para para realizar la gestión de seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

12 Metodología de Gestión de Riesgo.

13 Business Risk Profile.

14 Defense-in-Depth Index

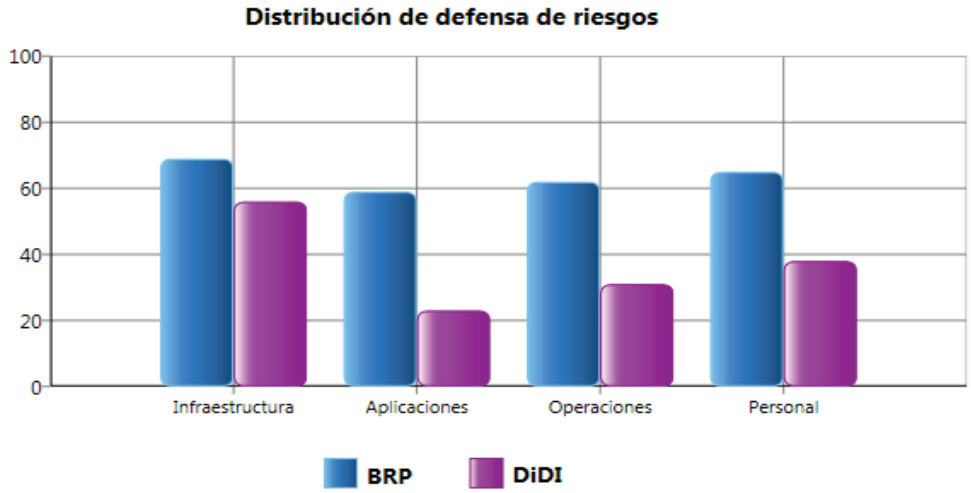
15 Areas of analysis.

1.3.1.1 Evaluación General

La Figura 1-10, dividida en áreas de análisis, muestra las diferencias en el resultado de la defensa en profundidad.

La barra azul muestra el nivel de riesgo al que está expuesto la empresa y la medida violeta muestra el nivel de controles que se han incluido considerando defensa en profundidad.

Figura 1-10: Distribución de defensa de Riesgos



Fuente: Evaluación realizada por los autores utilizando la herramienta MSAT. Quito. Octubre/2014

Resultados:

En la tabla 1-20 podemos apreciar la puntuación de perfil de riesgo de la institución financiera.

Tabla 1-20: Puntuación perfil de Riesgo de la Institución Financiera

Areas de análisis	Distribución de defensa de riesgos	Madurez de la seguridad
Infraestructura		
Aplicaciones		
Operaciones		
Personal		

Leyenda		
	Distribución pareja	Optimizada
	Disparidad leve	Estándar
	Disparidad significativa	Básica

Fuente: Evaluación realizada por los autores utilizando la herramienta MSAT. Quito. Octubre/2014

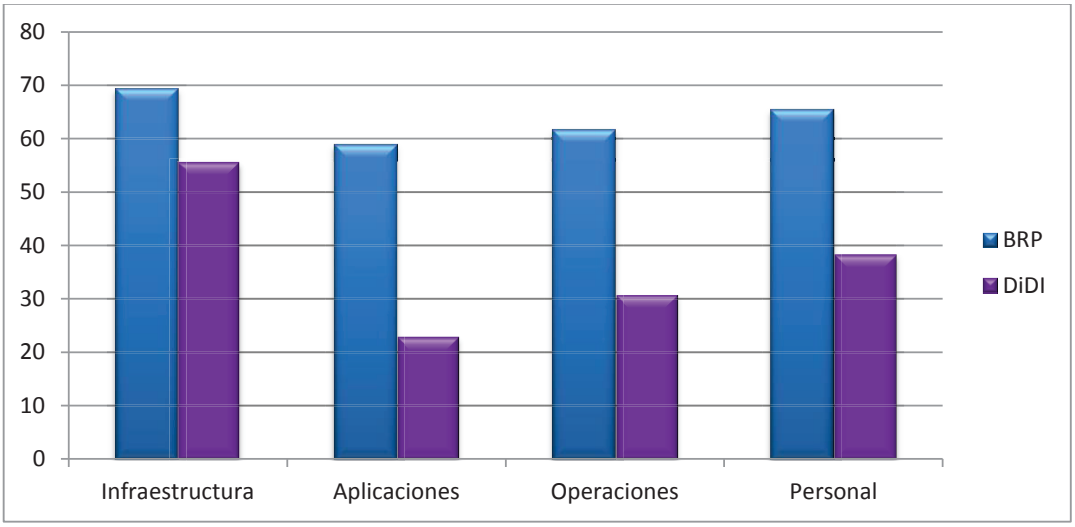
Por lo general, es mejor contar con una calificación de índice de defensa en profundidad (DiDI) del mismo nivel que otra del perfil de riesgo de la empresa (BRP) para la misma categoría.

Un desequilibrio, ya sea dentro de una categoría o entre categorías, en cualquier dirección, puede indicar la necesidad de evaluar las necesidades de control definidas para el área de Tecnología.

1.3.1.1.1 Interpretación del gráfico

La Figura 1-11 muestra la puntuación del Perfil de Riesgo de la Empresa vs Índice de defensa en profundidad (DiDI) en las áreas de análisis (AoAs).

Figura 1-11: Esquema de defensa en profundidad Riesgo vs Controles



Fuente: Evaluación realizada por los autores utilizando la herramienta MSAT. Quito. Octubre/2014

1.3.1.2 Medidas de defensa

Corresponden a un estado en el cual se indica si las defensas de la institución tiene falencias, si puede mejorar o cumple con las prácticas establecidas de seguridad.

La herramienta MSAT nos brinda la siguiente clasificación en base a las respuestas dadas durante la evaluación de riesgos, sin embargo el análisis está basado en la percepción de controles establecidos por el encuestado.

Esta evaluación nos permite tener una visión global del estado actual de la institución financiera, en la tabla 1-21 se verifica la Evaluación del Cumplimiento de las Normas de Seguridad.

Tabla 1-21: Tabla Evaluación de Cumplimiento de Normas de Seguridad.

Leyenda:	● Cumple las mejores prácticas recomendadas	● Necesita mejorar	● Carencias severas

Infraestructura	●
Defensa del perímetro	●
Reglas y filtros de cortafuegos	●
Antivirus	●
Antivirus - Equipos de escritorio	●
Antivirus – Servidores	●
Acceso remoto	●
Segmentación	●
Sistema de detección de intrusiones (IDS)	●
Inalámbrico	●
Autenticación	●
Usuarios administrativos	●
Usuarios internos	●
Usuarios de acceso remoto	●
Directivas de contraseñas	●
Directivas de contraseñas-Cuenta de administrador	●
Directivas de contraseñas-Cuenta de usuario	●
Directivas de contraseñas-Cuenta de acceso remoto	●
Cuentas inactivas	●
Gestión y control	●
Informes sobre incidentes y respuesta	●
Creación segura	●
Seguridad física	●
Aplicaciones	●
Implementación y uso	●
Equilibrio de carga	●
Clústeres	●
Aplicación y recuperación de datos	●
Fabricante de software independiente (ISV)	●
Desarrollado internamente	●
Vulnerabilidades	●
Diseño de aplicaciones	●
Autenticación	●
Directivas de contraseñas	●
Autorización y control de acceso	●
Registro	●
Validación de datos de entrada	●
Metodologías de desarrollo de seguridad de software	●

Operaciones	●
Entorno	●
Host [16]de gestión	●
Host de gestión-Servidores	●
Host de gestión - Dispositivos de red	●
Directiva de seguridad	●
Clasificación de datos	●
Eliminación de datos	●
Protocolos y Servicios	●
Uso aceptable	●
Gestión de cuentas de usuarios	●
Regulación	●
Directiva de seguridad	●
Gestión de actualizaciones y revisiones	●
Documentación de la red	●
Flujo de datos de la aplicación	●
Gestión de actualizaciones	●
Gestión de cambios y configuración	●
Copias de seguridad y recuperación	●
Archivos de registro	●
Planificación de recuperación ante desastres y reanudación de negocio	●
Copias de seguridad	●
Dispositivos de copia de seguridad	●
Copias de seguridad y restauración	●
Personal	●
Requisitos y evaluaciones	●
Requisitos de seguridad	●
Evaluaciones de seguridad	●
Directiva y procedimientos	●
Comprobaciones del historial personal	●
Directiva de recursos humanos	●
Relaciones con terceros	●
Formación y conocimiento	●
Conocimiento de seguridad	●
Formación sobre seguridad	●
Almacenamiento y comunicaciones de datos	●
Cifrado	●
Cifrado – Algoritmo	●

Fuente: Reporte MSAT Informe Completo. Quito. Enero/2015

[16] En español significa anfitrión, son las computadoras conectadas a una red, que proveen y utilizan servicios de ella. Los usuarios deben utilizar anfitriones para tener acceso a la red

A continuación describiremos los resultados dados por la herramienta MSAT, el informe completo lo encontramos en el Anexo 1-A.

1.3.1.2.1 Infraestructura

La seguridad de la infraestructura se centra en la manera como se debe administrar la red, su mantenimiento y configuración, así como también los procesos operativos ejecutados.

Defensa del Perímetro

Corresponde al primer escudo para la protección de acceso de intrusos, donde la red interna se conecta al exterior.

Reglas y filtro de Cortafuegos
Existen en todas las Oficinas

Se tiene creados uno o varios segmentos DMZ[17] para proteger los recursos corporativos accesibles a través de internet.
Se utiliza software de cortafuegos basados en Host para proteger los recursos.

No se comprueba regularmente los cortafuegos para asegurarse de que funciona correctamente.

Antivirus

Que no hay ningún software antivirus instalado en los hosts del perímetro de red.

Los equipos de escritorio utilizan soluciones antivirus.

[17] Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

Se han utilizado soluciones antivirus en el nivel del servidor.

Acceso Remoto

Existen empleados y/o socios que se conectan remotamente a la red interna y que ha dado el paso importante de utilizar tecnología de Red Privada Virtual (VPN) para permitirles el acceso. Sin embargo, no ha utilizado autenticación multi factor como un segundo escudo protector.

Segmentación

Los servicios ofrecidos en Internet se alojan en la red de su empresa.
La red presenta más de un segmento.
Actualmente no existe segmentación de la red en el entorno. Es importante mantener Los servicios extranet de clientes y socios en sus segmentos de red propios

Sistema de detección de Intrusos

Utiliza un sistema de detección de intrusiones basado en red (NIDS)
Utiliza un sistema de detección de intrusiones basado en host (HIDS)

Inalámbrico

Existe la opción de conexión inalámbrica a su red.
Se ha modificado el SSID[18] predeterminado del punto de acceso.
No ha desactivado la difusión del SSID en el punto de acceso.
No utiliza el cifrado WEP[19] en el entorno inalámbrico.
Utiliza el cifrado WPA[20] en el entorno inalámbrico.
Utiliza la restricción por MAC[21] en el entorno inalámbrico.

---

[18] (Service Set Identifier) es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.
[19] Wired Equivalent Privacy, es el sistema de cifrado incluido en el estándar IEEE 802.11.
[20] Wi-Fi Protected Access *es* un sistema para proteger las redes inalámbricas.

La red inalámbrica se considera de no confianza.

Autenticación

Permite que usuarios no autorizados ingresen a los sistemas ya sea de manera local como remota.

Usuarios Administrativos

No se utilizan inicios de sesión distintos para la administración de seguridad de los sistemas ni de los dispositivos del entorno.
Los usuarios no tienen habilitados accesos administrativos a sus estaciones de trabajo
Este momento sólo se requiere autenticación de contraseñas complejas para el acceso administrativo a dispositivos y hosts.

Usuarios Internos

Actualmente se requiere sólo autenticación de contraseñas complejas para que los usuarios accedan a la red interna y a los hosts. Una contraseña se considera compleja si cumple los siguientes criterios:

- Alfanumérica.
- Incluye mayúsculas y minúsculas.
- Al menos un carácter especial.
- Longitud mínima de 8 caracteres.

Usuarios Accesos Remoto

Los empleados pueden conectarse a la red de forma remota.
Los contratistas pueden conectarse a la red de forma remota.
Terceros usuarios pueden conectarse a la red de forma remota.

---

[21] Media Access Control es un identificador único de 48 bits de una tarjeta o dispositivo de red.

Directivas de contraseñas

Las cuentas de administrador no utilizan directivas de contraseñas.
Las cuentas de usuarios utilizan directivas de contraseñas.
Las cuentas de acceso remoto no utilizan directivas de contraseñas.

Cuentas Inactivas

Organización dispone de un proceso formal para revisar cuentas de usuarios inactivas.
Existen directivas para las actualizaciones de firmas de virus en el entorno.

Gestión y Control

Establecer procedimientos para la creación de informes de incidentes y sus respuestas, problemas o preocupaciones sobre seguridad y designar un equipo de respuesta de emergencia que incluya representantes de varias disciplinas, incluida tecnología, recurso humanos y legal son fundamentales para responder a todos los incidentes y problemas de seguridad.

Creación Segura

- No se han instalado cortafuegos particulares en todas las estaciones de trabajo del entorno.
- Los procesos de creación de los dispositivos de infraestructura están documentados.
- No hay software de acceso remoto del lado del cliente instalado en las estaciones de trabajo que se conectan remotamente a la red corporativa
- Los procesos de creación de los servidores están documentados
- No utiliza ningún software de cifrado de discos en el entorno
- Los procesos de creación de las estaciones de trabajo y los portátiles están documentados

- Utiliza algún software de control/gestión remota en el entorno
- Utiliza un protector de pantalla protegido por contraseña en el entorno
- No se utilizan módems en el entorno.

Seguridad Física

- Se han instaurado controles de seguridad física para proteger los activos de la empresa.
- No se ha instalado ningún sistema de alarma para detectar ni informar de intrusiones
- Todo o parte de lo siguiente está implementado. (Tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada).
- Los equipos de la red se hallan en una habitación cerrada con acceso restringido.
- Tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada no están implementados.
- Los equipos de la red se encuentran además en un armario cerrado.
- Tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada no están implementados.
- Los servidores se hallan en una habitación cerrada con acceso restringido.

Todo o parte de lo siguiente está implementado. (Tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada).
Los servidores se encuentran además en un armario cerrado.
Las estaciones de trabajo no están protegidas con cables de seguridad.
Los ordenadores portátiles están protegidos con cables de seguridad.

Los materiales impresos confidenciales no se almacenan en armarios con llave.

1.3.1.2.2 Aplicaciones

Es necesario tener una comprensión total de la seguridad de las aplicaciones, la arquitectura, así como de un conocimiento sólido de la base de la aplicación del usuario. Sólo entonces podrá comenzar a identificar las posibles amenazas.

Implementación y Uso

Equilibrio de Carga

No se utilizan equilibradores de carga en el entorno

Clústeres

No se utiliza la agrupación en clústeres en el entorno

Aplicación y Recuperación de Datos

Su empresa tiene una línea de aplicaciones empresariales
No se realizan periódicamente pruebas de la recuperación de aplicaciones y datos

Vendedor independiente de software (ISV)

Otros fabricantes han desarrollado una o más de las aplicaciones principales del entorno.
Los fabricantes independientes de software no le suelen ofrecer revisiones ni actualizaciones de seguridad.

Desarrollado Internamente.

La empresa utiliza macros personalizadas en las aplicaciones ofimáticas.
El equipo interno de desarrollo de software no le suele ofrecer revisiones ni actualizaciones de seguridad.

Vulnerabilidades

La empresa utiliza macros personalizadas en las aplicaciones ofimáticas.
No hay procedimientos que aborden los aspectos vulnerables de la seguridad conocidos.

Diseño de Aplicaciones

Las aplicaciones deben utilizar un mecanismo de seguridad que no permita que personas ajenas a los sistemas puedan tener acceso a la información, y cualquier tipo de violación a la seguridad.

Autenticación

Se usa la autenticación de contraseñas complejas en las aplicaciones principales.

Directivas de contraseñas

Se usan controles de contraseñas complejas en todas las aplicaciones principales.
La caducidad de las contraseñas se controla en todas las aplicaciones principales.
Se utilizan controles de bloqueo de cuentas en todas las aplicaciones principales.

Autorización y control de Acceso

Las aplicaciones principales limitan el acceso a datos y funciones confidenciales según los privilegios de la cuenta.

Registro

Existen varios eventos registrados por las aplicaciones del entorno. Las aplicaciones deben registrar todos los eventos según las prácticas recomendadas.

- No se registran los intentos fallidos de autenticación.
- No se registran los intentos de autenticación correctos.
- No se registran los errores de las aplicaciones.
- No se registran los accesos denegados a los recursos.
- No se registran los accesos correctos a los recursos.
- Se registran los cambios en los datos.
- No se registran los cambios en las cuentas de usuario.

Validación de Datos de Entrada

- Si se validan los datos de entrada de todos los usuarios finales.
- No se validan los datos de entrada de las aplicaciones de cliente.
- No se validan los datos de entrada que proceden de un "feed de datos"[22].

Metodologías de desarrollo de seguridad de Software

Su organización utiliza herramientas de pruebas de software de seguridad como parte del proceso de desarrollo de seguridad.

[22] Es un archivo formado por una lista de productos que utilizan grupos de atributos que definen cada uno de sus productos de forma exclusiva

Su organización no proporciona formación sobre metodologías de seguridad para software para su personal de desarrollo

Almacenamiento de datos y comunicaciones

Los datos son uno de los recursos más importantes de la empresa, se debe asegurar siempre su integridad y seguridad ya que cualquier pérdida o manipulación podría causar pérdidas.

Cifrado

Las aplicaciones no cifran los datos cuando están almacenados o se están transmitiendo.

1.3.1.2.3 Operaciones

Esta área de análisis examina las prácticas, procedimientos y pautas operativas que sigue la empresa para ayudar a mejorar la defensa en profundidad. Esta evaluación examina directivas y procedimientos que regulan las creaciones del sistema, la documentación de la red y el uso de tecnología en el entorno. También incluye las actividades de apoyo necesarias para gestionar la información y los procedimientos que utilizan los administradores y el equipo de operaciones en el entorno.

Entorno

Host de Gestión de Servidores
Existe un equipo de gestión dedicado a los servidores

Host de Gestión de Dispositivos de Red
Existe un equipo de gestión dedicado a administrar dispositivos de red

Política de Seguridad

Corresponden a una serie de procedimientos normados que abarcan a todas las áreas de la empresa y que deben garantizar y regular el uso de la tecnología y procesos de la organización.

Clasificación de datos

No existe conocimiento del personal de la empresa sobre la clasificación de los datos.

Eliminación de datos

No existe conocimiento del personal de la empresa sobre la clasificación de los datos.

Protocolos y Servicios

Existen pautas que tratan los servicios y protocolos permitidos, pero no están documentadas

Protocolos y Servicios

Existen pautas que tratan los servicios y protocolos permitidos, pero no están documentadas

Uso Aceptable

Existe una directiva corporativa para el uso aceptable

Gestión de Cuentas de usuario

Se utilizan directivas que regulan la gestión de cuentas de los usuarios individuales dentro del entorno

Regulación

Su empresa dispone de directivas para controlar el entorno
Políticas de Seguridad

Existe una directiva de seguridad de la información para controlar la actividad relacionada con la seguridad de la empresa

La directiva se desarrolló conjuntamente por el departamento de Tecnología y de representantes comerciales

Gestión de Actualizaciones y revisiones de Software

Para garantizar la seguridad de la información y de las aplicaciones que la manejan, se deben garantizar los procedimientos de actualización de Software y corrección de problemas detectados.

Documentación de la Red

Existen diagramas lógicos de red en su entorno que se actualizan con regularidad

Flujo de Datos de la aplicación

No existen diagramas de la arquitectura ni del flujo de datos de las aplicaciones principales

Administración de actualización de software

No existen directivas que regulen la gestión de actualizaciones ni revisiones de los sistemas operativos y de las aplicaciones

Administración de cambios y configuraciones

La empresa no dispone de ningún proceso de gestión de cambios ni configuraciones

Copias de Seguridad y Respaldos

La falta de respaldos de la información podría causar pérdidas potenciales en la empresa.

Archivos de registro de pistas de auditoría.

Actualmente no existe ningún registro activado en el entorno.

Recuperación ante desastres y continuidad del negocio

No se conoce si existen planes

Copias de seguridad

Se hacen copias de seguridad periódicas de los recursos críticos

Medios de copia de Seguridad

No existen directivas para la gestión ni el almacenamiento de los dispositivos de copias de seguridad

Copias de seguridad y restauración

No existen directivas para las pruebas periódicas de los procedimientos de copias de seguridad y restauración

1.3.1.2.4 Personal

Esta sección de la evaluación revisa aquellos procesos de la empresa que regulan las directivas de seguridad corporativa, los procesos de recursos humanos, así como la formación y la divulgación de materias de seguridad para los empleados

Requisitos y Evaluaciones

La empresa debe identificar a los individuos con experiencia en el tema de la seguridad para incluirlos en todas las reuniones y decisiones relacionadas.

Requisitos de Seguridad

Que existen equipos comerciales y de seguridad que trabajan definiendo requisitos de seguridad

El equipo de seguridad no participa en la fase de planificación ni diseño del ciclo de vida de la tecnología.

La empresa no tiene ningún modelo para la asignación de niveles de gravedad a cada componente del entorno informático

El equipo de seguridad no participa en la fase de implantación del ciclo de vida de la tecnología

Evaluación de Seguridad

Empresas independientes realizan evaluaciones de la seguridad en su empresa.

Las evaluaciones de la seguridad de su empresa no las realiza personal interno

Directiva y Procedimientos

Se deben realizar comprobaciones del historial personal para descubrir cualquier problema posible, con objeto de reducir el riesgo al que se exponen la empresa y los empleados. Este proceso también permite localizar cualquier problema o laguna en el currículum del aspirante.
El proceso de contratación de personal debe incluir una evaluación del historial laboral y cualquier antecedente penal del aspirante.

Comprobaciones del historial del personal

En la empresa no se llevan a cabo comprobaciones del historial personal como parte integral del proceso de contratación

Política de Recursos Humanos

No existe ninguna directiva formal para los empleados que dejan la empresa.

Relaciones con terceros

En la empresa gestiona el entorno informático
Existen directivas para regular las relaciones con terceros

Los sistemas se configuran por parte de los proveedores o distribuidores de hardware

Capacitación y Formación

Un programa formal de divulgación de las medidas de seguridad ayuda a los empleados a contribuir a la seguridad global de la empresa, puesto que se les mantiene informados acerca de los riesgos existentes.

Conocimiento de seguridad

Se ha asignado a un individuo o grupo la seguridad de su empresa.

El equipo de seguridad participa en la definición de los requisitos para las nuevas tecnologías o para las ya existentes.

Existe un programa de divulgación de las medidas de seguridad en la empresa.

Los cursos de formación se organizan anualmente

Más del 75% de los empleados han participado en un programa de divulgación sobre la seguridad

Los cursos de formación no tratan la seguridad informática, ni el uso de cortafuegos particulares y cifrados.

Formación de seguridad

La empresa no ofrece actualmente a los empleados formación específica por temas de seguridad.

1.3.1.3 Iniciativas de Seguridad.

Se puede determinar que las áreas de Infraestructura, Aplicaciones, Operaciones y Personal no cumplen con las mejores prácticas recomendadas y deben revisarse a detalle cada una de ellas.

1.4 DETERMINACION DE LOS RIESGOS POTENCIALES

Bajo la evaluación realizada con el aplicativo MSAT se determinan los siguientes riesgos potenciales.

1.4.1 RIESGOS DE PROBABILIDAD ALTA

Los puntos encontrados están asociados a Riesgos de acceso: Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información.
En la tabla 1-22 se pueden observar los riesgos de Probabilidad Alta

Tabla 1-22: Riesgos de Probabilidad Alta

Vulnerabilidad y Recomendación	
Tema del análisis	***Recomendación***
Prioridad alta	
Infraestructura - Gestión y control - Creación segura	Aplique una directiva que solicite una revisión periódica de las configuraciones predeterminadas de los cortafuegos para tener en cuenta los cambios en las aplicaciones o los servicios utilizados.
Infraestructura - Defensa del perímetro - Acceso remoto	Estudie utilizar la autenticación multifactor para la conexión de usuarios remotos a través de Internet a los recursos corporativos. Revise con regularidad la lista de acceso de los usuarios en el dispositivo VPN.
Infraestructura - Autenticación - Usuarios de acceso remoto	Si aún no lo ha hecho, estudie la utilización de un sistema de autenticación multifactor de acceso remoto y limite el acceso únicamente a aquellos empleados que tengan una necesidad empresarial de conectividad remota.
Personal - Directiva y procedimientos - Relaciones con terceros	Para reducir los riesgos que implica la ejecución de los servicios predeterminados, el personal interno debería configurar los sistemas siguiendo una simulación de creación.
Infraestructura - Defensa del perímetro – Segmentación	Asegúrese de que los cortafuegos, la segmentación y los sistemas de detección de intrusiones permiten proteger la infraestructura de la empresa de los ataques desde Internet.

Fuente: Reporte MSAT Informe Completo. Quito. Enero/2015

1.4.2 RIESGOS DE PROBABILIDAD MEDIA

En la tabla 1-23 se pueden observar los riesgos de probabilidad media que están asociados a falta de controles en la seguridad física, de red y procesos establecidos en el desarrollo de software.

Tabla 1-23: Riesgos de Probabilidad Intermedia

Vulnerabilidad y Recomendación	
Tema de análisis	**Recomendación**
Prioridad intermedia	
Infraestructura - Gestión y control - Seguridad física	Continúe utilizando los controles físicos y considere su uso en todos los equipos informáticos en caso de que aún no se haya realizado.
Infraestructura - Defensa del perímetro – Inalámbrico	Para reducir los riesgos asociados a las redes inalámbricas, la implantación no debe incluir la difusión del SSID, pero sí el cifrado WPA, además de tratar la red como de no confianza.
Personal - Requisitos y evaluaciones - Requisitos de seguridad	La asignación de niveles de importancia a cada componente de la infraestructura informática permite que la mayoría de los recursos se apliquen a aquéllos equipos establecidos como los más críticos, por lo que los sistemas que son menos críticos reciban menos recursos.
Aplicaciones - Diseño de aplicaciones – Registro	Para facilitar la gestión y el análisis de los archivos de registro, puede integrarlos en un mecanismo de registro central. Este mecanismo guarda estos archivos según la directiva corporativa de retención de datos.

Aplicaciones - Diseño de aplicaciones - Validación de datos de entrada	Siga auditando cada aplicación para asegurarse de que se validan los datos de entrada de forma sistemática y apropiada. Las restricciones de validación de datos de entrada deben permitir datos con sintaxis y semántica correctas y no efectuar únicamente el análisis para la detección de caracteres no válidos.

Fuente: Reporte MSAT Informe Completo. Quito. Enero/2015

1.4.3 RIESGOS DE PROBABILIDAD BAJA

Los riesgos encontrados están asociados a mejorar los controles existentes y la documentación que debe existir para los procedimientos establecidos. Los riesgos de probabilidad baja los podemos aprecia en la tabla 1-24.

Tabla 1-24: Riesgos de Probabilidad Baja

Vulnerabilidad y Recomendación	
Tema de análisis	**Recomendación**
Prioridad baja	
Operaciones - Entorno - Host de gestión-Servidores	Piense en utilizar un intérprete de órdenes seguras (Security Shell) o VPN para asegurar los protocolos de gestión de texto sin formato.
Operaciones - Entorno - Host de gestión - Dispositivos de red	Pruebe todos los sistemas de gestión que utilizan protocolo SNMP para asegurar que tengan las actualizaciones más recientes y que no utilicen cadenas comunitarias predeterminadas.
Operaciones - Directiva de seguridad - Protocolos y servicios	Documente las pautas de los protocolos y servicios permitidos y publique esta información en la intranet[23] corporativa. Considere la implantación de directivas que regulen los cambios en las pautas.
Operaciones - Directiva de seguridad - Uso aceptable	Todos los empleados y clientes que utilizan recursos corporativos deben estar familiarizados con estas directivas. Publíquelas en la intranet y estudie introducirlas en el curso de orientación de empleados nuevos.
Operaciones - Copias de seguridad y recuperación - Copias de seguridad	Audite los mecanismos para realizar copias de seguridad y asegúrese de que se utilizan a menudo para los recursos críticos. Pruebe con regularidad el proceso de restauración para garantizar la recuperación de datos desde los dispositivos de copias de seguridad.

Fuente: Reporte MSAT Informe Completo. Quito. Enero/2015

[23] Red informática que utiliza la tecnología del Protocolo de Internet dentro de una organización.

CAPITULO 2: PLANIFICACION DEL SISTEMA DE SEGURIDAD DE LA INFORMACION

2.1 ANALISIS Y EVALUACION DE RIESGOS

En este capítulo se realizará el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, para lo cual se debe identificar las vulnerabilidades que los debilitan y las amenazas que lo rodea con el fin de valorar el grado de riesgo al que está expuesto. Con esta información la alta gerencia define si los riesgos encontrados deber ser eliminados, ignorados, asumidos, mitigados o controlados.

El análisis de riesgo es el punto central de la definición de una estrategia de seguridad, la que debe estar alineada con la visión de la organización y su entorno operacional.

2.1.1 METODOLOGIA DE EVALUACION DE RIESGOS

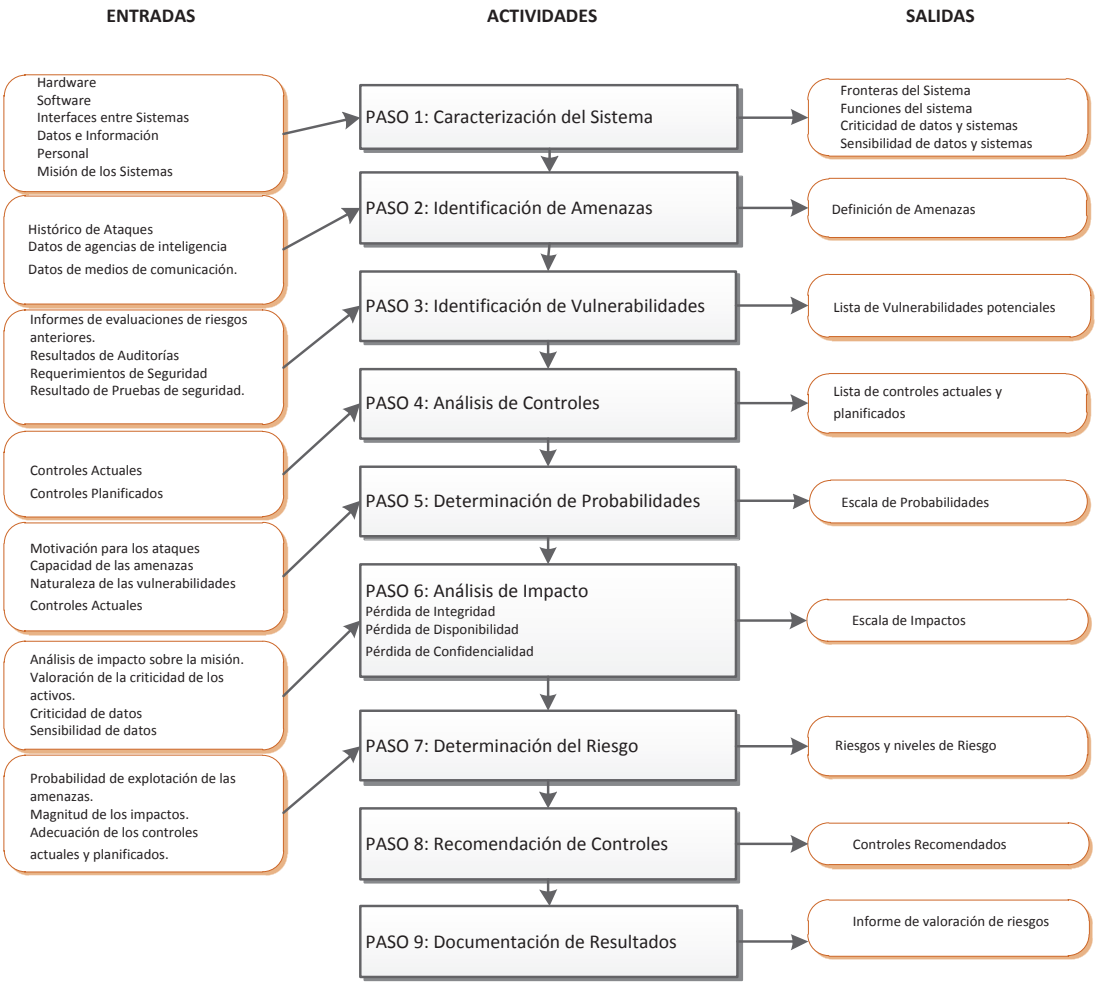
La metodología seleccionada para esta evaluación es la NIST 800-30 acorde a la evaluación y justificación descrita en el Anexo 2-A, para el manejo de riesgos de Seguridad de la Información, consta de los siguientes pasos:

Paso 1.	Caracterización del Sistema
Paso 2.	Identificación de las Amenazas
Paso 3.	Identificación de las Vulnerabilidades
Paso 4.	Análisis de Controles
Paso 5.	Determinación de la Probabilidad
Paso 6.	Análisis del Impacto
Paso 7.	Medición del Riesgo
Paso 8.	Recomendaciones para el Control
Paso 9.	Documentación de Resultados

2.1.1.1 Pasos de la Metodología

En la figura 2-1 podemos verificar la metodología de trabajo que utilizaremos en el presente trabajo.

Figura 2-1: Metodología de Evaluación de Riesgos



Fuente: http://csrc.nist.gov/publications/PubsSPs.html#800-30 Ultimo Acceso: Febrero 2015

De acuerdo a la metodología descrita, se describe los pasos a seguir:

Paso 1. Caracterización del Sistema:

En este paso se identifican, analizan y valoran los activos de la organización; los límites del sistema tecnológico son detallados, junto con los recursos y la

información que constituyen el sistema. Lo cual permite definir el alcance de la evaluación del riesgo y proporciona información de la infraestructura tecnológica de la empresa.

Dentro de la caracterización los siguientes puntos son evaluados:

- Hardware
- Software
- Las interfaces del sistema (por ejemplo, la conectividad interna y externa)
- Los datos y la información
- Las personas que apoyan y utilizan el sistema tecnológico
- La misión del sistema (por ejemplo, los procesos realizados por el sistema de TI
- Sistema y criticidad de datos.
- Sistema y sensibilidad de los datos.
- Las políticas de seguridad que rigen el sistema de TI
- La arquitectura de seguridad del sistema.

Paso 2. Identificación de Amenazas

El objetivo de este paso es identificar las potenciales amenazas sobre los recursos del sistema y elaborar un listado de las que son aplicables en el sistema informático que se está evaluando.

La identificación de amenazas está adaptada a las personas, organización y su entorno de procesamiento. Las fuentes de información para la identificación se lo realizan mediante fuentes ya definidas por organismos internacionales, así como características propias del entorno de la institución financiera.

Paso 3. Identificación de Vulnerabilidades

El objetivo de este paso es elaborar una lista de las vulnerabilidades del sistema (defectos o debilidades) que podrían ser explotados por amenazas potenciales y determinar la calidad de los controles de seguridad implementados.

La identificación de vulnerabilidades se realizará mediante el levantamiento de información utilizando para ello encuestas al personal, revisión en situ del cumplimiento de controles de seguridad y los resultados de evaluaciones realizadas por terceros al ambiente de producción de la institución financiera.

Paso 4. Análisis de Controles

En este paso se analiza los controles que se han implementado o están previstos para su aplicación, cuyo objeto es minimizar o eliminar la probabilidad de materializar una amenaza sobre las vulnerabilidades existentes del sistema

Paso 5. Determinación de Probabilidades

El objetivo es indicar la probabilidad de que una vulnerabilidad puede ser explotada versus a una amenaza específica asociada, la escala de las vulnerabilidades están listadas en la Tabla 2-1

Tabla 2-1: Escala de manejo de Vulnerabilidad

Escala para manejo de Vulnerabilidad	
Calificación de Vulnerabilidad	**Descripción**
Muy Alto	Fallo operativo total, insalvable.
Alto	Pérdida severa de la capacidad operacional y altamente dañino y extremadamente costosa sin embargo la operatividad mínima se mantiene.
Moderado	Impacto sustancial operacional, muy costoso.
Bajo	Notable impacto operativo pero limitado, algunos costos.
Muy Bajo	Mínimo o ningún impacto operacional, costos insignificantes.

Fuente: Los Autores, acorde a lo establecido en la escala de vulnerabilidades de la Metodología NIST800-30.

Paso 6. Análisis de Impacto

En este punto se determina los efectos adversos resultantes de un ejercicio de amenaza exitosa de una vulnerabilidad. Un análisis del impacto (También conocido como análisis de impacto en el negocio [BIA] para algunas organizaciones prioriza el impacto asociado con el compromiso de los activos

de información de una organización basada en una evaluación cualitativa o cuantitativa de la sensibilidad y criticidad de dichos activos.

Independientemente del método utilizado para determinar el grado de sensibilidad de un sistema informático y sus datos, son los propietarios de los sistemas y de la información los responsables de determinar el nivel de impacto de su propio sistema y la información. Por consiguiente, en el análisis de impacto, el enfoque apropiado es entrevistar al propietario (s) del sistema de información. En la tabla 2-2 se encuentra la información de la escala de amenazas.

Tabla 2-2: Escala de manejo de Amenaza

Escala para la medición de Amenazas	
Escala Amenaza	***Descripción***
Muy Alto	Estamos obligados a experimentar nuevos incidentes de este tipo - de hecho, es probable que estén ocurriendo ahora mismo.
Alto	Somos propensos a experimentar incidentes de esta naturaleza dentro de poco.
Moderado	Es muy posible que vamos a experimentar incidentes de esta naturaleza
Bajo	Los incidentes de esta naturaleza no son comunes, pero hay una posibilidad real de que sé experimentan en algún momento futuro
Muy Bajo	A pesar de que son concebibles, probablemente nunca se experimenten incidentes de esta naturaleza

Fuente: Los Autores, acorde a lo establecido en la escala de amenazas de la Metodología NIST800-30.

El impacto negativo de un evento de seguridad se puede describir en términos de la pérdida o degradación de una o de una combinación de cualquiera de los tres objetivos de seguridad: integridad, disponibilidad y confidencialidad.

Pérdida de la integridad.

La integridad se pierde si se realizan cambios en los datos ya sea por actos intencionales o accidentales. Si la pérdida de integridad de los datos no se corrige, podrían causar inexactitud, fraude o decisiones erróneas. Además, la falta de la integridad puede ser el primer paso de un ataque exitoso contra el sistema para generar pérdida de disponibilidad o confidencialidad.

Pérdida de la disponibilidad.

Si un sistema de TI de misión crítica no está disponible para sus usuarios finales, la misión de la organización puede verse afectada. La pérdida de la funcionalidad del sistema y eficacia operativa, por ejemplo, puede resultar en la pérdida de tiempo productivo, por lo tanto obstaculizar el rendimiento de los usuarios finales de sus funciones en el apoyo a la misión de la organización.

Pérdida de confidencialidad.

La confidencialidad de los datos se refiere a la protección de los activos de la información contra la divulgación no autorizada. El impacto de la divulgación no autorizada de información confidencial puede ir desde la puesta en peligro de la seguridad nacional, problemas legales y de reputación por la ley de protección de datos, entre otros.

Paso 7. Determinación del Riesgo

En este punto se realiza la determinación del riesgo para una amenaza/vulnerabilidad particular, la misma que se puede expresar como una función de la probabilidad de intentar ejercer una vulnerabilidad dada sobre una amenaza determinada.

El análisis y estimación del riesgo, se dará considerando el siguiente criterio:

Riesgo (R) = Amenaza x Vulnerabilidad

De acuerdo a lo establecido en la escala de riesgo de la metodología NIST800-30. El riesgo se clasificará acorde a la siguiente escala:

Riesgo Muy Alto
Riesgo Alto
Riesgo Moderado
Riesgo Bajo
Riesgo Muy Bajo

En la Tabla 2-3 se encuentra definido gráficamente la clasificación de Riesgos.

Tabla 2-3: Clasificación de Riesgos

Amenaza \ Vulnerabilidad	Muy Alto	Alto	Moderado	Bajo	Muy Bajo
Muy Alto	Muy Alto	Alto	Moderado	Bajo	Muy Bajo
Alto	Muy Alto	Alto	Moderado	Bajo	Muy Bajo
Moderado	Alto	Moderado	Moderado	Bajo	Muy Bajo
Bajo	Moderado	Bajo	Bajo	Bajo	Muy Bajo
Muy Bajo	Bajo	Bajo	Muy Bajo	Muy Bajo	Muy Bajo

Fuente: Los Autores, acorde a lo establecido en la escala de riesgos de la Metodología NIST800-30.

Paso 8. Recomendación de Controles.

Durante este paso, se definen los controles que podrían mitigar o eliminar los riesgos identificados. El objetivo de los controles recomendados es reducir el nivel de riesgo para el sistema y sus datos. El control debe ser evaluado en función de los costos monetarios como operativos y por tanto la viabilidad de su implementación.

De acuerdo a la clasificación del Riesgo, se definirá un plan de acción y prioridad para su tratamiento, la matriz de prioridad está definida en la Tabla 2-4

Tabla 2-4: Matriz Prioridad de acuerdo a la clasificación del Riesgo.

MATRIZ DE PRIORIDAD DE ACUERDO A LA CLASIFICACION DEL RIESGO	
CLASIFICACION	**PRIORIDAD**
Riesgo Muy Alto	Requiere de atención inmediata y seguimiento del Comité de Riesgos y Comité de Seguridad
Riesgo Alto	Requiere de atención inmediata y seguimiento de la Gerencia de Riesgos y la Jefatura de Seguridad de la Información
Riesgo Moderado	Requiere de atención y seguimiento de Riesgo Operativo y la Jefatura de Seguridad de la Información
Riesgo Bajo	Requiere de atención y seguimiento de Riesgo Tecnológico y la Jefatura de Seguridad de la Información
Riesgo Muy Bajo	No se requiere atención inmediata, el proceso puede ser llevado por la Jefatura de Seguridad como un proceso de mejora

Fuente: Los Autores, acorde a lo establecido en la escala de riesgos de la Metodología NIST800-30.

Paso 9. Documentación de Resultados.

Una vez que la evaluación de riesgos se ha completado, los resultados deben ser documentados en un informe y comunicados en una reunión a la alta dirección.

Un informe de evaluación de riesgos es un informe de gestión que ayuda a la alta dirección, a los propietarios, a tomar decisiones sobre la política, procedimientos, el presupuesto, y evaluación de controles sugeridos.

2.1.2 RESULTADOS

REPORTE DE EVALUACION DE RIESGOS

El objetivo de realizar una evaluación de riesgo es definir qué es un riesgo, la magnitud (impacto) de los daños causados por la amenaza, las causas o eventos con el potencial de causar daños a la infraestructura tecnológica y a la información, y qué hacer ante el riesgo.

Para realizar esta evaluación se realizó las siguientes actividades para el levantamiento de información y diagnóstico:

1. Entrevistas
2. Evaluación de aplicativos y controles (listas de verificación)
3. Revisión de documentación de la empresa.
4. Levantamiento de Activos de Información, de acuerdo a las gerencias responsables.

A. Observación en prueba de recorrido

Considerando los servicios más importantes para la entidad financiera la evaluación abarco los siguientes procesos de negocio.

- Préstamos Hipotecarios (PH).
- Préstamos Quirografarios (PQ).
- Préstamos Prendarios (PP).

B. Caracterización del Sistema.

La caracterización del sistema se encuentra descrita en el capítulo I, para complementar la información se incluye los activos de información y su respectiva clasificación, cabe indicar que acorde a la clasificación se mantiene 4 tipos de información (pública, interna, confidencial y restringida).

Se estableció el alcance del ejercicio de evaluación del riesgo y proporciona información esencial con el propósito de garantizar la protección de datos y significa definir, dependiendo del tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso a la información y mecanismos de control de acceso a la misma, en la tabla 2-5 podemos apreciar el resumen de la clasificación de la información.

Tabla 2-5: Resumen de la clasificación de la Información de Préstamos Quirografarios, Préstamos Hipotecario y Préstamos Prendarios.

MACRO PROCESO	**PRÉSTAMOS**		
PROCESO	**PRÉSTAMO QUIROGRAFARIO**	**PRÉSTAMO HIPOTECARIO**	**PRÉSTAMO PRENDARIO**
ACTIVO DE INFORMACIÓN	Información de Cliente	Información de Cliente	Información de Cliente
	Información del Préstamo	Información del Préstamo	Información del Préstamo
DESCRIPCION	Datos relacionados a todo el proceso de solicitud, aprobación, instrumentación y desembolso	Datos relacionados a todo el proceso de solicitud, aprobación, instrumentación y desembolso	Datos relacionados a todo el proceso de solicitud, aprobación, instrumentación y desembolso
CLASIFICACION	Confidencial	Confidencial	Confidencial
CRITICIDAD	Alta	Alta	Alta
TITULAR DE INFORMACIÓN	Gerente de Crédito	Gerente de Crédito	Gerente de Crédito

Fuente: Los autores

C. Identificación de las Amenazas

Se identificó las potenciales amenazas que podrían explotar las vulnerabilidades del sistema y se categoriza acorde a la guía de la NIST 800-30.

Las amenazas se clasifican en:

i. Amenazas Naturales
ii. Amenazas Ambientales
iii. Amenazas Humanas
iv. Amenazas Técnicas
v. Amenazas Organizacionales

i. Amenazas Naturales

En la tabla 2-6 podemos apreciar las amenazas naturales y sus consecuencias en caso de presentarse el evento.

Tabla 2-6: Amenazas Naturales

FUENTE	ACCIONES
Movimientos Telúricos	Destrucción Infraestructura Daño al personal
Lluvias	Suspensión Energía Eléctrica Daños de Equipos por inundaciones Daños en documentación física
Erupción Volcánica	Destrucción Infraestructura e información Daños al personal
Tormenta Eléctrica	Suspensión Energía Eléctrica Suspensión de Telecomunicaciones

Fuente: Los autores.

ii. Amenazas Ambientales

En la tabla 2-7 podemos apreciar las amenazas ambientales y sus consecuencias en caso de presentarse el evento.

Tabla 2-7: Amenazas Ambientales

FUENTE	ACCIONES
Falta de Servicios Básicos (Luz, Agua)	Suspensión Energía Eléctrica Falta de Disponibilidad Servicios Des configuración de aplicación Falta en la integridad de la información
Contaminación	Daños de Equipos Problemas de salud al personal

Fuente: Los autores.

iii. Amenazas Humanas:

En la tabla 2-8 podemos apreciar las amenazas humanas y sus consecuencias en caso de presentarse el evento.

Tabla 2-8: Amenazas Humanas

FUENTE	ACCIONES
Salida del personal	Falta de capacitación del personal nuevo Suspensión o demoras en el servicio proporcionado
Fraudes Internos –Externos	Pérdida de dinero Pérdida de imagen Pérdida de Reputación Juicios para la institución – personal
Vandalismo	Daños de Equipos Pérdidas financieras
Hurto	Pérdidas financieras Pérdida de Información Juicios a la institución
Intrusiones (Hacker - Cracker)	Accesos no autorizados Pérdida de Integridad Pérdida de Información Pérdida de Disponibilidad
Empleados descontentos	Daños en los equipos Daños en la información Salida del personal
Negligencia	Destrucción de Equipos Falta de Servicios Perdida de información
Falta de Capacitación – Conocimiento	Daños en los equipos Daños en la información- Falta de Integridad Tiempos de respuesta altos No cumplimiento con los objetivos institucionales
Incumplimiento de Leyes	Multas / Sanciones Pérdida de Reputación
Falta de Pagos Servicios Básicos	Falta de servicios básicos Falta de disponibilidad de sistemas informáticos
Divulgación de Información Confidencial	Pérdidas financieras Juicios a la institución Pérdida de Reputación
Incumplimiento Políticas de Seguridad	Accesos no autorizados Pérdida de Integridad Pérdida de Información Pérdida de Disponibilidad

Fuente: Los autores

iv. Amenazas Técnicas:

En la tabla 2-9 podemos apreciar las amenazas técnicas y sus consecuencias en caso de presentarse el evento.

Tabla 2-9: Amenazas Técnicas

FUENTE	ACCIONES
Pérdida o Robo de Equipos	Accesos no autorizados Pérdida de Integridad Pérdida de Información Costos de Reposición
Infiltración sitio Web	Accesos no autorizados Pérdida de Integridad Pérdida de Información
Intervención de correos y llamadas	Accesos no autorizados Pérdida de Integridad Pérdida de Información Pérdida de Disponibilidad
Mal manejo de equipos y software	Daño en los equipos o aplicativos Pérdida de Integridad Pérdida de Información Pérdida de Disponibilidad
Falta de respaldos	Perdida de Disponibilidad Falta de servicio a los clientes internos y externos
Pérdida de contraseñas	Accesos no autorizados Pérdida de Integridad Pérdida de Información Pérdida de Disponibilidad
Accesos no autorizados	Accesos no autorizados Pérdida de Integridad Pérdida de Información Pérdida de Disponibilidad
Negación de servicios	Falta de operatividad del sistema - Pérdida de Disponibilidad
Falta de Licencias	Suspensión del servicio a nuevos usuarios - Pérdida de Disponibilidad Incumplimiento Leyes o Regulaciones Multas

Fuente: Los autores.

v. Amenazas Organizacionales:

En la tabla 2-10 podemos apreciar las amenazas organizacionales y sus consecuencias en caso de presentarse el evento.

Tabla 2-10: Amenazas Organizacionales

FUENTE	ACCIONES
Falta de procedimientos establecidos y normados	Deficiencias en los procesos Pérdida de integridad Pérdida de confidencialidad Actividades no autorizadas o falta de actividades
Falta de segregación de funciones	Pérdida de integridad Operaciones irregulares Fraudes

FUENTE	ACCIONES
Uso inadecuado de recursos	Falla o mal uso de los recursos Gastos innecesarios de recursos
Falta de monitoreo o control	Fraudes Perdida de integridad, disponibilidad y confidencialidad
Falta de estandarización en infraestructura	Problemas de instalación, configuración o ingreso de nuevos componentes en la infraestructura
Falta de continuidad en la alta gerencia	Falta de cumplimiento objetivos y culminación de proyectos en tiempos establecidos
Falta de plan de continuidad o contingencia	Falta de disponibilidad Corte de los servicios a los clientes Problemas Legales y de reputación

Fuente: Los autores.

D. Identificación de las Vulnerabilidades

Las vulnerabilidades detectadas en la evaluación de la institución financiera se clasificaron acorde al tipo de amenaza existente y los controles que actualmente existen dentro de la institución y son:

Amenazas Naturales vs Vulnerabilidades

En la tabla 2-11 se pueden apreciar las amenazas naturales, las vulnerabilidades y si existen controles en la actualidad.

Tabla 2-11: Amenazas Naturales vs Vulnerabilidades

AMENAZA	VULNERABILIDAD	CONTROLES ACTUALES
Movimientos Telúricos	No se han realizado planes de evacuación del edificio matriz desde la creación de la institución financiera.	No existen controles
Movimientos Telúricos	La institución financiera no cuenta con un plan de continuidad de negocio. El plan de contingencia no funciona adecuadamente en casos de contingencia real.	No existen controles
Erupciones Volcánicas	No se han realizado planes de evacuación del edificio matriz desde la creación de la institución financiera.	No existen controles
Erupciones Volcánicas	La institución financiera no cuenta con un plan de continuidad de negocio. El plan de contingencia no funciona adecuadamente en casos de contingencia real.	No existen controles
Tormentas Eléctricas	No se tiene contemplado respaldos para el sitio alterno que garantice recuperación de los sistemas. La información para procesamientos de Préstamos Quirografarios y Préstamos Hipotecarios reside en el sitio alterno por lo que no se puede garantizar la disponibilidad de los servicios proporcionados por terceros. El plan de contingencia no funcionó adecuadamente en casos reales de indisponibilidad del servicio.	Respaldos en Cinta

AMENAZA	VULNERABILIDAD	CONTROLES ACTUALES
Lluvias	No se realiza una adecuada validación de los lugares asignados para manejo de información, se evidencia pérdida de información de clientes por inundaciones en las bodegas de archivo.	Se adecuaron bodegas en sitio alterno.

Fuente: Los autores.

Amenazas Ambientales vs Vulnerabilidades

En la tabla 2-12 se pueden apreciar las amenazas ambientales, las vulnerabilidades y si existen controles en la actualidad.

Tabla 2-12: Amenazas Ambientales vs Vulnerabilidades

AMENAZA	VULNERABILIDAD	CONTROLES ACTUALES
Falta de Servicios Básicos (Luz, Agua)	No se tiene contemplado un plan en el cual se revise y garantice el pago de todos los servicios básicos que utiliza la institución financiera.	No existen controles
Contaminación	No se realiza una adecuada validación de los lugares en los que podría existir contaminación de distinta índole y que puedan afectar a la salud de las personas y normal funcionamiento de los quipos.	No existen controles.

Fuente: Los autores.

Amenazas Humanas vs Vulnerabilidades

En la tabla 2-13 se pueden apreciar las amenazas humanas, las vulnerabilidades y si existen controles en la actualidad.

Tabla 2-13: Amenazas Humanas vs Vulnerabilidades

AMENAZA	VULNERABILIDAD	CONTROLES ACTUALES
Divulgación de Información Confidencial	No se realiza seguimiento para el cumplimiento de clasificación de activos y la gestión de controles requeridos acorde a dicha clasificación.	No existen controles

AMENAZA	VULNERABILIDAD	CONTROLES
Divulgación de Información Confidencial	No se tiene un procedimiento establecido para etiquetado de la información acorde a la clasificación de la información. La política informa que en caso de no tener definida el tipo de información se considerará pública.	No existen controles
Divulgación de Información Confidencial	La institución financiera mantiene habilitado los puertos USB de un 90% de los equipos, el personal saca información en discos externo a discreción. La institución financiera no cuenta con un Servidor Compartido para traspaso de información.	No existen controles
Divulgación de Información Confidencial	No se cumple con el proceso de borrado de información de equipos en casos de salida del personal. Es frecuente encontrar información de otras áreas y de usuarios anteriores.	No existen controles
Divulgación de Información Confidencial	No existe control sobre la transferencia de información en medios magnéticos, existen equipos que pueden realizar copia de información en discos compactos (CD), disco digital versátil (DVD) u otros dispositivos de almacenamiento externo sin requerir la autorización de tecnología o seguridad	No existen controles
	No existen controles para la encriptación de información sensible, cuando esta se encuentra en tránsito. No existe control para evitar el reenvío de información de la institución financiera a cuentas personales.	
Divulgación de Información Confidencial	Existe compartición de claves por parte de los funcionarios.	No existen controles
	Existen varios aplicativos que no mantienen encriptado la clave en sus sistemas de almacenamiento. En el área de Tecnología existe la práctica de manejo de archivos comunes donde se guardan las claves de usuarios con privilegios de administración y que son usadas por el personal tecnológico a discreción del mismo.	
Divulgación de Información Confidencial	No existe una adecuada restricción de acceso para los aplicativos que se encuentran en la intranet de la institución financiera. No se manejan pistas de auditoría transaccionales en los aplicativos de la intranet.	No existen controles
Divulgación de Información Confidencial	La institución financiera no cuenta con un programa de puesto despejado, todas las áreas manejan información confidencial que se encuentra disponible a simple vista en formato físico o digital, existen gavetas sin seguridad. Se encuentra información en impresoras. Los equipos manejan políticas de bloqueo a los 5 minutos, sin embargo se evidencia equipos que no cumplen con dicha política.	No existen controles
Divulgación de Información Confidencial	Existen acuerdos de confidencialidad que no cuentan con la firma de la Gerencia General.	Acuerdos de Confidencialidad vigentes.

AMENAZA	VULNERABILIDAD	CONTROLES
Divulgación de Información Confidencial	El área de desarrollo accede a bases de datos de desarrollo que contienen información de producción, por lo que existe pérdida de confidencialidad de la información e incumplimiento a la normativa vigente.	No existen controles
Divulgación de Información Confidencial	No se realiza un proceso de enmascaramiento de la información confidencial que se utiliza en pruebas por parte de las áreas de desarrollo y QA.	Tecnología adquirió una herramienta para que se enmascare la data en desarrollo, pero aún no se encuentra operativo el proceso.
Divulgación de Información Confidencial	No existe un proceso de recopilación, seguimiento y custodia de evidencia de incidentes de seguridad. No existe proceso de mitigación de incidentes y cierre de vulnerabilidades encontradas.	No existen controles
Divulgación de Información Confidencial	Debido a la falta de implementación de controles y cultura de protección de datos, existe informalidad en el manejo, traslado y resguardo de la información de clientes y empleados internos. Se evidencia la distribución de la nómina de empleados con sueldos, puestos vacantes por la misma área de TTHH, sin que exista necesidad de ello. Acceso indiscriminado a aplicativos de la institución a pasantes y personal que no requiere dicha información, pero que cuentan con la autorización de la gerencia respectiva. Entrega de base de datos de producción para pruebas de proveedores las mismas que salen de las instalaciones de la institución financiera a ambientes controlados por el proveedor	Convenio de Confidencialidad
Empleados descontentos	No existe un proceso establecido para un manejo adecuado de altas y bajas en los distintos recursos administrados por las áreas, el área de Seguridad envía un correo solicitando eliminación de accesos sin embargo no se controla el cumplimiento del mismo y se evidencia accesos activos de personal que ha salido meses atrás.	Convenio de confidencialidad
Empleados descontentos	No se realiza el cambio de accesos o desactivación acorde a los tiempos establecidos para la salida o cambio de funciones de personal o de terceros en los distintos sistemas o recursos de la institución financiera.	Convenio de confidencialidad
Fraudes Internos –Externos	Dentro de las áreas de negocio y de soporte, existe acceso a manipulación de información que no está acorde a sus funciones debido a falta de segregación de funciones y ambientes.	Convenio de Confidencialidad
Fraudes Internos –Externos	Los administradores tecnológicos no mantienen un procedimiento para la asignación, modificación o eliminación de accesos.	No existen controles

AMENAZA	VULNERABILIDAD	CONTROLES
	El área de Seguridad no tiene control sobre los accesos administrador por otras áreas y no se realiza un control sobre los mismos.	
Fraudes Internos –Externos	No se realiza evaluaciones a las actividades realizadas por los usuarios en los distintos aplicativos de la institución financiera.	No existen controles
	Existen aplicativos que no guarda pistas de auditoría de las actividades realizada por los clientes de (Préstamos Quirografarios y Préstamos Hipotecarios)	
Fraudes Internos –Externos	En varios aplicativos el control de la administración de bases o plataformas es compartida con el proveedor por lo que no se garantiza el ingreso o cambio de registros de los sistemas.	No existen controles
Fraudes Internos –Externos	No se realiza evaluaciones a las actividades realizadas por usuarios privilegiados en los distintos aplicativos e infraestructura de la institución financiera.	No existen controles
Fraudes Internos –Externos	Al momento los aplicativos no cuentan con reportes de Auditoría que permitan la evaluación oportuna de los sistemas de la información por parte de las áreas de Seguridad de la Información y Auditoría Interna de la institución financiera.	Revisión de pistas de auditoría a nivel de aplicativo, en aquellos que al momento tienen implementado.
Fraudes Internos –Externos	Proveedores acceden a datos de producción con perfil del área de Tecnología de la institución financiera.	No existen controles
	Tecnología no se capacita sobre procesos realizados por el proveedor.	
Fraudes Internos –Externos	No existe respuesta oportuna a incidentes con el objeto de mitigar y evitar mayores riesgos.	No existen controles
Hurto	No existe un área definida para carga y despacho; todo proceso se realiza por la misma puerta de ingreso principal de la institución financiera y en otros casos ingresan por el parqueadero	No existen controles
Hurto	Se evidencia equipos que no cuentan con candados para evitar pérdida de los mismos. Existen equipos que no son de propiedad de la institución financiera ingresando a la red de la institución.	Existen cámaras de video instaladas en las oficinas de la institución financiera.
Hurto	El personal no mantiene normas de seguridad sobre los equipos asignados, se evidencia computadores desatendidos en oficinas o salas de reunión que no cuentan con candados o bloqueo de la sesión activa.	Existen cámaras de video instaladas en las oficinas de la institución financiera.
Incumplimiento Políticas de Seguridad	Al momento se tiene un Comité de Riesgos que asume las actividades de un Comité de Seguridad.	Norma JB-2014-3066establece tener un Comité de Seguridad en la entidad bancaria

AMENAZA	VULNERABILIDAD	CONTROLES
Incumplimiento de Leyes	No existe normativa, ni procedimientos que aseguren el cumplimiento de requisitos legales, reglamentarios y contractuales para derecho de propiedad intelectual.	No existen controles
Incumplimiento Políticas de Seguridad	El personal de Tecnología ingresa mediante VPN a servidores de la institución financiera para procesos de soporte, incumpliendo la política de Seguridad de la institución financiera.	No existen controles
Incumplimiento Políticas de Seguridad	Los contratos del personal suelen regularizarse después que el funcionario se encuentra laborando en la institución.	No existen controles
Incumplimiento Políticas de Seguridad	No existe control sobre el proceso de entrega de información y uso adecuado del mismo por parte de un tercero.	Acuerdo de Confidencialidad
Incumplimiento Políticas de Seguridad	No existe un proceso formal para evaluación de los proveedores y los controles de seguridad implementados para resguardar la información de la institución financiera. No se cumple las sanciones definidas a nivel contractual en caso de incumplimiento por parte del proveedor.	Contrato con los proveedores
Incumplimiento Políticas de Seguridad	No existen procesos de control y evaluación de Riesgo con los proveedores. La institución financiera incumple fechas de pago a los proveedores.	Contrato con los proveedores
Incumplimiento de Leyes	No existe el soporte adecuado del área Legal en los procesos de creación y evaluación de requerimientos funcionales.	No existen controles
Incumplimiento Políticas de Seguridad	No existe un proceso de revisión periódica de la Política de Seguridad de la Información.	No existen controles
Incumplimiento Políticas de Seguridad	No existe una exigencia de la dirección para colaboradores, contratistas y terceras partes, sobre uso adecuado de los recursos de la institución financiera y acorde a las políticas de seguridad de la institución.	No existen controles
Incumplimiento Políticas de Seguridad	El procedimiento de manejo de cambios no es integral y no cumplen los controles de seguridad solicitados por la Jefatura de Seguridad de la Información.	No existen controles
Incumplimiento Políticas de Seguridad	No existe un plan de implementación de un SGSI, por lo que no se realiza un proceso de evaluación de nivel de cumplimiento e implementación de normas de seguridad.	No existen controles
Intrusiones (Hacker - Cracker)	No se realiza evaluaciones independientes del proceso de implementación y control definido por la Jefatura de Seguridad de la Información a través de un proceso anual de hacker ético a la infraestructura tecnológica.	No existen controles
Incumplimiento Políticas de Seguridad	No existe una metodología que garantice la evaluación de seguridad en los proyectos que salen a producción o de aquellos que cambian debido a nuevos requerimientos.	No existen controles
Incumplimiento Políticas de Seguridad	No se tiene normativa sobre los estándares de controles criptográficos permitidos en la Institución.	No existen controles
Intrusiones (Hacker - Cracker)	No existe un proceso de aprendizaje y evaluación para generación de causas raíz de los incidentes de seguridad.	No existen controles

Fuente: Los autores.

Amenazas Organizacionales vs Vulnerabilidades

En la tabla 2-14 se muestran las amenazas organizacionales, las vulnerabilidades y si existen controles en la actualidad.

Tabla 2-14: Amenazas Organizacionales vs Vulnerabilidades

AMENAZA	VULNERABILIDAD	CONTROLES ACTUALES
Falta de continuidad en la alta gerencia	No se cumplan acuerdos pactados y no existe continuidad en los proyectos.	No existen controles
Falta de contraparte del área de Seguridad	No existe un acuerdo de seguridad entre el proveedor y la Institución Financiera, en el que se especifique los requisitos de seguridad en el acceso, procesamiento, comunicación, gestión de la información, de los servicios de procesamiento, incorporación de nueva funcionalidad, nuevos productos o servicios.	No existen controles
Falta de estandarización en infraestructura	No existe una regulación del manejo de controles criptográficos y evaluación de los mismos.	No existen controles
Falta de plan de continuidad o contingencia	No se tiene identificado los procesos críticos de la institución. El plan de contingencia existente es únicamente documental.	No existen controles
Falta de plan de continuidad o contingencia	No existe un proceso de seguimiento y control para realizar la implementación de un plan de continuidad de negocio.	No existen controles
Falta de procedimientos establecidos y normados.	No existe un plan de implementación y cumplimiento de las políticas y reglamentos de Seguridad de la Información.	Al momento está para proceso de aprobación un manual de seguridad que establece lineamientos para el cumplimiento de las áreas, procesos de control y de sanción en caso de ser necesario.
Falta de procedimientos establecidos y normados	Existen pasos a producción que no son validados por el área de Seguridad o que a su vez fueron realizados con Seguridad y que en el transcurso del proceso fueron cambiados por terceros.	No existen controles
Falta de procedimientos establecidos y normados	No se realiza un proceso de evaluación y clasificación de incidentes, al momento se realiza reporte mensual de los temas que el área de Seguridad tuvo conocimiento en el mes y se informa en el Comité de Riesgos (CAIR), sin embargo no se realiza un seguimiento adecuado y cierre de los incidentes encontrados.	No existen controles
Falta de procedimientos establecidos y normados	La institución financiera no cuenta con un inventario actualizado y completo de los activos de información y sus responsables.	No existen controles
Falta de procedimientos establecidos y normados	No existe información actualizada de titulares de la información y sus delegados.	No existen controles
Falta de procedimientos establecidos y normados	No existe un inventario de recursos y de administradores.	No existen controles
Falta de procedimientos establecidos y normados	No existe un proceso de control cruzado sobre perfiles y procesos.	No existen controles
Falta de procedimientos establecidos y normados	No se encuentran establecidas y definidas las áreas restringidas.	No existen controles
Falta de procedimientos establecidos y normados	El control de acceso al edificio no siempre registra las visitas y no hay una bitácora de ingreso y salida de equipos.	No existen controles
Falta de procedimientos establecidos y normados	No está definido procesos de control y evolución de riesgos.	No existen controles
Falta de procedimientos establecidos y normados	El área de Tecnología no cuenta al momento con procedimientos aprobados sobre su operatividad.	No existen controles

AMENAZA	VULNERABILIDAD	CONTROLES
Falta de procedimientos establecidos y normados	No existen procedimientos establecidos para intercambio de información con proveedores eventuales o permanentes.	No existen controles
Falta de procedimientos establecidos y normados.	No se realiza control sobre la información que se entrega por medios físicos o magnéticos e incluso en declaraciones en la prensa.	No existen controles
Falta de procedimientos establecidos y normados	No existe control sobre las actividades de los Administradores de Red quienes tienen acceso total a al Directorio Activo, Correo Electrónico y manejo de Internet.	No existen controles
Falta de procedimientos establecidos y normados	No se realiza revisión técnica luego de efectuar cambios en el Sistema Operativo.	No existen controles
Falta de procedimientos establecidos y normados	No se maneja un proceso definido para versionamiento de los aplicativos y no existe control adecuado y resguardo de los mismos.	No existen controles
Falta de procedimientos establecidos y normados	No se incluye ningún proceso específico para la protección de los sistemas.	No existen controles
Falta de procedimientos establecidos y normados	No existen procesos de control y evaluación de Riesgo con los proveedores.	No existen controles
Falta de procedimientos establecidos y normados	No existe un proceso establecido de control y evaluación de proveedores.	No existen controles
Falta de procedimientos establecidos y normados	No existe un procedimiento establecido para manejo de incidentes de seguridad de la información.	No existen controles
Falta de segregación de funciones	Se verifica que existe falta de segregación de funciones en los procesos operativos y tecnológicos de la institución financiera.	No existen controles
Uso inadecuado de recursos	No existe un control o procesos establecidos por los administradores de todas las áreas para revisión de perfiles y derechos de acceso a los aplicativos.	No existen controles
Falta de procedimientos establecidos y normados	No se realiza un proceso de evaluación y clasificación de incidentes, al momento se realiza reporte mensual de los temas que el área de Seguridad tuvo conocimiento en el mes y se informa en el Comité de Riesgos (CAIR), sin embargo no se realiza un seguimiento adecuado y cierre de los incidentes encontrados.	No existen controles
Falta de estandarización en infraestructura	No se encuentra garantizada la conexión de todos los equipos a UPS.	No existen controles
Falta de estandarización en infraestructura	No existe estándares de cableado y elementos de comunicación. No existe coordinación con las áreas de infraestructuras para realizar compras e instalación.	No existen controles
Falta de estandarización en infraestructura	No existe una política de actualización de equipos de forma masiva, por lo que no se garantiza el cierre de vulnerabilidades.	No existen controles
Falta de estandarización en infraestructura	No existe un adecuado proceso de actualización de versiones y sincronización de relojes en las máquinas de registro de ingreso. No se encuentra normado la hora que debe tomar para registros de pistas de auditorías, en algunos casos toma el del servidor de aplicativo y otros del servidor de base de datos)	No existen controles

AMENAZA	VULNERABILIDAD	CONTROLES
Falta de estandarización en infraestructura	No existe separación de redes, no se tienen separados usuarios, ni servicios. Manejan una red plana, no se tiene controles de enrutamiento discriminando el trafico confidencial	No existen controles
Falta de monitoreo o control	No se maneja un proceso de gestión de vulnerabilidades integral, no se verifica el cumplimiento en todos los equipos de la institución financiera.	No existen controles
Falta de monitoreo o control	No existe un proceso para manejo de incidentes, seguimiento y cierre de los mismos, así como la definición de controles que eviten que estos incidentes vuelvan a ocurrir.	No existen controles
Falta de monitoreo o control	No se tiene cultura para notificación de incidentes de seguridad tanto de usuarios internos, clientes o proveedores.	No existen controles
Falta de procedimientos establecidos y normados	No existen procedimientos formales para cumplir un ciclo de desarrollo del software, con estándares y metodologías.	No existen controles
Uso inadecuado de recursos	No existen procesos de control de instalación de SW en servidores y equipos por parte de proveedores.	No existen controles

Fuente: Los Autores.

Amenazas Técnicas vs Vulnerabilidades

En la tabla 2-15 se aprecian las amenazas técnicas, las vulnerabilidades y si existen controles en la actualidad.

Tabla 2-15: Amenazas Técnicas vs Vulnerabilidades

AMENAZA	VULNERABILIDAD	CONTROLES ACTUALES
Accesos no autorizados	No se tiene una herramienta de administración de accesos a los aplicativos de la intranet.	No existen controles
Accesos no autorizados	No se maneja un proceso adecuado de versionamiento.	No existen controles
Accesos no autorizados	No se realiza control específico en áreas como Cumplimiento, Tecnología y en el Data Center local se evidencia ingreso de personal sin que esto sea registrado en las bitácoras definidas como parte del procedimiento.	No existen controles
Accesos no autorizados	El área tecnológica no cuenta con entornos definidos para desarrollo, pruebas y producción para todos los aplicativos de la institución financiera.	No existen controles
Accesos no autorizados	No se encuentra delimitado las funciones del área de soporte y del área de Redes, por lo que no existen registros actualizados ni responsables del manejo y e identificación de IP fija, en los casos definidos.	No existen controles

AMENAZA	VULNERABILIDAD	CONTROLES ACTUALES
Accesos no autorizados	No existen reglas de expiración de claves que se utilizan para conexión vía VPN. No se realiza restricción de puertos físicos o control de los mismos.	No existen controles
Falta de Licencias	Existe falta de monitoreo y evaluación adecuada de capacidades en infraestructura actual o cambios a realizarse.	No existen controles
Falta de Licencias	No existe un proceso de escaneo periódico para evaluar que tienen los aplicativos, así como se instala software de Sistema Operativo y otros aplicativos específicos sin licencia.	No existen controles
Intervención de correos y llamadas	No se cuenta con un Servidor de Archivos, por lo cual los usuarios envían información confidencial por correo.	No existen controles
Mal manejo de equipos y software	No se realiza un control y unificación de controles criptográficos de los distintos aplicativos usados en la institución.	No existen controles
Mal manejo de equipos y software	No se maneja un plan de mantenimiento de equipos, se realiza cambios sólo en casos que el personal solicite cambio del mismo.	No existen controles
Mal manejo de equipos y software	No existe total cumplimiento del procedimiento establecido para reutilizar equipos, es común ver información de otros usuarios anteriores del equipo.	No existen controles
Negación de servicios	No se evidencia pruebas periódicas de procesos de restauración de respaldos de BDD que evidencien que los respaldos se encuentran generados correctamente. No se maneja una copia de respaldos en el sitio alterno que sea utilizada en casos de contingencia.	No existen controles
Negación de servicios	No se realizan los pagos de contratos con proveedores a tiempo lo que conlleva a que no se de servicios por parte del proveedor y falta de disponibilidad de soporte técnico. No existe un proceso de gestión de cambios en los servicios prestados por terceros.	No existen controles
Pérdida de contraseñas	No existe una política establecida para uso, protección y duración de las claves criptográficas, así como falta de registro y archivo de las claves que maneja la institución en los distintos aplicativos.	No existen controles
Pérdida o Robo de Equipos	No se cuenta con una seguridad física acorde a la información que manejan, no se realiza cierre de oficinas, archivadores sin llave.	No existen controles
Mal manejo de equipos y software	No existe control sobre los procesos de administración de usuarios, administradores tecnológicos y administradores de equipos de usuario, así como procesos que son administrados por proveedores. No existe un proceso establecido para la administración y control de cuentas genéricas y que en su gran mayoría maneja privilegios especiales.	No existen controles
Pérdida de contraseñas	No se cumple con la política de contraseñas y entrega segura de claves en los sistemas administrados por el área de Tecnología.	No existen controles
Pérdida de contraseñas	No existe un proceso formal para la entrega de claves a los usuarios por parte de los administradores. No se ha establecido un id único por funcionario para todos los aplicativos y sistemas de la institución financiera.	No existen controles

AMENAZA	VULNERABILIDAD	CONTROLES ACTUALES
Pérdida o Robo de Equipos	No existen procedimientos establecidos de control de salida e ingreso de equipos. El 50% de equipos portátiles no cuenta con encriptación de disco.	No existen controles
Pérdida o Robo de Equipos	No existe un inventario actualizado de activos. No se cumple el proceso de devolución de activos previo a la salida del personal.	No existen controles
Mal manejo de equipos y software	No existe control sobre los procesos de administración de usuarios, administradores tecnológicos y administradores de equipos de usuario, así como procesos que son administrados por proveedores. No existe un proceso establecido para la administración y control de cuentas genéricas y que en su gran mayoría maneja privilegios especiales.	No existen controles
Pérdida de contraseñas	No se cumple con la política de contraseñas y entrega segura de claves en los sistemas administrados por el área de Tecnología.	No existen controles
Pérdida de contraseñas	No existe un proceso formal para la entrega de claves a los usuarios por parte de los administradores. No se ha establecido un id único por funcionario para todos los aplicativos y sistemas de la institución financiera.	No existen controles
Pérdida o Robo de Equipos	No existen procedimientos establecidos de control de salida e ingreso de equipos. El 50% de equipos portátiles no cuenta con encriptación de disco.	No existen controles
Pérdida o Robo de Equipos	No existe un inventario actualizado de activos. No se cumple el proceso de devolución de activos previo a la salida del personal.	No existen controles

Fuente: Los Autores.

E. Análisis de los controles

Los controles definidos son las acciones o procesos que se utiliza para mitigar el riesgo, los controles que mantiene la entidad bancaria no cumplen adecuadamente su propósito por lo que el nivel de riesgo se mantiene y se han detallado para un tema documental pero se consideran ineficientes para el propósito de disminuir el riesgo inherente detallado en este trabajo. (Véase H. Amenazas vs Vulnerabilidades)

F. *Determinación de la Probabilidad*

(Véase H. Medición del Riesgo)

G. Análisis del Impacto

(Véase H. Medición del Riesgo)

H. Medición del Riesgo

En esta etapa se levantó una matriz de riesgos en la que se incluye un campo llamado "**Identificador del Riesgo**" con el propósito de nominar de manera única los hallazgos encontrados; el mismo que está compuesto por la letra "R" y un número secuencial, ver Anexo 2-B.

Evaluación del Riesgo vs Amenazas Naturales

En la tabla 2-16 se muestra la evaluación del riesgo vs amenazas naturales.

Tabla 2-16: Evaluación del Riesgo vs Amenazas Naturales

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R45	Movimientos Telúricos	No se han realizado planes de evacuación del edificio matriz desde la creación de la institución financiera.	Moderado	Alto	Moderado
R103	Movimientos Telúricos	La institución financiera no cuenta con un plan de continuidad de negocio. El plan de contingencia no funciona adecuadamente en casos de contingencia real.	Moderado	Muy Alto	Moderado
R115	Erupción Volcánica	No se han realizado planes de evacuación del edificio matriz desde la creación de la institución financiera.	Moderado	Alto	Moderado
R116	Erupción Volcánica	La institución financiera no cuenta con un plan de continuidad de negocio. El plan de contingencia no funciona adecuadamente en casos de contingencia real.	Moderado	Alto	Moderado
R106	Tormenta Eléctrica	No se tiene contemplado respaldos para el sitio alterno que garantice recuperación de los sistemas. La información para procesamientos de Préstamos Quirografarios y Préstamos Hipotecarios reside en el proveedor por lo que no se puede garantizar la disponibilidad de los servicios proporcionados por terceros. El plan de contingencia no	Bajo	Alto	Bajo

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
		funciono adecuadamente en casos reales de indisponibilidad de servicio.			
R109	Lluvias	No se realiza una adecuada validación de los lugares asignados para manejo de información, se evidencia pérdida de información de clientes por inundaciones en las bodegas de archivo	Muy Alto	Muy Alto	Muy Alto

Fuente: Los Autores.

Evaluación del Riesgo vs Amenazas Ambientales

En la tabla 2-17 se muestra la evaluación del riesgo vs amenazas ambientales

Tabla 2-17: Evaluación del Riesgo vs Amenazas Ambientales

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO de la VULNERABILIDAD	RIESGO
R130	Falta de Servicios Básicos (Luz, Agua)	No se tiene contemplado un plan en el cual se revise y garantice el pago de todos los servicios básicos que utiliza la institución financiera.	Bajo	Alto	Bajo
R131	Contaminación	No se realiza una adecuada validación de los lugares en los que podría existir contaminación de distinta índole y que puedan afectar a la salud de las personas y normal funcionamiento de los quipos.	Baja	Muy Alto	Moderado

Fuente: Los Autores.

Valoración del Riesgo x Amenazas Humanas

En la tabla 2-18 se muestra la evaluación del riesgo vs amenazas humanas

Tabla 2-18: Evaluación del Riesgo vs Amenazas Humanas

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R20	Divulgación de Información Confidencial	No se realiza seguimiento para el cumplimiento de clasificación de activos y la gestión de controles requeridos acorde a dicha clasificación.	Muy Alto	Muy Alto	Muy Alto
R21	Divulgación de Información Confidencial	No se tiene un procedimiento establecido para etiquetado de la información acorde a la clasificación de la información. La política informa que en caso de no tener definida el tipo de información se considerará pública	Muy Alto	Muy Alto	Muy Alto
R23	Divulgación de Información Confidencial	La institución financiera mantiene habilitado los puertos USB (universal serie bus) de un 90% de los equipos, el personal saca información en discos externo a discreción. La institución financiera no cuenta con un Servidor Compartido para traspaso de información	Muy Alto	Muy Alto	Muy Alto
R24	Divulgación de Información Confidencial	No se cumple con el proceso de borrado de información de equipos en casos de salida del personal. Es frecuente encontrar información de otras áreas y de usuarios anteriores.	Muy Alto	Alto	Alto
R25	Divulgación de Información Confidencial	No existe control sobre la transferencia de información en medios magnéticos, existen equipos que pueden realizar copia de información en CD, DVD, dispositivo externo de almacenamiento sin requerir la autorización de tecnología o seguridad No existen controles para la encriptación de información sensible, cuando esta se encuentra en tránsito. No existe control para evitar el reenvío de información de la institución financiera a cuentas personales.	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R34	Divulgación de Información Confidencial	Existe compartición de claves por parte de los funcionarios. Existen varios aplicativos que no mantienen encriptado la clave en sus sistemas de almacenamiento. En el área de Tecnología existe la práctica de manejo de archivos comunes donde se guardan las claves de usuarios con privilegios de administración y que son usadas por el personal tecnológico a discreción del mismo.	Muy Alto	Muy Alto	Muy Alto
R35	Divulgación de Información Confidencial	No existe una adecuada restricción de acceso para los aplicativos que se encuentran en la intranet de la institución financiera. No se manejan pistas de auditoría transaccionales en los aplicativos de la intranet.	Muy Alto	Muy Alto	Muy Alto
R56	Divulgación de Información Confidencial	La institución financiera no cuenta con un programa de puesto despejado, todas las áreas manejan información confidencial que se encuentra disponible a simple vista en formato físico o digital, existen gavetas sin seguridad. Se encuentra información en impresoras. Los equipos manejan políticas de bloqueo a los 5 minutos, sin embargo se evidencia equipos que no cumplen con dicha política.	Muy Alto	Muy Alto	Muy Alto
R77	Divulgación de Información Confidencial	Existen acuerdos de confidencialidad que no cuentan con la firma de la Gerencia General.	Muy Alto	Muy Alto	Muy Alto
R86	Divulgación de Información Confidencial	El área de desarrollo accede a bases de datos de desarrollo que contienen información de producción, por lo que existe pérdida de confidencialidad de la información e incumplimiento a la normativa vigente.	Muy Alto	Muy Alto	Muy Alto
R90	Divulgación de Información Confidencial	No se realiza un proceso de enmascaramiento de la información confidencial que se utiliza en pruebas por parte de las áreas de desarrollo y QA.	Muy Alto	Muy Alto	Muy Alto
R102	Divulgación de Información Confidencial	No existe un proceso de recopilación, seguimiento y custodia de evidencia de incidentes de seguridad. No existe proceso de mitigación de incidentes y cierre de vulnerabilidades encontradas	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R110	Divulgación de Información Confidencial	Debido a la falta de implementación de controles y cultura de protección de datos, existe informalidad en el manejo, traslado y resguardo de la información de clientes y empleados internos. Se evidencia la distribución de la nómina de empleados con sueldos, puestos vacantes por la misma área de TTHH, sin que exista necesidad de ello. Acceso indiscriminado a aplicativos de la institución financiera a pasantes y personal que no requiere dicha información, pero que cuentan con la autorización de la gerencia respectiva. Entrega de base de datos de producción para pruebas de proveedores las mismas que salen de las instalaciones de la institución financiera a ambientes controlados por el proveedor	Muy Alto	Muy Alto	Muy Alto
R28	Empleados descontentos	No existe un proceso establecido para un manejo adecuado de altas y bajas en los distintos recursos administrados por las áreas, el área de Seguridad envía un correo solicitando eliminación de accesos sin embargo no se controla el cumplimiento del mismo y se evidencia accesos activos de personal que ha salido meses atrás.	Muy Alto	Muy Alto	Muy Alto
R33	Empleados descontentos	No se realiza el cambio de accesos o desactivación acorde a los tiempos establecidos para la salida o cambio de funciones de personal o de terceros en los distintos sistemas o recursos de la institución financiera.	Muy Alto	Muy Alto	Muy Alto
R22	Fraudes Internos – Externos	Dentro de las áreas de negocio y de soporte, existe acceso a manipulación de información que no está acorde a sus funciones debido a falta de segregación de funciones y ambientes.	Muy Alto	Muy Alto	Muy Alto
R29	Fraudes Internos – Externos	Los administradores de usuarios y recursos no mantienen un procedimiento para un manejo adecuado de la asignación, modificación o eliminación los distintos recursos administrados por otras áreas de la institución financiera o proveedores, el área de Seguridad no tiene control sobre los accesos administrador por otras áreas y no se realiza un	Muy Alto	Alto	Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
		control sobre los mismos.			
R63	Fraudes Internos – Externos	No se realiza evaluaciones a los registros o eventos sobre procesos de usuarios en los distintos aplicativos e infraestructura de la institución financiera; existen aplicativos que no guarda pistas de auditoria transaccionales de las actividades realizada por los clientes (de Préstamos Quirografarios y Préstamos Hipotecarios, Administración usuarios de Préstamos Quirografarios y Préstamos Hipotecarios)	Muy Alto	Muy Alto	Muy Alto
R64	Fraudes Internos – Externos	En varios aplicativos el control de la administración de bases o plataformas es compartida con el proveedor por lo que no se garantiza el ingreso o cambio de registros de los sistemas.	Muy Alto	Muy Alto	Muy Alto
R65	Fraudes Internos – Externos	No se realiza evaluaciones a los registros o eventos sobre procesos de usuarios privilegiados (Administradores de Usuario o Administradores Tecnológicos o Administrador de base de datos) en los distintos aplicativos e infraestructura de la institución financiera.	Muy Alto	Muy Alto	Muy Alto
R70	Fraudes Internos – Externos	Al momento los aplicativos no cuentan con reportes de Auditoría que permitan la evaluación oportuna de los sistemas de la información por parte de las áreas de Seguridad de la Información y Auditoría Interna de la institución financiera.	Muy Alto	Alto	Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R87	Fraudes Internos – Externos	En varios aplicativos de negocio el proveedor es quién realiza el desarrollo y modificación de aplicativo, con lo cual se evidencia que desarrolladores externos acceden a datos de producción y tienen control de los procesos a nivel de pruebas e inclusive en bases de producción. EL área de desarrollo no toma control y conocimiento sobre procesos realizados y en caso de necesitar cambios se envía requerimientos al proveedor con costo para la institución financiera. Exista una rotación de personal media alta en el área de desarrollo por lo que no existe continuidad sobre el conocimiento requerido y desarrollos quedan incompletos.	Muy Alto	Muy Alto	Muy Alto
R100	Fraudes Internos – Externos	No existe respuesta oportuna a incidentes con el objeto de mitigar y evitar mayores riesgos.	Muy Alto	Muy Alto	Muy Alto
R47	Hurto	No existe un área definida para carga y despacho todo proceso se realiza por la misma puerta de ingreso principal de la institución financiera y en otros casos ingresan por el parqueadero	Muy Alto	Muy Alto	Muy Alto
R48	Hurto	Se evidencia equipos que no cuentan con candados para evitar pérdida de los mismos. Existen equipos que no son de propiedad de la institución financiera ingresando a la red de la institución.	Muy Alto	Alto	Alto
R55	Hurto	El personal no mantiene normas de seguridad sobre los equipos asignados, se evidencia computadores desatendidos en oficinas o salas de reunión que no cuentan con candados o bloqueo de la sesión activa.	Modera	Muy Alto	Moderado
R108	Incumplimiento de Leyes	No existe normativa, ni procedimientos que aseguren el cumplimiento de requisitos legales, reglamentarios y contractuales.	Modera	Muy Alto	Moderado
R3	Incumplimiento Políticas de Seguridad	Al momento se tiene un Comité de Riesgos que asume las actividades de un Comité de Seguridad, no existe apoyo para que se cumpla la implementación de un SGSI y manejo adecuado de incidentes de seguridad.	Muy Alto	Alto	Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R9	Incumplimiento Políticas de Seguridad	El personal de Tecnología ingresa mediante VPN a servidores de la institución financiera para procesos de soporte, sin embargo la política de Seguridad dice que no se debe realizar soporte remoto.	Muy Alto	Muy Alto	Muy Alto
R12	Incumplimiento Políticas de Seguridad	Se incluye dentro del contrato que debe cumplir con la Política de Seguridad de la Información sin embargo los contratos suelen regularizarse previo ya a la salida del personal o al menos con una diferencia de 3 a 6 meses desde que el servidor empezó a laborar.	Muy Alto	Muy Alto	Muy Alto
R14	Incumplimiento Políticas de Seguridad	No existen procesos disciplinarios establecidos para incumplimiento a la política de Seguridad de la Información, existen casos identificados sin que se realice sanciones a pesar de la gravedad de los mismos.	Muy Alto	Muy Alto	Muy Alto
R75	Incumplimiento Políticas de Seguridad	Se maneja acuerdos de intercambio de información con varios proveedores, sin embargo no existe un proceso formal para entrega de información y uso adecuado del mismo.	Muy Alto	Muy Alto	Muy Alto
R91	Incumplimiento Políticas de Seguridad	No existe un proceso formal establecido para evaluación de proveedores y sobre el uso que este da a la información, no se ha definido una lista de proveedores críticos, por lo que no se realiza un proceso de evaluación del servicio prestado y su cumplimiento. En incidentes ocurridos por los servicios prestados no se aplican las sanciones definidas a nivel contractual.	Muy Alto	Muy Alto	Muy Alto
R93	Incumplimiento Políticas de Seguridad	No existe procesos de control y evaluación de Riesgo con los proveedores, los niveles de escalamiento o servicio no se cumplen en su totalidad.	Muy Alto	Muy Alto	Muy Alto
R10	Negligencia	Las carpetas de empleados no cuentan con toda la documentación solicitada en la lista de documentos establecidos para el ingreso, así como el perfil de la persona no está acorde a las necesidades del puesto.	Muy Alto	Alto	Alto
R11	Negligencia	Existe personal laborando sin un contrato formal que proteja al empleado o a la institución financiera.	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R13	Negligencia	No existe un proceso de inducción sobre Seguridad de la Información.	Muy Alto	Muy Alto	Muy Alto
R15	Negligencia	El área de TTHH no informa oportunamente de la salida o cambios de funciones del personal.	Muy Alto	Muy Alto	Muy Alto
R36	Negligencia	No se cumple con la asignación de claves en el Directorio Activo acorde al instructivo de Tecnología. En los otros sistemas administrados por Tecnología no existen procedimientos establecidos.	Muy Alto	Muy Alto	Muy Alto
R88	Negligencia	Existen proyectos que pasan a producción sin la aprobación y evaluación del área de negocio.	Muy Alto	Muy Alto	Muy Alto
R89	Negligencia	No existe un proceso formal de paso a producción que abarque la evaluación funcional, controles requeridos y autorizaciones necesarias.	Muy Alto	Muy Alto	Muy Alto
R78	Incumplimiento Políticas de Seguridad	No existe una metodología que garantice la evaluación de seguridad en los proyectos que salen a producción o de aquellos que cambian debido a nuevos requerimientos	Moderado	Alto	Medio
R107	Incumplimiento de Leyes	No existe el soporte adecuado del área Legal en los procesos de creación y evaluación de requerimientos funcionales	Modera	Muy Alto	Moderado
R2	Incumplimiento Políticas de Seguridad	No existe un proceso de revisión periódica de la Política de Seguridad de la Información	Muy Alto	Moderado	Moderado
R18	Incumplimiento Políticas de Seguridad	No existe una exigencia de la dirección para colaboradores, contratistas y terceras partes, sobre uso adecuado de los recursos de la institución financiera y acorde a las políticas de seguridad de la institución	Muy Alto	Muy Alto	Muy Alto
R58	Incumplimiento Políticas de Seguridad	El procedimiento de manejo de cambios no es integral y no cumplen los controles de seguridad solicitados por la Jefatura de Seguridad de la Información	Muy Alto	Muy Alto	Muy Alto
R113	Incumplimiento Políticas de Seguridad	No existe un plan de implementación de un SGSI, por lo que no se realiza un proceso de evaluación de nivel de cumplimiento e implementación de normas de seguridad	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R112	Intrusiones (Hacker - Cracker)	No se realiza evaluaciones independientes del proceso de implementación y control definido por la Jefatura de Seguridad de la Información a través de un proceso anual de hacker ético a la infraestructura tecnológica.	Muy Alto	Muy Alto	Muy Alto
R101	Intrusiones (Hacker - Cracker)	No existe un proceso de aprendizaje y evaluación para generación de causas raíz de los incidentes de seguridad	Muy Alto	Muy Alto	Muy Alto

Fuente: Los Autores.

Valoración del Riesgo x Amenaza Organizacionales

En la tabla 2-19 se muestra la evaluación del riesgo vs amenazas organizacionales

Tabla 2-19: Evaluación del Riesgo vs Amenazas Organizacionales

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R5	Falta de continuidad en la alta gerencia	No se cumplan acuerdos pactados y no existe continuidad en los proyectos.	Moderado	Alto	Medio
R6	Falta de contraparte del área de Seguridad	No existe un acuerdo de seguridad entre el proveedor y la Institución Financiera, en el que se especifique los requisitos de seguridad en el acceso, procesamiento, comunicación, gestión de la información, de los servicios de procesamiento, incorporación de nueva funcionalidad, nuevos productos o servicios	Muy Alto	Muy Alto	Muy Alto
R111	Falta de estandarización en infraestructura	No existe una regulación del manejo de controles criptográficos y evaluación de los mismos.	Muy Alto	Muy Alto	Muy Alto
R104	Falta de plan de continuidad o contingencia	No se tiene identificado los procesos críticos de la institución. El plan de contingencia existente es únicamente documental.	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R105	Falta de plan de continuidad o contingencia	No existe un proceso de seguimiento y control para realizar la implementación de un plan de continuidad de negocio.	Muy Alto	Muy Alto	Muy Alto
R1	Falta de procedimientos establecidos y normados	No existe un plan de implementación y cumplimiento de las políticas y reglamentos de Seguridad de la Información	Muy Alto	Muy Alto	Muy Alto
R7	Falta de procedimientos establecidos y normados	Existen pasos a producción que no son validados por el área de Seguridad o que a su vez fueron realizados con Seguridad y que en el transcurso del proceso fueron cambiados por terceros.	Muy Alto	Muy Alto	Muy Alto
R16	Falta de procedimientos establecidos y normados	La institución financiera no cuenta con un inventario actualizado y completo de los activos de información y sus responsables	Modera	Moderado	Moderado
R17	Falta de procedimientos establecidos y normados	No existe información actualizada de titulares de la información y sus delegados	Moderado	Moderado	Medio
R26	Falta de procedimientos establecidos y normados	No existe un inventario de recursos y de administradores	Muy Alto	Muy Alto	Muy Alto
R27	Falta de procedimientos establecidos y normados	No existe un proceso de control cruzado sobre perfiles y procesos	Muy Alto	Muy Alto	Muy Alto
R42	Falta de procedimientos establecidos y normados	No se encuentran establecidas y definidas las áreas restringidas.	Muy Alto	Muy Alto	Muy Alto
R43	Falta de procedimientos establecidos y normados	EL control de acceso al edificio no siempre registra las visitas y no hay una bitácora de ingreso y salida de equipos	Muy Alto	Muy Alto	Muy Alto
R52	Falta de procedimientos establecidos y normados	No está definido procesos de control y evolución de riesgos	Muy Alto	Muy Alto	Muy Alto
R53	Falta de procedimientos establecidos y normados	El área de Tecnología no cuenta al momento con procedimientos aprobados sobre su operatividad	Muy Alto	Muy Alto	Muy Alto
R57	Falta de procedimientos establecidos y normados	No existen procedimientos establecidos para intercambio de información con proveedores eventuales o permanentes.	Muy Alto	Muy Alto	Muy Alto
R74	Falta de procedimientos establecidos y normados	No se realiza control sobre la información que se entrega por medios físicos o magnéticos e incluso en declaraciones en la prensa	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R80	Falta de procedimientos establecidos y normados	No existe control sobre las actividades de los Administradores de Red quienes tienen acceso total a directorio activo, Correo Electrónico y manejo de Internet	Muy Alto	Muy Alto	Muy Alto
R82	Falta de procedimientos establecidos y normados	No existe un proceso de verificación de código o validación que el cambio realizado considere todo el proceso de negocio	Muy Alto	Muy Alto	Muy Alto
R83	Falta de procedimientos establecidos y normados	No se realiza revisión técnica luego de efectuar cambios en el SO	Muy Alto	Muy Alto	Muy Alto
R84	Falta de procedimientos establecidos y normados	No se maneja un proceso definido para versionamiento de los aplicativos y no existe control adecuado y resguardo de los mismos	Muy Alto	Muy Alto	Muy Alto
R85	Falta de procedimientos establecidos y normados	No se incluye ningún proceso específico para la protección de los sistemas.	Muy Alto	Muy Alto	Muy Alto
R92	Falta de procedimientos establecidos y normados	No existen procesos de control y evaluación de Riesgo con los proveedores.	Muy Alto	Muy Alto	Muy Alto
R94	Falta de procedimientos establecidos y normados	No existe un proceso establecido de control y evaluación de proveedores	Muy Alto	Muy Alto	Muy Alto
R96	Falta de procedimientos establecidos y normados	No existe un procedimiento establecido para manejo de incidentes de seguridad de la información.	Muy Alto	Muy Alto	Muy Alto
R4	Falta de segregación de funciones	Se verifica que existe falta de segregación de funciones en los procesos operativos y tecnológicos de la institución financiera	Muy Alto	Alto	Alto
R32	Uso inadecuado de recursos	No existe un control o procesos establecidos por los administradores de todas las áreas para revisión de perfiles y derechos de acceso a los aplicativos	Muy Alto	Muy Alto	Muy Alto
R99	Falta de procedimientos establecidos y normados	No se realiza un proceso de evaluación y clasificación de incidentes, al momento se realiza reporte mensual de los temas que el área de Seguridad tuvo conocimiento en el mes y se informa en el Comité de Riesgos, sin embargo no se realiza un seguimiento adecuado y cierre de los incidentes encontrados.	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R67	Uso inadecuado de recursos	No existen procesos de control de instalación de software en servidores y equipos por parte de proveedores.	Muy Alto	Muy Alto	Muy Alto
R49	Falta de estandarización en infraestructura	No se encuentra garantizada la conexión de todos los equipos a UPS	Muy Alto	Muy Alto	Muy Alto
R50	Falta de estandarización en infraestructura	No existe estándares de cableado y elementos de comunicación. No existe coordinación con las áreas de infraestructuras para realizar compras e instalación	Muy Alto	Alto	Alto
R61	Falta de estandarización en infraestructura	No existe una política de actualización de equipos de forma masiva, por lo que no se garantiza el cierre de vulnerabilidades	Muy Alto	Moderado	Moderado
R66	Falta de estandarización en infraestructura	No existe un adecuado proceso de actualización de versiones y sincronización de relojes en las máquinas de registro de ingreso. No se encuentra normado la hora que debe tomar para registros de pistas de auditoría en algunos casos toma el del servidor de aplicativo y otros del servidor de base de datos)	Muy Alto	Muy Alto	Muy Alto
R73	Falta de estandarización en infraestructura	No existe separación de redes, no se tienen separados usuarios, ni servicios. Manejan una red plana, no se tiene controles de enrutamiento discriminando el trafico confidencial	Muy Alto	Muy Alto	Muy Alto
R68	Falta de monitoreo o control	No se maneja un proceso de gestión de vulnerabilidades integral, no se verifica el cumplimiento en todos los equipos de la institución financiera	Muy Alto	Alto	Alto
R97	Falta de monitoreo o control	No existe un proceso para manejo de incidentes, seguimiento y cierre de los mismos, así como la definición de controles que eviten que estos incidentes vuelvan a ocurrir	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R98	Falta de monitoreo o control	No se tiene cultura para notificación de incidentes de seguridad tanto de usuarios internos, clientes o proveedores	Muy Alto	Muy Alto	Muy Alto
R81	Falta de procedimientos establecidos y normados	No existen procedimientos formales para cumplir un ciclo de desarrollo del software, con estándares y metodologías	Muy Alto	Muy Alto	Muy Alto

Fuente: Los Autores.

Valoración del Riesgo x Amenaza Técnicas

En la tabla 2-20 se muestra la evaluación del riesgo vs amenazas técnicas.

Tabla 2-20: Valoración del Riesgo x Amenaza Técnicas

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R38	Accesos no autorizados	No se tiene una herramienta de administración de accesos a los aplicativos de la intranet	Muy Alto	Muy Alto	Muy Alto
R39	Accesos no autorizados	No se maneja un proceso adecuado de versionamiento.	Muy Alto	Muy Alto	Muy Alto
R46	Accesos no autorizados	No se realiza control específico en áreas como Cumplimiento, Tecnología y en el Data Center local se evidencia ingreso de personal sin que esto sea registrado en las bitácoras definidas como parte del procedimiento	Muy Alto	Muy Alto	Muy Alto
R60	Accesos no autorizados	El área tecnológica no cuenta con entornos definidos para desarrollo, pruebas y producción para todos los aplicativos de la institución financiera	Muy Alto	Muy Alto	Muy Alto
R71	Accesos no autorizados	El área tecnológica no cuenta con entornos definidos para desarrollo, pruebas y producción para todos los aplicativos de la institución financiera. No se encuentra delimitado las funciones del área de soporte y del área de Redes, por lo que no existen registros actualizados ni responsables del manejo de	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
		IP fija, en los casos requeridos.			
R72	Accesos no autorizados	No existen reglas de expiración de claves que se utilizan para conexión mediante una red privada virtual (VPN). No se realiza restricción de puertos físicos o control de los mismos	Muy Alto	Muy Alto	Muy Alto
R59	Falta de Licencias	Existe falta de monitoreo y evaluación adecuada de capacidades en infraestructura actual o cambios a realizarse	Muy Alto	Muy Alto	Muy Alto
R76	Intervención de correos y llamadas	No se cuenta con un servidor de archivos, por lo cual los usuarios envían información confidencial por correo	Muy Alto	Muy Alto	Muy Alto
R40	Mal manejo de equipos y software	No se realiza un control y unificación de controles criptográficos de los distintos aplicativos usados en la institución	Muy Alto	Muy Alto	Muy Alto
R51	Mal manejo de equipos y software	No se maneja un plan de mantenimiento de equipos, se realiza cambios sólo en casos que el personal solicite cambio del mismo	Muy Alto	Muy Alto	Muy Alto
R54	Mal manejo de equipos y software	No existe total cumplimiento del procedimiento establecido para reutilizar equipos, es común ver información de otros usuarios anteriores del equipo	Muy Alto	Muy Alto	Muy Alto
R62	Negación de servicios	No se evidencia pruebas periódicas de procesos de restauración de respaldos de BDD que evidencien que los respaldos se encuentran generados correctamente. No se maneja una copia de respaldos sitio alterno que sea utilizada en casos de contingencia	Muy Alto	Moderado	Moderado
R95	Negación de servicios	No se realizan los pagos de contratos con proveedores a tiempo lo que conlleva a que no se de servicios por parte del proveedor y falta de disponibilidad de soporte técnico. No existe un proceso de gestión de cambios en los servicios prestados por terceros	Muy Alto	Muy Alto	Muy Alto

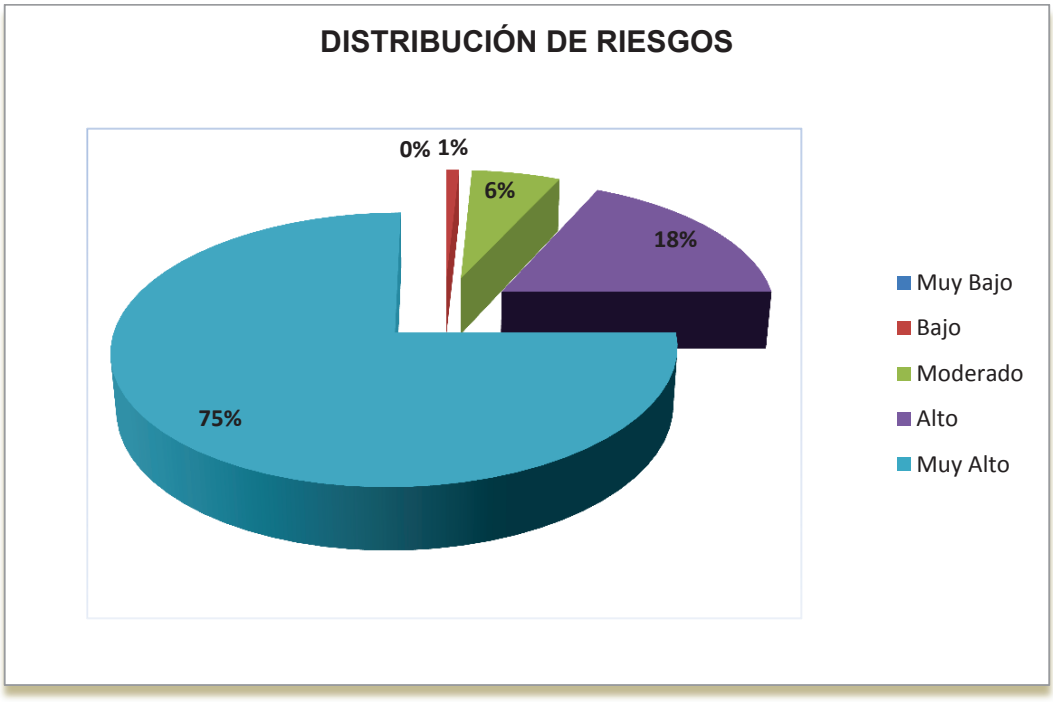
IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
R41	Pérdida de contraseñas	No existe una política establecida para uso, protección y duración de las claves criptográficas, así como falta de registro y archivo de las claves que maneja la institución en los distintos aplicativos	Muy Alto	Muy Alto	Muy Alto
R44	Pérdida o Robo de Equipos	No se cuenta con una seguridad física acorde a la información que manejan, no se realiza cierre de oficinas, archivadores sin llave.	Muy Alto	Muy Alto	Muy Alto
R30	Mal manejo de equipos y software	No existe control sobre los procesos de administración de usuarios, administradores tecnológicos y administradores de equipos personales así como procesos que son administrados por proveedores. No hay un proceso establecido para la administración de cuentas genéricas y que en su gran mayoría maneja privilegios especiales.	Muy Alto	Alto	Alto
R31	Pérdida de contraseñas	No se cumple con la política de contraseñas y entrega segura de claves en los sistemas administrados por el área de Tecnología.	Muy Alto	Muy Alto	Muy Alto
R37	Pérdida de contraseñas	No existe un proceso formal para la entrega de claves a los usuarios por parte de los administradores. No se ha establecido un id único por funcionario para todos los aplicativos y sistemas de la institución financiera.	Muy Alto	Alto	Alto
R8	Pérdida o Robo de Equipos	No existen procedimientos establecidos de control de salida e ingreso de equipos. El 50% de equipos portátiles no cuenta con encriptación de disco.	Muy Alto	Muy Alto	Muy Alto
R19	Pérdida o Robo de Equipos	No existe un inventario actualizado de activos. No se cumple el proceso de devolución de activos previo a la salida del personal.	Alto	Alto	Alto
R79	Incumplimiento Políticas de Seguridad	No se tiene normativa sobre los estándares de controles criptográficos permitidos en la Institución.	Muy Alto	Muy Alto	Muy Alto
R44	Pérdida o Robo de Equipos	Las áreas no cuentan con una seguridad física acorde a la información que manejan, no se realiza cierre de oficinas personales, archivadores sin llave. La información se deja a la vista. El acceso físico se lo establece mediante la	Muy Alto	Muy Alto	Muy Alto

IDENTIFICADOR DEL RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD de la AMENAZA	IMPACTO POR LA VULNERABILIDAD	RIESGO
		identificación de la huella digital, lo cual es manejado por Seguridad Física. Se observa que ingresan otras personas que no pertenecen al área, ya que no existe un proceso normado de control y manejo adecuado de accesos físicos.			

Fuente: Los Autores.

De acuerdo a los resultados del análisis de riesgo realizado a la institución financiera se muestra la distribución de los riesgos en la figura 2-2.

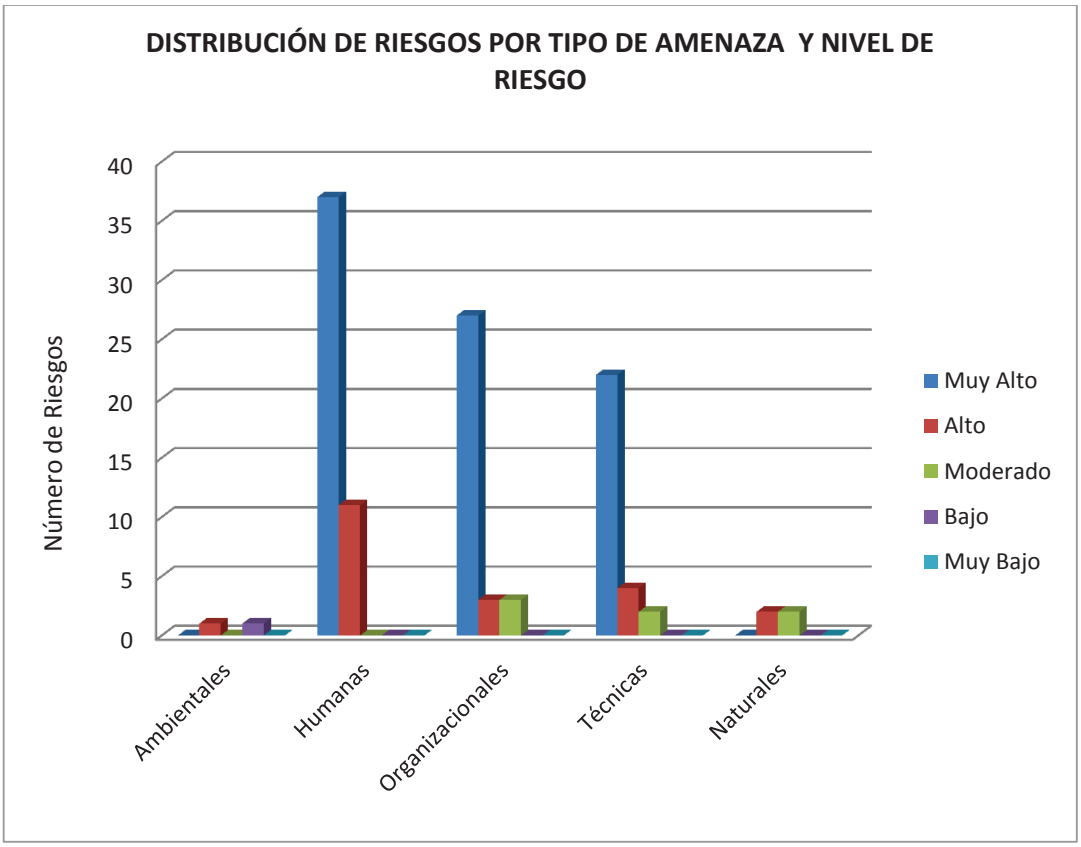
Figura 2-2: Distribución de Riesgos de acuerdo a su clasificación



Fuente: Los autores

En la figura 2-3 se muestran la distribución de los riesgos por tipo de amenaza y el impacto.

Figura 2-3: Distribución de Riesgos por tipo de Amenaza y nivel de riesgo



Fuente: Los autores

En la tabla 2-21 se muestra el mapa de calor el cual permite visualizar de manera rápida la probabilidad de los riesgos y su intensidad en caso de materialicen. Como se puede apreciar la gran mayoría de los riesgos están ubicados en los niveles superiores.

Tabla 2-21: Matriz de calor

Amenazas \ Vulnerabilidad	Muy Alto	Alto	Moderado	Bajo	Muy Bajo
Muy Alto	R1 R6 R7 R8 R9 R11 R12 R13 R14 R15 R18 R20 R21 R22 R23 R25 R26 R27 R28 R31 R32 R33 R34 R35 R36 R38 R39 R40 R41 R42 R43 R44 R46 R47 R49 R51 R52 R53 R54 R56 R57 R58 R59 R60 R63 R64 R65 R67 R69 R71 R72 R73 R74 R75 R76 R77 R79 R80 R81 R82 R83 R84 R85 R86 R87 R88 R89 R90 R91 R92 R93 R94 R95 R96 R97 R98 R99 R100 R101 R102 R104 R105 R109 R110 R111 R112 R113	R3 R4 R10 R24 R29 R30 R37 R48 R50 R68 R70 R114	R2 R61 R62		
Alto		R19 R66			
Moderado	R5 R55 R78 R103 R107 R108 R116	R45	R16 R17 R115		
Bajo		R106			
Muy Bajo					

Fuente: Los autores

I. Recomendaciones para el control

Véase Capítulos 2.2 Determinación de Requerimientos de Seguridad y 2.3. Medición del Riesgo.

J. Informe

Véase el capítulo 2.4 Establecer Plan de Acción del SGSI.

2.2 DETERMINACION DE REQUERIMIENTOS DE SEGURIDAD

Para la aplicación de controles recomendados para mitigar el riesgo, se han considerado los controles definidos acorde a la NIST 800-30, la cual indica que se deben clasificar en seguridad técnica, seguridad administrativa y seguridad operacional, o una combinación de tales controles, para maximizar la eficacia de los controles de sus sistemas de Tecnología y de su negocio.

Los controles de seguridad cuando se usan apropiadamente pueden impedir o limitar los daños que afecten a la misión de una organización.

El proceso de recomendación de controles implicará elegir entre una combinación de controles de seguridad técnica, administrativa y operacional para mejorar la postura de seguridad de la organización.
A continuación se establece una primera evaluación sobre la necesidad de controles a manejar en los riesgos detectados en la institución financiera acorde a los criterios de seguridad establecidos en la norma:

2.2.1 CONTROLES DE SEGURIDAD ADMINISTRATIVA

Los controles de Seguridad Administrativa se centran en la definición y documentación de la política de protección de información, pautas y normas, que se llevarán a cabo a través de procedimientos operativos para cumplir con los objetivos de la entidad financiera.
Estos pueden ser preventivos, de detección y recuperación, se puede verificar los controles en la tabla 2-22:

Tabla 2-22: Controles de Seguridad Administrativa.

AREA	CONTROLES DE SEGURIDAD	TIPO	RIESGOS	REQUERIDO
Seguridad Administrativa	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	Preventivo	R3, R4, R5, R6, R107, R108, R109 , R91, R92, R93, R78 , R110	Sí
	Plan de seguridad del sistema o aplicación	Preventivo	R1, R7, R8 , R91, R92, R93	Sí

AREA	CONTROLES DE SEGURIDAD	TIPO	RIESGOS	REQUERIDO
	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	Preventivo	R16, R17, R18, R19, R26, R28, R29, R30, R31, R32, R33, R34	Sí
	Capacitación técnica y en seguridad	Preventivo	R13	Sí
	Evaluación del personal, previo a la contratación, dentro de sus funciones y control de salida	Detección	R10, R11, R12, R14, R15	Sí
	Revisión Periódica de Controles de Seguridad	Detección	R2, R94, R95, R112, R113, R114 , R91, R92, R93, R70	Sí
	Auditorías periódicas	Detección	R94, R95, R112, R113, R114	Sí
	Evaluación del riesgo	Detección	R94, R95, R112, R113, R114	Sí
	Capacidad de respuesta a incidentes	Recuperación	R96, R97, R98, R99, R100, R101, R102	Sí
	Continuidad del negocio	Recuperación	R42, R43, R44, R47, R103, R104, R105	Sí

Fuente: Los autores, basado en los controles definidos en la NIST800-30

2.2.2 CONTROLES DE SEGURIDAD OPERACIONAL

Con en el objeto de dar continuidad a los lineamientos y estándares de la organización, se establece una serie de controles que asegure que las normas sean operativas y se apliquen acorde a los objetivos y misión de la empresa.

Estos pueden ser de tipo preventivo o correctivo, en la tabla 2-23 se puede verificar los controles mencionados.

Tabla 2-23: Controles de Seguridad Operacional

AREA	CONTROLES DE SEGURIDAD	TIPO	RIESGOS	REQUERIDO
Seguridad Operacional	Definición de procedimientos de control de acceso físico o digital	Preventivo	R27	Si
	Distribución y etiquetado de información	Preventivo	R20, R21, R22	Si
	Control de Virus o Vulnerabilidades técnicas	Preventivo	R61,R67, R68, R69	Si
	Protección de las instalaciones tecnológicas	Preventivo	R63, R64, R65, R66	Si
	Protección del cableado estructurado y suministros eléctricos	Preventivo	R9, R50, R71, R72, R73, R80, R81,R82,R83,R84,R85,R86,R86,R88,R89,R90	Si

AREA	CONTROLES DE SEGURIDAD	TIPO	RIESGOS	REQUERIDO
	Procedimientos de respaldos de información	Preventivo	R62	Si
	Procedimientos de mantenimiento externo y de transporte para respaldos	Preventivo	R23, R24, R25	Si
	Protección de estaciones de trabajo, portátiles y computadores personales	Preventivo	R48, R49, R51, R52, R53, R54, R55, R56	Si
	Controles específicos en caso de incendio	Preventivo	R45	Si
	Mantener fuentes de energía alternas	Preventivo	R106	Si
	Control de las condiciones ambientales (humedad y temperatura)	Preventivo	R45	Si
	Acceso y disposición de medios de almacenamiento	Correctivos	R45	Si
	Proporcionar seguridad física específica (sensores de movimiento, CCTV, etc.)	Correctivos	R45, R46	Si
	Garantizar la seguridad del medio ambiente (detectores de humo)	Correctivos	R48, R46	Si

Fuente: Los autores, basado en los controles definidos en la NIST800-30

2.2.3 CONTROLES DE SEGURIDAD TECNICA

Los controles de seguridad técnica son aquellos que se puede automatizar y configurar para proteger contra cierto tipo de amenazas, estos puede ser medidas simples o complejas.

Los controles técnicos se pueden agrupar en tres categorías principales, según el propósito de este: apoyo, preventivo y el de detección y recuperación, en la tabla 2-24 se muestran los controles indicados.

Tabla 2-24: Controles de Seguridad Técnica

AREA	CONTROLES DE SEGURIDAD	TIPO	RIESGOS	REQUERIDO
Seguridad Técnica	Identificación de forma única a usuarios, procesos y recursos de información	Apoyo	R35, R36, R37	Si
	Administración de claves criptográficas	Apoyo	R40, R41, R111	Si
	Configuración de la seguridad en los sistemas tecnológicos de la información	Apoyo	R78, R57,R58,R59,R60, R79	Si

AREA	CONTROLES DE SEGURIDAD	TIPO	RIESGOS	REQUERIDO
	Protección del sistema (Diseño e implementación del sistema)	Apoyo	R57,R58,R59,R60	Si
	Identificación y Autentificación	Preventivo	R39	Si
	Autorización	Preventivo	R39	Si
	Integridad, Disponibilidad y Confidencialidad de los datos	Preventivo	R110	Si
	Protección de las Comunicaciones	Preventivo	R74, R75, R76, R77, R78, R79	Si
	Privacidad de las transacciones	Preventivo	R110	Si
	Control de pruebas de integridad	Detección y Recuperación	R80, R81,R82,R83,R84,R85,R86,R86,R88,R89,R90	Si
	Restauración a un estado seguro	Detección y Recuperación	R80, R81,R82,R83,R84,R85,R86,R86,R88,R89,R90	Si
	Detección de Virus y Erradicación	Detección y Recuperación	R61, R67, R68, R69	Si
	Detección de Intrusos y Contención	Detección y Recuperación	R67, R68, R69	Si
	Auditoría del sistema	Detección y Recuperación	R70, R94, R95, R112, R113, R114	Si

Fuente: Los autores, basado en los controles definidos en la NIST800-30

2.3 DETERMINACION DE CONTROLES ACORDE A LA ISO 27001:2013

Para determinar los controles requeridos por la institución financiera dentro del marco de referencia establecido entre la NIST y la ISO; bajo los términos de mantener una misión aceptable para la organización, se procede a mapear los áreas de seguridad administrativa, operacional y técnica con los controles de la norma ISO/IEC 27001:2013, dando como resultado la tabla adjunta.

Tabla 2-25: Mapeo de Areas de seguridad y controles de la Norma ISO 27001:2013

Área de Seguridad	Criterio de Seguridad	LITERAL	CONTROLES ISO/IEC 27001: 2013
Seguridad Administrativa	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	6.1.1	Asignación de responsabilidades para seguridad de la información
		6.1.2	Segregación de tareas
		6.1.3	Contacto con las autoridades
		6.1.4	Contacto con grupos de interés especial

Área de Seguridad	Criterio de Seguridad	LITERAL	CONTROLES ISO/IEC 27001: 2013
		14.1.1	Análisis y especificación de los requisitos de seguridad
		15.1.1	Política de seguridad de la información para proveedores
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores
		15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones
		18.1.1	Identificación de la legislación aplicable
		18.1.2	Derechos de propiedad intelectual (DPI)
		18.1.3	Protección de los registros de la organización
		18.1.4	Protección de datos y privacidad de la información personal
	Capacidad de respuesta a incidentes	16.1.1	Responsabilidad y procedimientos
		16.1.2	Notificación de los eventos de seguridad de la información
		16.1.3	Notificación de puntos débiles de la seguridad
		16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones
		16.1.5	Respuesta a los incidentes de seguridad
		16.1.6	Aprendizaje de los incidentes de seguridad de la información
		16.1.7	Recopilación de evidencias
	Capacitación técnica y en seguridad	7.2.2	Concienciación, educación y capacitación en SI
	Continuidad del negocio	11.1.1	Perímetro de seguridad física
		11.1.2	Controles físicos de entrada
		11.1.3	Seguridad de oficinas, despachos y recursos
		11.1.6	Áreas de acceso público, carga y descarga
		17.1.1	Planificación de la continuidad de la seguridad de la información
		17.1.2	Implantación de la continuidad de la seguridad de la información
		17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Área de Seguridad	Criterio de Seguridad	LITERAL	CONTROLES ISO/IEC 27001: 2013
	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	8.1.1	Inventarios de activos
		8.1.2	Propiedad de los activos
		8.1.3	Uso aceptable de los activos
		8.1.4	Devolución de activos
		9.1.1	Políticas de control de accesos
		9.2.1	Gestión de altas/bajas en el registro de usuarios
		9.2.2	Gestión de los derechos de accesos asignados a usuarios
		9.2.3	Gestión de los derechos de acceso con privilegios especiales
		9.2.4	Gestión de información confidencial de autentificación de usuarios
		9.2.5	Revisión de los derechos de acceso de los usuarios
		9.2.6	Retirada o adaptación de los derechos de acceso
		9.3.1	Uso de la información confidencial para la autentificación
	Evaluación del personal, previo a la contratación, dentro de sus funciones y control de salida	7.1.1	Investigación de antecedentes
		7.1.2	Términos y condiciones de contratación
		7.2.1	Responsabilidad de gestión
		7.2.3	Proceso disciplinario
		7.3.1	Cese o cambio de puesto de trabajo
	Plan de seguridad del sistema o aplicación	5.1.1	Conjunto de políticas para la seguridad de la información
		6.1.5	Seguridad de la información en la gestión de proyectos
		6.2.1	Políticas de uso de dispositivos para movilidad
	Revisión Periódica de Controles de Seguridad	5.1.2	Revisión de las políticas para la seguridad de la información
		15.2.1	Supervisión y revisión de los servicios prestados por terceros
		15.2.2	Gestión de cambios en los servicios prestados por terceros

Área de Seguridad	Criterio de Seguridad	LITERAL	CONTROLES ISO/IEC 27001: 2013
		18.2.1	Revisión independiente de la seguridad
		18.2.2	Cumplimiento de las políticas y normas de seguridad
		18.2.3	Comprobación del cumplimiento
Seguridad Técnica	Identificación de forma única a usuarios, procesos y recursos de información	9.4.1	Restricción del acceso a la información
		9.4.2	Procedimientos seguros de inicio de sesión
		9.4.3	Gestión de contraseñas de usuario
	Identificación y Autentificación	9.4.5	Control de acceso al código fuentes de los programas
	Administración de claves criptográficas	10.1.1	Política de uso de los controles criptográficos
		10.1.2	Gestión de claves
	Configuración de la seguridad en los sistemas tecnológicos de la información	12.1.1	Documentación de procedimientos de operación
		12.1.2	Gestión de cambios
		12.1.3	Gestión de capacidades
		12.1.4	Separación de entornos de desarrollo, prueba y producción
	Auditoría del sistema	12.7.1	Controles de auditoría de los sistemas de información
	Protección de las Comunicaciones	13.2.1	Políticas y procedimientos de intercambio de información
		13.2.2	Acuerdos de intercambio
		13.2.3	Mensajería electrónica

Área de Seguridad	Criterio de Seguridad	LITERAL	CONTROLES ISO/IEC 27001: 2013
		13.2.4	Acuerdos de confidencialidad y secreto
	Configuración de la seguridad en los sistemas tecnológicos de la información	14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas
	Administración de claves criptográficas	18.1.5	Regulación de los controles criptográficos
Seguridad Operacional	Control de las condiciones ambientales (humedad y temperatura)	11.1.4	Protección contra las amenazas externas y ambientales
	Control de pruebas de integridad	14.2.1	Política de desarrollo seguro de software
		14.2.2	Procedimientos de control de cambios en los sistemas
		14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
		14.2.4	Restricciones a los cambios en los paquetes de software
		14.2.5	Uso de principio de ingeniería en protección de sistemas
		14.2.6	Seguridad en entornos de desarrollo
		14.2.7	Externalización del desarrollo del software
		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas
		14.2.9	Pruebas de aceptación
		14.3.1	Protección de los datos utilizados en pruebas
	Control de Virus o Vulnerabilidades técnicas	12.2.1	Controles para el código malicioso
		12.5.1	Instalación del software en sistemas en producción
		12.6.1	Gestión de las vulnerabilidades técnicas
		12.6.2	Restricciones en la instalación del software
	Definición de procedimientos de control de acceso físico o digital	9.1.2	Control de acceso a las redes y servicios asociados
	Distribución y etiquetado de información	8.2.1	Directrices de clasificación
		8.2.2	Etiquetado y manipulado de la información
		8.2.3	Manipulación de activos
	Garantizar la seguridad del medio ambiente (detectores de humo)	9.4.4	Uso de herramientas de administración de sistemas
	Mantener fuentes de energía alternas	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información
	Procedimientos de mantenimiento externo y de transporte para	8.3.1	Gestión de soportes extraíbles
		8.3.2	Eliminación de soportes

Área de Seguridad	Criterio de Seguridad	LITERAL	CONTROLES ISO/IEC 27001: 2013
	respaldos	8.3.3	Soportes físicos en tránsito
	Procedimientos de respaldos de información	12.3.1	Copias de seguridad de la información
	Proporcionar seguridad física específica (sensores de movimiento, CCTV, etc.)	11.1.5	El trabajo en áreas seguras
	Protección de estaciones de trabajo, portátiles y computadores personales	11.2.1	Emplazamiento y protección de equipos
		11.2.2	Instalación de suministros
		11.2.4	Mantenimiento de los equipos
		11.2.5	Salida de activos fuera de las dependencias de la empresa
		11.2.6	Seguridad de los equipos y activos fuera de las instituciones
		11.2.7	Reutilización o retirada segura de dispositivos de almacenamientos
		11.2.8	Equipo informático de usuario desatendido
		11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla
	Protección de las Comunicaciones	14.1.3	Protección de las transacciones por redes telemáticas
	Protección de las instalaciones tecnológicas	12.4.1	Registro y gestión de eventos de actividad
		12.4.2	Protección de los registros de información
		12.4.3	Registros de actividades del administrador y operado del sistema
		12.4.4	Sincronización de relojes
	Protección del cableado estructurado y suministros eléctricos	6.2.2	Teletrabajo
		11.2.3	Seguridad del cableado
		13.1.1	Controles de red
		13.1.2	Mecanismos de seguridad asociados a servicios en red
		13.1.3	Segregación de redes

Fuente: Los Autores.

2.4 ESTABLECER PLAN DE ACCION DEL SGSI

Con el objeto de establecer el plan de acción a seguir por la institución financiera, se debe gestionar los riesgos identificados mediante la aplicación de controles seleccionados, las acciones apropiadas por el personal, la disponibilidad de infraestructura tecnológica que apoye a la automatización de controles y cierre de vulnerabilidades; esto enmarcado en una clara estrategia

administrativa que evalúe el tipo de tratamiento a realizarse con los riesgos identificado.

2.4.1 OPCIONES PARA EL TRATAMIENTO DEL RIESGO

La institución financiera puede optar por:

ACEPTAR: Significa asumir un riesgo y las consecuencias de su materialización. Los riesgos se deberían aceptar cuando la frecuencia es baja y el impacto leve, y no pone en peligro la estabilidad de la organización.

MITIGAR: En este caso el objetivo es cerrar las vulnerabilidades de forma parcial o completa con el objeto de que el riesgo no se materialice, esto puede ser mediante la implementación de controles humanos, tecnológicos o administrativos.

TRANSFERIR: El transferir un riesgo se da cuando se traspasa el riesgo a otra compañía, ya sea por medio de un contrato de tercerización o una póliza de seguro.

2.4.2 EVALUACION GENERAL DEL NIVEL DE CUMPLIMIENTO DEL SGSI

De acuerdo a la evaluación realizada, se determinó que los riesgos de clasificación alta y muy alta superan el 90%, por lo que requieren atención inmediata y seguimiento por la alta directiva, la misma que deberá priorizar y establecer el tratamiento de los riesgos acorde al costo/beneficio de implementar el control en beneficio de la institución.

Considerando los resultados obtenidos en la evaluación se sugiere establecer los planes de acción a corto, mediano y largo plazo citados a continuación:

Plan de Acción a Corto Plazo

1. Actualización de Política y Aprobación del Reglamento, las mismas que deberán ser difundidas y formalizadas.

2. Definición de Comité y establecer Presupuesto 2016.
3. Establecer Proceso Disciplinario con el área de Talento Humano (TTHH) por faltas a las políticas internas de seguridad, así como la implementación de Controles de Ingreso y Salida del personal.
4. Mantener un proceso establecido y operativo de Incidentes de Seguridad.
5. Segregación de Ambientes y Áreas en TI.
6. Implementar un procedimiento de control de ingreso y salida de personal y recursos de la institución.
7. Definir Acuerdos de Nivel de Operación internos entre las unidades de negocio.
8. Incluir en los planes de auditoría las actividades y procesos realizados por terceros.
9. Promover la disponibilidad y adecuada capacitación de funcionarios alternos, en caso de ausencia del titular.
10. Desarrollar, divulgar y realizar pruebas a planes de recuperación de la infraestructura tecnológica.
11. Configuración de servidores y equipos de comunicación con lineamientos básicos de seguridad.

Plan de Acción a Mediano Plazo

1. Levantamiento de Recursos y Administradores.
2. Establecer procedimientos para el ciclo de desarrollo de aplicativos.
3. Implementar tecnologías y procedimientos de monitoreo a nivel de red, equipos de comunicaciones, sistemas de detección de intrusos, cortafuegos, en el perímetro de seguridad electrónica.
4. Seguridad Física (Escritorio Limpio – Destrucción Segura).
5. Definición de permisos de Red, Internet, Servidor de archivos y desactivación USB.
6. Establecer proveedores críticos y procesos de evaluación a los mismos.
7. Establecer Auditoría independiente para evaluación de controles establecidos.
8. Definición e implementación de un Plan de Continuidad de Negocio.

Plan de Acción a Largo Plazo

1. Adquisición de soluciones que permitan fortalecer y automatizar los controles de seguridad como por ejemplo: correlacionador de eventos, Sistema de prevención de pérdida de datos, Gestión de Identidad centralizado, entre otros.

Para el cumplimiento de los objetivos definidos en cada plan de acción se deberá considerar al menos los factores críticos de éxito o fracaso identificados en la evaluación realizada y que se listan a continuación.

Factores Críticos de Éxito:

1. Definir y establecer los objetivos de seguridad de la información y planes para lograrlo.
2. Definir las competencias necesarias para la adecuada gestión de las actividades relacionadas con la implementación del SGSI, generación de planes y responsables.
3. Revisar y actualizar periódicamente la Política de Seguridad de la Información.
4. Incluir la seguridad de la información en la gestión de proyectos, independiente del tipo de proyecto.
5. Apoyo de la alta dirección
6. Participación Integra de todas las áreas de la entidad bancaria
7. Proceso de concientización y capacitación permanente.

Factores Críticos para el fracaso:

1. Rotación de los miembros de la alta Gerencia, falta de apoyo o de continuidad del proyecto.
2. Falta de personal y de presupuesto;
3. Manejo de excepciones en los controles establecidos bajo aprobación de la alta gerencia.

CAPITULO 3: DETERMINACION DE LAS ESTRATEGIAS DE IMPLEMENTACION DEL PLAN DE SEGURIDAD

3.1 REQUERIMIENTOS LEGALES Y ORGANIZACIONALES

El marco legal y operacional que define los controles que deben ser requeridos y que regulan el proceso de la institución financiera es de carácter nacional e interno. Se han identificado las siguientes normativas legales que rigen a la institución financiera y que nos permitirán definir los controles que deben ser considerados, entre las más importantes se indican las siguientes:

- Nacionales.
  - Ley Orgánica de Código Penal
  - Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
  - Ley de Propiedad Intelectual
  - Ley Orgánica del Sector Público (LOSEP)
  - Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)
- Resoluciones de la Superintendencia de Bancos y Seguros
  - Normas Generales para las instituciones financieras. CAP V. de la Gestión de Riesgo Operativo (incluye: JB-2005-834, JB-2012-2148 Y JB-2014-3066)
  - JB-2009-1405
- Internas
  - Política de Seguridad de la Información de la Institución Financiera
  - Reglamento de Seguridad de la Información de la Institución Financiera

3.1.1 LEGISLACION NACIONAL

3.1.1.1 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Se detalla a continuación algunos artículos que aplican a la institución financiera, la ley completa se la puede revisar en el Anexo 3-A:

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

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

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

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

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

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

3.1.1.2 Ley de Propiedad Intelectual

Se detalla a continuación algunos artículos que aplican a la institución financiera, la ley completa se la puede revisar en el Anexo 3-B:

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

La propiedad intelectual comprende:

1. Los derechos de autor y derechos conexos.
2. La propiedad industrial, que abarca, entre otros elementos, los siguientes:

a. Las invenciones;

b. Los dibujos y modelos industriales;

c. Los esquemas de trazado (topografías) de circuitos integrados;

d. La información no divulgada y los secretos comerciales e industriales;

e. Las marcas de fábrica, de comercio, de servicios y los lemas comerciales;

f. Las apariencias distintivas de los negocios y establecimientos de comercio;

g. Los nombres comerciales;

h. Las indicaciones geográficas; e,

i. Cualquier otra creación intelectual que se destine a un uso agrícola, industrial o comercial.

Art. 186. Serán responsables por la divulgación, adquisición o utilizaciones no autorizadas de información no divulgada en forma contraria a los usos y prácticas honestas y legales, no solamente quienes directamente las realicen, sino también quien obtenga beneficios de tales actos o prácticas.

Art. 187. La protección de la información no divulgada prevista en el artículo 173 perdurará mientras existan las condiciones allí establecidas.

Art. 190. Toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a una información no divulgada, deberá abstenerse de usarla y de divulgarla, sin causa justificada, calificada por el juez competente y sin consentimiento del titular, aun cuando su relación laboral, desempeño de su profesión o relación de negocios haya cesado.

3.1.1.3 Ley Orgánica del Sector Público (LOSEP)

Se detalla a continuación algunos artículos que aplican a la institución financiera, la ley completa se la puede revisar en el Anexo 3-C:

Art. 5.- Requisitos para el ingreso.- Para ingresar al servicio
Público se requiere:
a) Ser mayor de 18 años y estar en el pleno ejercicio de los derechos previstos por la Constitución de la República y la Ley para el desempeño de una función pública;
b) No encontrarse en interdicción civil, no ser el deudor al que se siga proceso de concurso de acreedores y no hallarse en de estado insolvencia fraudulenta declarada judicialmente;
c) No estar comprendido en alguna de las causales de prohibición para ejercer cargos públicos;
d) Cumplir con los requerimientos de preparación académica y demás competencias exigibles previstas en esta Ley y su Reglamento;
e) Haber sufragado, cuando se tiene obligación de hacerlo, salvo las causas de excusa previstas en la Ley;
f) No encontrarse en mora del pago de créditos establecidos a favor de entidades u organismos del sector público, a excepción de lo establecido en el Artículo 9 de la presente Ley;
g) Presentar la declaración patrimonial juramentada en la que se incluirá lo siguiente:

a. Autorización para levantar el sigilo de sus cuentas bancarias;
b. Declaración de no adeudar más de dos pensiones alimenticias; y,
c. Declaración de no encontrarse incurso en nepotismo, inhabilidades o prohibiciones previstas en la Constitución de la República y el ordenamiento jurídico vigente.

h) Haber sido declarado triunfador en el concurso de méritos y oposición, salvo en los casos de las servidoras y servidores públicos de elección popular o de libre nombramiento y remoción; e,
i) Los demás requisitos señalados en la Constitución de la República y la Ley.

Exceptúense los casos específicos y particulares que determina la Ley.

Las instituciones públicas sujetas a esta Ley, garantizarán que los procesos de selección e incorporación al servicio público, promuevan políticas afirmativas de inclusión a grupos de atención prioritaria, la interculturalidad y, la presencia paritaria de hombres y mujeres en los cargos de nominación y designación. Las personas extranjeras residentes en el Ecuador podrán prestar sus servicios en calidad de servidoras o servidores públicos en asuntos en los cuales por su naturaleza se requiera contar con los mismos, sin perjuicio de la aplicación de los convenios bilaterales de reciprocidad que rijan esta materia, previo informe y de ser el caso el permiso de trabajo otorgado por el Ministerio de Relaciones Laborales. Para ocupar puestos de carrera, deberán tener una residencia en el país de al menos 5 años y haber cumplido el respectivo concurso de méritos y oposición.

En caso de requerirse la contratación de personas extranjeras, la autoridad nominadora, previo informe motivado de la unidad de administración del talento humano solicitará la respectiva autorización del Ministerio de Relaciones Laborales.

Art. 41.- Responsabilidad administrativa.- La servidora o servidor público que incumpliere sus obligaciones o contraviniere las disposiciones de esta Ley, sus reglamentos, así como las leyes y normativa conexa, incurrirá en responsabilidad administrativa que será sancionada disciplinariamente, sin perjuicio de la acción civil o penal que pudiere originar el mismo hecho.

La sanción administrativa se aplicará conforme a las garantías básicas del derecho a la defensa y el debido proceso.

Art. 42.- De las faltas disciplinarias.- Se considera faltas disciplinarias aquellas acciones u omisiones de las servidoras o servidores públicos que contravengan las disposiciones del ordenamiento jurídico vigente en la República y esta ley, en lo atinente a derechos y prohibiciones constitucionales o legales.

Serán sancionadas por la autoridad nominadora o su delegado.

Para efectos de la aplicación de esta ley, las faltas se clasifican en leves y graves.

a.- Faltas leves.- Son aquellas acciones u omisiones realizadas por descuidos o desconocimientos leves, siempre que no alteren o perjudiquen gravemente el normal desarrollo y desenvolvimiento del servicio público.
Se considerarán faltas leves, salvo que estuvieren sancionadas de otra manera, las acciones u omisiones que afecten o se contrapongan a las disposiciones administrativas establecidas por una institución para velar por el orden interno, tales como incumplimiento de horarios de trabajo durante una jornada laboral, desarrollo inadecuado de actividades dentro de la jornada laboral; salidas cortas no autorizadas de la institución; uso indebido o no uso de uniformes; desobediencia a instrucciones legítimas verbales o escritas; atención indebida al público y a sus compañeras o compañeros de trabajo, uso inadecuado de bienes, equipos o materiales; uso indebido de medios de comunicación y las demás de similar naturaleza.

Las faltas leves darán lugar a la imposición de sanciones de amonestación verbal, amonestación escrita o sanción pecuniaria administrativa o multa.
b.- Faltas graves.- Son aquellas acciones u omisiones que contraríen de manera grave el ordenamiento jurídico o alteraren gravemente el orden institucional. La sanción de estas faltas está encaminada a preservar la probidad, competencia, lealtad, honestidad y moralidad de los actos realizados por las servidoras y servidores públicos y se encuentran previstas en el artículo 48 de esta ley.
La reincidencia del cometimiento de faltas leves se considerará falta grave.
Las faltas graves darán lugar a la imposición de sanciones de suspensión o destitución, previo el correspondiente sumario administrativo.
En todos los casos, se dejará constancia por escrito de la sanción impuesta en el expediente personal de la servidora o servidor.
Art. 43.- Sanciones disciplinarias.- Las sanciones disciplinarias por orden de gravedad son las siguientes:
a) Amonestación verbal;
b) Amonestación escrita;
c) Sanción pecuniaria administrativa;
d) Suspensión temporal sin goce de remuneración; y,

e) Destitución.

La amonestación escrita se impondrá cuando la servidora o servidor haya recibido, durante un mismo mes calendario, dos o más amonestaciones verbales.

La sanción pecuniaria administrativa o multa no excederá el monto del diez por ciento de la remuneración, y se impondrá por reincidencia en faltas leves en el cumplimiento de sus deberes. En caso de reincidencia, la servidora o servidor será destituido con sujeción a la ley.

Las sanciones se impondrán de acuerdo a la gravedad de las faltas.

Art. 22.- Deberes de las o los servidores públicos.- Son deberes de las y los servidores públicos:

a) Respetar, cumplir y hacer cumplir la Constitución de la República, leyes, reglamentos y más disposiciones expedidas de acuerdo con la Ley;

b) Cumplir personalmente con las obligaciones de su puesto, con solicitud, eficiencia, calidez, solidaridad y en función del bien colectivo, con la diligencia que emplean generalmente en la administración de sus propias actividades;

g) Elevar a conocimiento de su inmediato superior los hechos que puedan causar daño a la administración;

h) Ejercer sus funciones con lealtad institucional, rectitud y buena fe. Sus actos deberán ajustarse a los objetivos propios de la institución en la que se desempeñe y administrar los recursos públicos con apego a los principios de legalidad, eficacia, economía y eficiencia, rindiendo cuentas de su gestión;

i) Cumplir con los requerimientos en materia de desarrollo institucional, recursos humanos y remuneraciones seleccionados por el ordenamiento jurídico vigente;

j) Someterse a evaluaciones periódicas durante el ejercicio de sus funciones; y, Custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión tenga bajo su responsabilidad e impedir o evitar su uso indebido, sustracción, ocultamiento o inutilización.

3.1.1.4 Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)

Se detalla a continuación algunos artículos que aplican a la institución financiera, la ley completa se la puede revisar en el Anexo 3-D:

Art. 1.- Principio de Publicidad de la Información Pública.-
El acceso a la información pública es un derecho de las personas que garantiza el Estado.
Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONG's), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley.

La presente Ley garantiza y norma el ejercicio del derecho fundamental de las personas a la información conforme a las garantías consagradas en la Constitución Política de la República, Pacto Internacional de Derechos Civiles y Políticos, Convención Interamericana sobre Derechos Humanos y demás instrumentos internacionales vigentes, de los cuales nuestro país es signatario.
Persigue los siguientes objetivos:
a) Cumplir lo dispuesto en la Constitución Política de la República referente a la publicidad, transparencia y rendición de cuentas al que están sometidas todas las instituciones del Estado que conforman el sector público, dignatarios, autoridades y funcionarios públicos, incluidos los entes señalados en el artículo anterior, las personas jurídicas de derecho privado que realicen obras, servicios, etc., con asignaciones públicas. Para el efecto, adoptarán las

medidas que garanticen y promuevan la organización, clasificación y manejo de la información que den cuenta de la gestión pública;
c) Permitir la fiscalización de la administración pública y de los recursos públicos, efectivizándose un verdadero control social;
d) Garantizar la protección de la información personal en poder del sector público y/o privado;

Art. 5.- Información Pública.-
Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.

Art. 6.- Información Confidencial.-
Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.
El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.
No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas

Art. 9.- Responsabilidad sobre la entrega de la Información Pública.-
El titular de la entidad o representante legal, será el responsable y garantizará la atención suficiente y necesaria a la publicidad de la información pública, así como su libertad de acceso.

Su responsabilidad será recibir y contestar las solicitudes de acceso a la información, en el plazo perentorio de diez días, mismo que puede prorrogarse por cinco días más, por causas debidamente justificadas e informadas al peticionario.

Art. 10.- Custodia de la Información.-
Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción.
Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública. Los documentos originales deberán permanecer en las dependencias a las que pertenezcan, hasta que sean transferidas a los archivos generales o Archivo Nacional.
El tiempo de conservación de los documentos públicos, lo determinará la Ley del Sistema de Archivo Nacional y las disposiciones que regulen la conservación de la información pública confidencial.
Los documentos de una institución que desapareciere, pasarán bajo inventario al Archivo Nacional y en caso de fusión interinstitucional, será responsable de aquello la nueva entidad.

3.1.1.5 Resoluciones de la Superintendencia de Bancos y Seguros

NORMA DE RIESGO OPERATIVO
Se detalla a continuación algunos artículos que aplican a la institución financiera, la ley completa se la puede revisar en el Anexo 3-E:

TITULO X. DE LA GESTION Y ADMINISTRACION DE RIESGOS

SECCION I.- AMBITO, DEFINICIONES Y ALCANCE

ARTÍCULO 1.- Las disposiciones de la presente norma son aplicables a las instituciones financieras públicas y privadas, al Banco Central de Ecuador, a las compañías de arrendamiento mercantil, a las compañías emisoras y administradores de tarjetas de crédito y a las corporaciones de desarrollo de mercado secundario de hipotecas, cuyo control compete a la Superintendencia de Bancos y Seguros, a las cuales, en el texto de este capítulo se las denominará como instituciones controladas

SECCION II.- FACTORES DE RIESGO OPERATIVO

ARTÍCULO 4.- Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

4.3 Tecnología de información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Aplican todos lo literales del artículo 4.3, exceptuado 4.3.6 Cajeros automáticos, 4.3.7 Puntos de Venta.

4.4 Eventos externos.- En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus Eventos externos.- En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

SECCION IV.- CONTINUIDAD DEL NEGOCIO

ARTÍCULO 15.- Las instituciones controladas deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio. (Reenumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008)

Para el efecto, deberán efectuar adecuados estudios de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no tenerlo, esto dependerá de la criticidad de cada proceso de la entidad; para aquellos de muy alta criticidad se deberá implementar un plan de continuidad, para otros, bastará con un plan de contingencia.

Las instituciones controladas deberán establecer un proceso de administración de la continuidad de los negocios, que comprenda los siguientes aspectos claves. Aplican todos los literales del artículo 15.

ARTÍCULO 16.- Los planes de contingencia y de continuidad de los negocios deben comprender las previsiones para la reanudación y recuperación de las

operaciones. (Reenumerado con resolución No. JB-2008-1202 de 23 de octubre del 2008). Aplican todos los literales del artículo 16.

SECCION VI.- SERVICIOS PROVISTOS POR TERCEROS (incluida con resolución No. JB-2014-2798 de 19 de febrero del 2014)

ARTÍCULO 20.- Para mantener un adecuado control de los servicios provistos por terceros, incluidos las instituciones de servicios auxiliares del sistema financiero, las instituciones controladas deberán contar con un proceso integral para la administración de proveedores de servicios que incluya las actividades de pre contratación, suscripción, cumplimiento y renovación del contrato, para lo cual deberán por lo menos cumplir con lo siguiente: (remunerado con resolución No. JB-2008-1202 de 23 de octubre del 2008 y sustituido incluida con resolución No. JB-2014-2798 de 19 de febrero del 2014). Aplican todos los literales del artículo 20.

SECCION VII.- SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 21.- Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardad la información contra el uso, revelación y modificación no autorizados, así como los daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y deben al menos; (artículo incluido con resolución No JB-2014-3066 de 2 de septiembre 2014). Aplican todos los literales del artículo 21.

ARTÍCULO 22.- Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información y que considere al menos lo siguiente: (artículo incluido con resolución No JB-2014-3066 de 2 de septiembre 2014). Aplican todos los literales del artículo 22.

SECCION IX.- DISPOSICIONES TRANSITORIAS

PRIMERA.- Las disposiciones reformadas de esta norma deberán cumplirse conforme al cronograma: (disposición transitoria sustituida con resolución No JB-2014-3066 de 2 de septiembre 2014)

SEGUNDA.- Las instituciones del sistema financiero para dar cumplimiento a las disposiciones transitorias de la sección VI, de este capítulo, tendrán un plazo de trescientos setenta 370 días, a partir de la publicación de esta reforma en el Registro Oficial.

TERCERA.- Las instituciones del sistema financiero deben reportar el nivel cumplimiento de las disposiciones referidas en la primera y segunda transitoria en las siguientes fechas: 31 de enero del 2015, 31 de julio del 2015 y 31 de diciembre del 2015. (Incluida con resolución No. JB-2014-3033 de 6 de agosto del 2014).

CUARTA.- La Institución Financiera (objeto de este proyecto) implementará las disposiciones del numeral 4.3 Tecnología de información" del artículo 4, conforme al siguiente cronograma: (incluida con resolución No. JB-2014-3033 de 6 de agosto del 2014)

1. Las disposiciones relacionadas con los factores: procesos, administración del riesgo operativo, servicios provistos por terceros y los numerales de canales electrónicos:
4.3.8.2, 4.3.8.3, 4.3.8.4, 4.3.8.11, 4.3.8.12, 4.3.8.18, 4.3.11.2, deben ser cumplidos hasta diciembre de 2014;
2. Las disposiciones relacionadas con el factor personas y los numerales de canales electrónicos: 4.3.8.1, 4.3.8.25, 4.3.8.16, 4.3.8.15, 4.3.8.7, 4.3.8.6, 4.3.11.10, 4.3.11.3, 4.3.11.9 y 4.3.11.11, deben ser cumplidos hasta junio de 2015; y,
3. Las disposiciones normativas relacionadas con el factor tecnología de la información, deben ser implementadas hasta el mes de diciembre de 2015.

Adicionalmente, las disposiciones relacionadas con la continuidad del negocio, deben ser implementadas hasta el mes de octubre de 2016.
El ente de control en cualquier momento puede realizar una supervisión in situ a fin de verificar el avance del cumplimiento de acuerdo al cronograma enviado por la entidad.

RESOLUCION JB-2009-1405

ARTÍCULO 2.- Dentro de los noventa (90) días posteriores al inicio de sus operaciones, el representante legal de la Institución Financiera deberá presentar a la Superintendencia de Bancos y Seguros, la siguiente información:
2.1 Plan estratégico para un horizonte mínimo de cinco (5) años;
2.2 Manuales operativos; e,
2.3 Implementación de un sistema de control interno que garantice el desenvolvimiento de las operaciones dentro del marco legal y mitigación de los riesgos financieros y operacionales.

3.1.1.7 Código Orgánico Integral Penal

Se detalla a continuación algunos artículos que aplican a la institución financiera, la ley completa se la puede revisar en el Anexo 3-F

Artículo 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.
No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Artículo 179.- Revelación de secreto.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.
Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Será sancionada con pena privativa de libertad de tres a cinco años:
1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal
O de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo

electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.
Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Artículo 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.
Con igual pena será sancionada la persona que:
1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos

destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.
La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

3.1.2 LEGISLACION INTERNA

3.1.2.1 Ley de la Institución Financiera

Se encuentra en la intranet de la Institución Financiera, por temas acuerdo de confidencialidad no se puede incluir en este trabajo.

3.1.2.2 Política de Seguridad de la Información de la Institución Financiera

Existe la Política en la Institución, pero por temas acuerdo de confidencialidad no se puede incluir en este trabajo.

3.1.2.3 Reglamento de Seguridad de la Información de la Institución

Reglamento de Seguridad de la información de la Institución Financiera está en el repositorio común, pero por temas acuerdo de confidencialidad no se puede incluir en este trabajo.

3.2 ALCANCES Y LIMITES DEL SGSI

El alcance de este plan se definió con la institución financiera y abarca la evaluación de los productos o servicios considerados como críticos dentro de la institución, en lo que se refiere a la infraestructura tecnológica se evalúa en sitio la tecnología ubicada en la matriz de la ciudad de Quito Distrito Metropolitano.

Se excluye una evaluación en sitio a la infraestructura de Hosting y Housing que posee la institución financiera, así como también a la infraestructura tecnológica de proveedores externos.

Los aspectos considerados en este trabajo abarca la seguridad técnica, administrativa y operacional.

3.2.1 LIMITES DEL SGSI

3.2.1.1 Servicios implicados

Los servicios que serán parte del alcance son:

Productos Primarios:

- Préstamos Hipotecarios.
- Préstamos Quirografarios.
- Préstamos Prendarios.

Productos Secundarios:

Se incluyen las unidades de soporte y asesoría que apoyan a los servicios primarios seleccionados.

- Tecnología.
- Talento Humano
- Seguridad Física
- Proveedores

3.2.1.2 Localizaciones Físicas

La locación física considerada para el SGSI fue la matriz principal de la institución financiera localizada en la ciudad de Quito.

3.2.1.3 Sistemas de información

Aplican todos los sistemas de información afectados o que dan soporte a los productos primarios y secundarios y que adicionalmente manejen información de clasificación interna, confidencial o crítica de la institución o de sus clientes. Los aplicativos evaluados fueron.

Sistema de Préstamos Prendarios
Sistema de Préstamos Quirografarios
Sistema de Préstamos Hipotecarios

3.2.1.4 Terceros y externos relacionados con el SGSI

La institución financiera maneja varios proveedores, sin embargo al momento no se maneja un inventario y evaluación de los servicios proporcionados, criticidad de los mismos, así como tipo de información manejada. Sobre el estudio realizado establecemos los proveedores mínimos que deberían ser parte del SGSI.

- Empresa proveedora de Servicios Telecomunicaciones.
- Empresa proveedora de Internet (ISP).
- Empresa proveedor de Servicios Hosting y Housing.
- Empresa proveedora de la evaluación del score crediticio de los clientes.
- Empresa proveedora desarrolladora del Sistema Bancario.
- Empresa proveedora de los aplicativos requeridos en Fábrica de Operaciones.
- Empresa proveedora de aplicativos y documentación histórica de Fabrica de Operaciones

Quedan excluidas las empresas que manejen información pública, así como las que dan acceso a servicios públicos primarios como luz, agua, entre otros.

3.2.1.4 Dependencias

Existe dependencia sobre la legislación que regula a la entidad financiera y sobre la normativa interna, la misma que ya fue mencionada en el capítulo 3.1.

En el caso de información existe dependencia total de la institución pública que provee la información de los clientes como insumo inicial para el procesamiento de préstamos.

3.3 POLITICA DEL SGSI

La empresa cuenta con una política y reglamento de Seguridad de la Información aprobada a nivel del Directorio de la Institución financiera, la cual dice textualmente:

En ejercicio de sus atribuciones, Resuelve: Expedir la Política de Seguridad de la Información con fecha 26 de Febrero del 2013. " [24]

Por acuerdo de confidencialidad tanto la política como el reglamento no se pueden incluir en este documento.

De acuerdo a la evaluación realizada a la política que actualmente mantiene la institución financiera, deberán ser consideradas para un proceso de actualización en el que se incluya como mínimo:

- Una definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información.
- El establecimiento del objetivo de la dirección como soporte de los objetivos y principios de la seguridad de la información.
- Una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la institución financiera, basado en normas internacionales, legales y regulatorias, así:
    1. Conformidad con los requisitos legislativos y contractuales actuales.
    2. Organización de la seguridad de la información y responsabilidades.
    3. Establecimiento de Controles al Personal.
    4. Definir Manejo de Activos.
    5. Establecer Control de Accesos.
    6. Incluir Manejo de Cifrado.
    7. Gestión de la continuidad del negocio.
    8. Consecuencias de las violaciones de la política de seguridad.

[24] Institución Financiera, Política de Seguridad de la Información - 26 Febrero 2013

9. Requisitos de uso de los Sistemas de Información como gestión de contraseñas, acceso a internet, uso de correo electrónico.
10. Controles técnicos.
    - Controles de cambio de software.
    - Controles de versión.
    - Seguridad de bases de datos.
    - Seguridad de redes y telecomunicaciones.
    - Seguridad de Sistemas operativos.
    - Seguridad de Cortafuegos.
    - Seguridad de servidores web.
    - Seguridad de Intranet.
    - Seguridad de comercio electrónico.
    - Cifrado de datos.
11. Controles establecidos sobre empresas externas o teletrabajo.
12. Manejo de Incidentes.
13. Establecimiento de Auditorías Internas y Externas.

❖ Es importante que se considere un propietario responsable del mantenimiento y revisión de la política conforme a un proceso de revisión periódico. Este proceso asegurará que la revisión responde a todo cambio que afecte a las bases de la evaluación original de riesgo como incidencias de seguridad significativas, nuevas vulnerabilidades y cambios organizativos o técnicos. Igualmente se definirán las revisiones periódicas de:

- La efectividad de la política (demostrada por el número e impacto de las incidencias de seguridad).
- El coste y el impacto de los controles en la eficiencia del negocio.
- Los efectos de los cambios tecnológicos.

3.4 ENUNCIADO DE APLICABILIDAD

La presente declaración incluye los controles que son relevantes para el sistema de gestión de seguridad de la institución financiera, en este enunciado se encuentra justificada la exclusión de ciertos controles y se muestra el motivo de la selección de los controles aplicables; esto bajo el criterio de la evaluación del riesgo, requisitos regulatorios, obligaciones contractuales y necesidades del negocio.

En la tablas 3-1 se detalla la definición para la selección de controles.

Tabla 3-1: Definición para la selección de controles

SELECCIONADO	Control requerido pero que no cuenta con un grado de implementación.
IMPLEMENTADO	Control requerido y que se encuentra implementado.
PARCIALMENTE IMPLEMENTADO	Control requerido y que cuenta con un grado de implementación mínimo.
NO SELECCIONADO	Control NO Aplicable.

Fuente: Los Autores

En la tablas 3-2 se describen los significados de las abreviaturas utilizadas en la evaluación.

Tabla 3-2: Descripción de abreviaturas de normas y leyes utilizadas en evaluación.

JUSTIFICACIÓN	
Abreviatura	**Significado**
NORMA RO	Normas Generales para Instituciones del Sistema Financiero CAPITULO V DE LA GESTION DE RIESGO OPERATIVO
POLÍTICA SI	Política de Seguridad de la Información de la Institución Financiera.
REGLAMENTO SI	Reglamento de la Seguridad de la Información de la Institución Financiera.
LOSEP	Ley Orgánica del Servicio Público.
COMERCIO ELECTRÓNICO	Ley de Comercio Electrónico de Ecuador.
LOTAIP	Ley Orgánica de Transparencia y Acceso a la Información Pública.

Fuente: Los autores.

A continuación se indican los objetivos de control y controles bajo el estándar de la ISO27001:2013 determinados en la evaluación realizada en el capítulo 2.3 con las respectivas justificaciones de su selección y exclusión; estos se encuentran divididos por dominio.

En la tabla 3-3 muestra el enunciado de aplicabilidad para el dominio de Políticas de Seguridad.

Tabla 3-3: Enunciado de aplicabilidad – Políticas de Seguridad

A.5 POLITICAS DE SEGURIDAD						
A.5.1 Política de Seguridad de la Información Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo a los requisitos del negocio y los reglamentos y leyes pertinentes			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.5.1.1	Documento de la política de seguridad de la información	Control: La dirección debe aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.	**IMPLEMENTADO**	Plan de seguridad del sistema o aplicación	NORMA RO	21.2
					POLITICA SI	TODO
					REGLAMENTO SI	21-a
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.5.1.2	Revisión de la política de seguridad de la información	Control: La política de seguridad de la información se debe revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz	**PARCIALMENTE IMPLEMENTADO**	Revisión Periódica de Controles de Seguridad	NORMA RO	21.1
					POLITICA SI	3.0 - 8.0
					REGLAMENTO SI	1.0 - 8.0 , 20-a, 20-b, 20-c
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-4 muestra el enunciado de aplicabilidad para el dominio de Organización de la Seguridad de la información.

Tabla 3-4: Enunciado de aplicabilidad – Organización de Seguridad de la Información

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION						
A.6.1 Organización interna Objetivo: Establecer un esquema directivo de gestión para iniciar y controlar la implementación de la seguridad de la información en la organización.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.6.1.1	Asignación de responsabilidades para la seguridad de la información	Control: Se deben definir y asignar claramente todas las responsabilidades para la seguridad de la información.	**IMPLEMENTADO**	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO	21.1
					POLITICA SI	3.0 - 8.0
					REGLAMENTO SI	1.0 - 8.0 , 20-a, 20-b, 20-c
					LOSEP	No Aplica
					COMERCIO	No Aplica

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION						
					ELECTRÓNICO	
					LOTAIP	No Aplica
A.6.1.2	Segregación de tareas	Control: Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.	SELECCIONADO	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO	3.4.5.15, 4.3.5.19
					POLITICA SI	3.0 - 8.0
					REGLAMENTO SI	No Aplica
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.6.1.3	Contacto con las autoridades	Control: Se debe mantener contactos apropiados con las autoridades pertinentes	IMPLEMENTADO	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO	21.1, 21.2
					POLITICA SI	3.0 - 8.0
					REGLAMENTO SI	1.0 - 8.0
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.6.1.4	Contacto con grupos de interés especial	Control: Mantener los contactos apropiados con grupos de interés especial, otros foros especializados en seguridad de la información y asociaciones de profesionales	SELECCIONADO	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO	21.1, 21.2
					POLITICA SI	3.0 - 8.0
					REGLAMENTO SI	1.0 - 8.0
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.6.1.5	Seguridad de la Información en gestión de proyectos	Control: Se debería contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización.	SELECCIONADO	Plan de seguridad del sistema o aplicación	NORMA RO	4.3.1.7
					POLITICA SI	3.0 - 8.0
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.6.2 Dispositivos para movilidad y trabajo Objetivo: Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.6.2.1	Política de uso de dispositivos para movilidad	Control: Se debe establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.	SELECCIONADO	Plan de seguridad del sistema o aplicación	NORMA RO	22.10
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	No Aplica
A.6.2.2	Teletrabajo	Control: Se debería desarrollar	SELECCIONADO	Protección del cableado	NORMA RO	22.11
					POLITICA SI	Falta Incluir

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION						
		e implantar una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo.		estructurado y suministros eléctricos	REGLAMENTO SI	13-e
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-5 muestra el enunciado de aplicabilidad para el dominio de Seguridad Ligada a los Recursos.

Tabla 3-5: Enunciado de aplicabilidad – Seguridad ligada a los recursos

A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS						
A.7.1 Antes de la contratación laboral Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y que su perfil es adecuado para los roles que se les considera, con lo cual reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.7.1.1	Investigación de Antecedentes	Control: Realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o terceros, de acuerdo a las leyes internas, reglamentos, ética y deben ser proporcionales a los requisitos del negocio.	**PARCIALMENTE IMPLEMENTADO**	Evaluación del personal, previo a la contratación, dentro de sus funciones y control de salida	NORMA RO	4.2.1
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	TODO
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.7.1.2	Términos y condiciones de contratación	Control: Como parte de su obligación contractual los empleados, contratistas y terceros deben firmar acuerdos sobre los términos y condiciones de su contrato laboral, en el que se debe establecer sus responsabilidades y las de la organización con respecto a la relación de seguridad de la información.	**PARCIALMENTE IMPLEMENTADO**	Evaluación del personal, previo a la contratación, dentro de sus funciones y control de salida	NORMA RO	4.2.1
					POLITICA SI	20-a
					REGLAMENTO SI	23-c
					LOSEP	TODO
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.7.2 Durante la contratación laboral Objetivo: Asegurar que los empleados, contratistas y terceros estén conscientes de las amenazas y vulnerabilidades respecto a la seguridad de la			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	

A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS						
información, sus responsabilidades y deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano						
A.7.2.1	Responsabilidades de la gestión	Control: La dirección debe exigir que los empleados contratistas y tercero apliquen la seguridad según la política y los procedimientos establecidos por la organización.	**PARCIALMENTE IMPLEMENTADO**	Evaluación del personal, previo a la contratación, dentro de sus funciones y control de salida	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.2.2 Falta Incluir Falta Incluir TODO No Aplica No Aplica
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Control: Todos los empleados de la organización y cuando apliquen contratistas y terceros deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.	**IMPLEMENTADO**	Capacitación técnica y en seguridad	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.2.2, 4.3.5.25,4.3.5. 26, 21.3 19 23-a, 23-b TODO No Aplica No Aplica
A.7.2.3	Proceso disciplinario	Control: Debe existir un proceso disciplinario formal y comunicado para los empleados que hayan cometido algún incumplimiento en los controles y políticas de la seguridad.	**SELECCIONADO**	Evaluación del personal, previo a la contratación, dentro de sus funciones y control de salida	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.2.2 37, 40 Falta Incluir TODO 57, 58, 59, 60, 61,62,63,64
A.7.3 Cese o cambio de funciones Objetivo: Asegurar que los empleados, contratistas y terceros cuando salen de la organización o cambian su contrato se realice de una forma ordenada y controlando los accesos.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL** **CRITERIO DE SEGURIDAD**	**LEGALES**	
A.7.3.1	Cese o cambio de puesto de trabajo	Control: Los derechos de accesos de todos los empleados, contratistas o terceros y a los servicios de procesamiento de información se deben retirar al finalizar su contratación laboral, contrato o acuerdo o se deben ajustar después del cambio. Incluye este proceso devolución de activos y evaluación de responsabilidades.	**PARCIALMENTE IMPLEMENTADO**	Evaluación del personal, previo a la contratación, dentro de sus funciones y control de salida	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.2.3 Falta Incluir Falta Incluir TODO No Aplica No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-6 muestra el enunciado de aplicabilidad para el dominio de Gestión de Activos

Tabla 3-6: Enunciado de aplicabilidad – Gestión de Activos

A.8 GESTION DE ACTIVOS						
A.8.1 Responsabilidad sobre los activos Objetivo: Identificar los activos en la organización y definir las responsabilidades para una protección adecuada.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.8.1.1	Inventario de Activos	Control: Todos los activos deben estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.	**PARCIALMENTE IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.1 Falta Incluir 14-a No Aplica No Aplica TODO
A.8.1.2	Propiedad de los Activos	Control: Toda la información y los activos asociados con los servicios de procesamiento de información deben ser propiedad de una parte designada de la organización.	**PARCIALMENTE IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.1 Falta Incluir Falta Incluir No Aplica No Aplica TODO
A.8.1.3	Uso aceptable de los activos	Control: Identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.	**SELECCIONADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.1, 22.4 12, 35 14-i, 21-d, 24-b No Aplica 2,3, 5, 6, 7,8, 9,19, 22, 57, 58, 59, 60, 61,62,63,64 TODO
A.8.1.4	Devolución de los activos	Control: Implementar un proceso formal para la devolución de los activos cuando los empleados, contratistas y proveedores hayan salido de la institución o se haya realizado	**PARCIALMENTE IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.1 Falta Incluir Falta Incluir No Aplica No Aplica TODO

A.8 GESTION DE ACTIVOS						
		cambio de funciones, con el objeto de preservar los activos de la organización.				
A.8.2 Clasificación de la Información Objetivo: Asegurar que se aplica un nivel de protección adecuado a la información.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.8.2.1	Directrices de clasificación	Control: La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.	**IMPLEMENTADO**	Distribución y etiquetado de información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.2 13,14,15,16,17 14-a, 14-b, 14c, 14-d, 14e No Aplica 5, 7, 21 TODO
A.8.2.2	Etiquetado y manipulación de la información	Control: Desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.	**SELECCIONADO**	Distribución y etiquetado de información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.1 18 14-a, 14-b, 14c, 14-d, 14e No Aplica 5,7, 21 TODO
A.8.2.3	Manipulación de activos	Control: Debe existir un proceso formal para el uso de los activos por parte de los empleados, contratistas y proveedores acorde a los procedimientos establecidos para manejo de la información y su etiquetado.	**PARCIALMENTE IMPLEMENTADO**	Distribución y etiquetado de información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.6 18 14-a, 14-b, 14c, 14-d, 14e No Aplica 2,3, 5, 6, 7,8, 21,22-d TODO
A.8.3 Manejo de los soportes de almacenamiento Objetivo: Evitar la divulgación, modificación, retiro o destrucción de activos no autorizados y la interrupción en las actividades de negocio.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.8.3.1	Gestión de soportes extraíbles	Control: Debe existir un proceso formal para la gestión de medios removibles	**PARCIALMENTE IMPLEMENTADO**	Procedimientos de mantenimiento externo y de transporte para respaldos	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.2 36,37 Falta Incluir No Aplica No Aplica No Aplica
A.8.3.2	Eliminación de soportes	Control: Cuando ya no se requieran estos medios, su	**SELECCIONADO**	Procedimientos de mantenimiento externo y de	NORMA RO POLITICA SI REGLAMENTO	22.3 31-b 14-f

A.8 GESTION DE ACTIVOS						
		eliminación se debe hacer de forma segura y sin riesgo, utilizando procedimientos formales.		transporte para respaldos	SI	
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	22-d
					LOTAIP	No Aplica
A.8.3.3	Soportes Físicos en Tránsito	Control: Establecer políticas, procedimientos y controles formales para proteger la información que se encuentre en tránsito independiente del medio de transmisión.	SELECCIONADO	Procedimientos de mantenimiento externo y de transporte para respaldos	NORMA RO	22.10, 22.14
					POLITICA SI	31-c, 37
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-7 muestra el enunciado de aplicabilidad para el dominio de Control de Accesos.

Tabla 3-7: Enunciado de aplicabilidad – Control de Accesos

A.9 CONTROL DE ACCESOS						
A.9.1 Requisitos del negocio para el control de acceso Objetivo: Mantener procesos establecidos para el control de acceso de usuarios acorde a las funciones desempeñadas dentro de la institución y bajo un procedimiento establecido.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar las políticas de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.	PARCIALMENTE IMPLEMENTADO	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO	4.3.5.7, 4.3.5.11, 4.3.5.12, 4.3.5.13, 4.3.5.14, 4.3.5.23, 4.3.5.29, 4.3.8.6,4.3.8.7, 4.3.8.9,4,3,8.1 0,4.3.8.11
					POLITICA SI	24-a, 24-b, 24-c
					REGLAMENTO SI	12, 12-g, 13-b
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	9,10
					LOTAIP	No Aplica
A.9.1.2	Control de acceso a las redes y servicios asociados	Control: Los usuarios sólo deben tener acceso a	PARCIALMENTE IMPLEMENTADO	Definición de procedimientos de control de acceso físico o	NORMA RO	4.3.8.8, 22.7
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	13-a, 24-a

A.9 CONTROL DE ACCESOS						
		los servicios para cuyo uso están específicamente autorizados .		digital	LOSEP COMERCIO ELECTRÓNICO LOTAIP	No Aplica 2,3, 5, 6, 7, 9,10 No Aplica
A.9.2 Gestión de acceso al usuario Objetivo: Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro del información de los servicios de procesamiento de información.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL** **CRITERIO DE SEGURIDAD**	**LEGALES**	
A.9.2.1	Gestión de altas/bajas en el registro de usuarios	Control: Debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.	**PARCIALMENTE IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.11, 22.12 Falta Incluir 13-c No Aplica No Aplica No Aplica
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Control: Restringir y controlar la asignación y uso de privilegios.	**PARCIALMENTE IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.11, 22.12 Falta Incluir 13-c No Aplica No Aplica No Aplica
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	Control: Restringir y controlar de forma específica los derechos de acceso con privilegios especiales.	**SELECCIONADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.11, 22.12 Falta Incluir 13-c, 13-j No Aplica No Aplica No Aplica
A.9.2.4	Gestión de información confidencial de autentificación de usuarios	Control: Mantener un procedimiento formal para la asignación de permisos sobre información acorde al tipo de clasificación de la misma.	**PARCIALMENTE IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.11, 22.12 Falta Incluir 12-e, 12-f No Aplica No Aplica No Aplica
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Control: La dirección debe establecer un procedimiento formal de revisión periódica	**PARCIALMENTE IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o	NORMA RO POLITICA SI REGLAMENTO SI LOSEP	22.11, 22.12 Falta Incluir 24-f No Aplica

A.9 CONTROL DE ACCESOS						
		de los derechos de acceso de los usuarios.		funciones de la persona	COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.9.2.6	Retirada o adaptación de los derechos	Control: Debe existir un procedimiento formal que establezca la retirada de permisos y recursos del personal o terceros, al momento de su salida o cambio de funciones en la institución.	**PARCIALMENTE IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO	22.11, 22.12
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	24-c, 24-d
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.9.3 Responsabilidad del usuario Objetivo: Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.9.3.1	Uso de la información confidencial para la autentificación	Control: Debe establecer procedimientos para el uso adecuado y protección de la información confidencial utilizada para autenticación del usuario. Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.	**IMPLEMENTADO**	Controles de seguridad personal, mínimos privilegios y acorde al cargo o funciones de la persona	NORMA RO	4.3.5.7, 4.3.5.11, 4.3.5.12, 4.3.5.13, 4.3.5.14, 4.3.5.23, 4.3.5.29, 4.3.8.6,4.3.8.7, 4.3.8.9,4,3,8.10,4.3.8.11
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	12-e, 12-f
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.9.4 Control de acceso a sistemas y aplicaciones Objetivo: Evitar el acceso no autorizado a servicios en la red.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.9.4.1	Restricción de accesos a la información	Control: Restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los	**PARCIALMENTE IMPLEMENTADO**	Identificación de forma única a usuarios, procesos y recursos de información	NORMA RO	22.11
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	12-e, 12-f, 24-b
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica

A.9 CONTROL DE ACCESOS						
		usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.			LOTAIP	No Aplica
A.9.4.2	Procedimientos seguros del inicio de sesión	Control: Controlar que el acceso a servicios de información solo pueda ser realizado a través de una conexión segura.	**IMPLEMENTADO**	Identificación de forma única a usuarios, procesos y recursos de información	NORMA RO	4.3.5.7, 4.3.5.11, 4.3.5.12, 4.3.5.13, 4.3.5.14, 4.3.5.23, 4.3.5.29, 4.3.8.6,4.3.8.7, 4.3.8.9,4,3,8.10,4.3.8.11
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	12-e, 12-f, 24-b
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.9.4.3	Gestión de contraseñas de usuario	Control: La asignación de contraseñas se debe controlar a través de un proceso formal de gestión.	**IMPLEMENTADO**	Identificación de forma única a usuarios, procesos y recursos de información	NORMA RO	4.3.5.7, 4.3.5.11, 4.3.5.12, 4.3.5.13, 4.3.5.14, 4.3.5.23, 4.3.5.29, 4.3.8.6,4.3.8.7, 4.3.8.9,4,3,8.10,4.3.8.11
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	12-b, 12-c, 23-d
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.9.4.4	Uso de herramientas de administración de sistemas	Control: Controlar y restringir en caso exista y aplicase herramientas de administración que puedan anular o controlar los sistemas o aplicaciones.		Garantizar la seguridad del medio ambiente (detectores de humo)	NORMA RO	4.3.4
			IMPLEMENTADO		POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.9.4.5	Control de acceso al código fuente de los programas	Control: Deben existir procedimientos formales que restrinjan el acceso al código fuente solo al personal de	**PARCIALMENTE IMPLEMENTADO**	Identificación y Autentificación	NORMA RO	4.3.6
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica

A.9 CONTROL DE ACCESOS						
		desarrollo y que su acceso pueda ser controlado y monitoreado.			LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-8 muestra el enunciado de aplicabilidad para el dominio de Cifrado.

Tabla 3-8: Enunciado de aplicabilidad – Cifrado

A.10 CIFRADO						
A.10.1 Controles Criptográficos Objetivo: Proteger la confidencialidad, autenticidad e integridad de la información, por medios criptográficos.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.10.1.1	Política de uso de los controles criptográficos	Control: Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	SELECCIONADO	Administración de claves criptográficas	NORMA RO	4.3.5.22, 22.14
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	16-a
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.10.1.2	Gestión de claves	Control: Mantener un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas por parte de la organización.	SELECCIONADO	Administración de claves criptográficas	NORMA RO	4.3.8.1
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-9 muestra el enunciado de aplicabilidad para el dominio de Seguridad Física y Ambiental

Tabla 3-9: Enunciado de aplicabilidad – Seguridad Física y Ambiental

A.11 SEGURIDAD FISICA Y AMBIENTAL						
A.11.1 Áreas Seguras Objetivo: Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.11.1.1	Perímetro de	Control:	NO	Continuidad del	NORMA RO	4.3.4.4

A.11 SEGURIDAD FISICA Y AMBIENTAL						
	Seguridad física	Utilizar perímetros de seguridad (barreras tales como paredes, puestas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.	SELECCIONADO	negocio	POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	30 19-a No Aplica No Aplica No Aplica
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	IMPLEMENTADO	Continuidad del negocio	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.4.4 30 19-b, 19-c, 19-e No Aplica No Aplica No Aplica
A.11.1.3	Seguridad de oficinas, despachos y recursos	Control: Diseñar y aplicar la seguridad física para oficinas, despachos y recursos.	PARCIALMENTE IMPLEMENTADO	Continuidad del negocio	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.4.4 Falta Incluir 19-f No Aplica No Aplica No Aplica
A.11.1.4	Protección contra las amenazas externas y ambientales	Control: Diseñar y aplicar la protección física contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	PARCIALMENTE IMPLEMENTADO	Control de las condiciones ambientales (humedad y temperatura)	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.4 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.11.1.5	El trabajo en áreas seguras	Control: Diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	NO SELECCIONADO	Proporcionar seguridad física específica (sensores de movimiento, CCTV, etc.)	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.4 Falta Incluir 19-d No Aplica No Aplica No Aplica
A.11.1.6	Áreas de acceso público, carga y descarga	Control: Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no	NO SELECCIONADO	Continuidad del negocio	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO	4.3.2.1, 4.3.4.6, 4.3.4 Falta Incluir Falta Incluir No Aplica No Aplica

A.11 SEGURIDAD FISICA Y AMBIENTAL						
		autorizado a las instalaciones se deben controlar y, si es de posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.			LOTAIP	No Aplica
A.11.2 Seguridad de los equipos Objetivo: Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.11.2.1	Emplazamiento y protección de equipos	Control: Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno y las oportunidades de acceso no autorizado.	**PARCIALMENTE IMPLEMENTADO**	Protección de estaciones de trabajo, portátiles y computadores personales	NORMA RO	4.3.4, 4.3.5.1, 4.3.4
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.11.2.2	Instalaciones de suministro	Control: Los equipos deben estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	**IMPLEMENTADO**	Protección de estaciones de trabajo, portátiles y computadores personales	NORMA RO	4.3.4
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.11.2.3	Seguridad de cableado	Control: El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debe estar protegido contra interceptaciones o daños.	**IMPLEMENTADO**	Protección del cableado estructurado y suministros eléctricos	NORMA RO	4.3.4
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.11.2.4	Mantenimiento de los equipos	Control: Los equipos deben recibir mantenimiento adecuado para asegurar su continuidad e integridad.	**PARCIALMENTE IMPLEMENTADO**	Protección de estaciones de trabajo, portátiles y computadores personales	NORMA RO	4.3.4, 4.3.4, 4.3.4
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.11.2.5	Salida de activos fuera de las dependencias de la organización	Control: Mantener un procedimiento de salida de los activos teniendo en cuenta los diferentes	**SELECCIONADO**	Protección de estaciones de trabajo, portátiles y computadores personales	NORMA RO	4.3.4
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica

A.11 SEGURIDAD FISICA Y AMBIENTAL						
		riesgos de trabajar fuera de las instalaciones de la organización.			COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Control: Suministrar seguridad para los equipos y activos fuera de las instalaciones teniendo en cuenta los riesgos y la clasificación de los activos al trabajar fuera de las instalaciones de la organización.	SELECCIONADO	Protección de estaciones de trabajo, portátiles y computadores personales	NORMA RO	4.3.4
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	Control: Verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.	SELECCIONADO	Protección de estaciones de trabajo, portátiles y computadores personales	NORMA RO	4.3.4
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.11.2.8	Equipo informático de usuario desatendido	Control: Los usuarios deben asegurar de que los equipos no supervisados cuentan con la protección adecuada.	SELECCIONADO	Protección de estaciones de trabajo, portátiles y computadores personales	NORMA RO	4.3.8.6
					POLITICA SI	21-b
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Control: Adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.	PARCIALMENTE IMPLEMENTADO	Protección de estaciones de trabajo, portátiles y computadores personales	NORMA RO	22.1, 22.4
					POLITICA SI	31-a
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-10 muestra el enunciado de aplicabilidad para el dominio de Seguridad en la Operativa.

Tabla 3-10: Enunciado de aplicabilidad – Seguridad en la Operativa

A.12 SEGURIDAD EN LA OPERATIVA						
A.12.1 Responsabilidades y procedimientos de operación Objetivo: Asegurar la operación correcta y segura de los servicios de procesamiento de información			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.12.1.1	Documentación de procedimientos de operación	Control: Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.	**PARCIALMENTE IMPLEMENTADO**	Configuración de la seguridad en los sistemas tecnológicos de la información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.4.1 Falta Incluir 21-d No Aplica No Aplica No Aplica
A.12.1.2	Gestión de cambios	Control: Controlar los cambios en los servicios y los sistemas de procesamiento de información.	**PARCIALMENTE IMPLEMENTADO**	Configuración de la seguridad en los sistemas tecnológicos de la información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.4.3, 22.5 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.12.1.3	Gestión de capacidades	Control: Monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.	**PARCIALMENTE IMPLEMENTADO**	Configuración de la seguridad en los sistemas tecnológicos de la información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.4.2 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	Control: Las instalaciones de desarrollo, ensayo y operación deben estar separadas para reducir los riesgos de acceso o cambios no autorizados.	**PARCIALMENTE IMPLEMENTADO**	Configuración de la seguridad en los sistemas tecnológicos de la información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.4.4 Falta Incluir 14-i No Aplica No Aplica No Aplica
A.12.2 Protección contra código malicioso Objetivo: Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	

A.12 SEGURIDAD EN LA OPERATIVA						
A.12.2.1	Controles contra código malicioso	Control: Implementar de controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como los procedimientos apropiados de concientización de los usuarios.	SELECCIONADO	Control de Virus o Vulnerabilidades técnicas	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.5.6 Falta Incluir 13-g, 21-c, 21-b No Aplica No Aplica No Aplica
A.12.3 Copias de seguridad Objetivo: Alcanzar un grado de protección deseado contra la pérdida de datos.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL** **CRITERIO DE SEGURIDAD**	**LEGALES**	
A.12.3.1	Copias de seguridad de la información	Control: Realizar copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo al procedimiento de respaldo acordada.	**PARCIALMENTE IMPLEMENTADO**	Procedimientos de respaldos de información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.5.2 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.12.4 Registro de actividad y supervisión Objetivo: Registrar los eventos relacionados con la seguridad de la información y generar evidencias.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL** **CRITERIO DE SEGURIDAD**	**LEGALES**	
A.12.4.1	Registro y gestión de eventos de actividad	Control: Elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.	**PARCIALMENTE IMPLEMENTADO**	Protección de las instalaciones tecnológicas	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.5.18 Falta Incluir 25-f, 25-g, 26-a No Aplica No Aplica No Aplica
A.12.4.2	Protección de los registros de información	Control: Los servicios y la información de la actividad de registro se deben proteger contra el acceso o la manipulación no autorizada.	**PARCIALMENTE IMPLEMENTADO**	Protección de las instalaciones tecnológicas	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	4.3.5.1, 4.3.5.2 21-b 21-b No Aplica No Aplica
A.12.4.3	Registros de actividad del administrador y operador del sistema	Control: Se deben registrar las actividades tanto del operador como	SELECCIONADO	Protección de las instalaciones tecnológicas	NORMA RO POLITICA SI REGLAMENTO SI	4.3.12, 4.3.8.15, 4.3.8.16 Falta Incluir No Aplica

A.12 SEGURIDAD EN LA OPERATIVA						
		del administrador del sistema.		Protección de las instalaciones tecnológicas	LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.	IMPLEMENTADO		NORMA RO	4.3.5.17
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	15-e
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.12.5 Control de software en explotación Objetivo: Garantizar la integridad de los sistemas operacionales para la organización.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.12.5.1	Instalación del software en sistemas en producción	Control: Implementar procedimientos para controlar la instalación de software en sistemas operacionales.	IMPLEMENTADO	Control de Virus o Vulnerabilidad técnicas	NORMA RO	22.9
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	17-c, 21-b
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.12.6 Gestión de la vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.	SELECCIONADO	Control de Virus o Vulnerabilidades técnicas	NORMA RO	4.3.5.8,4.3.8.2, 4.3.8.3
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	17-d
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.12.6.2	Restricciones en la instalación de software	Control: Controlar la realización de modificación de los paquetes de software, limitarlas a los cambios necesarios, y	IMPLEMENTADO	Control de Virus o Vulnerabilidades técnicas	NORMA RO	4.3.5.16, 22.9
					POLITICA SI	22, 23
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica

A.12 SEGURIDAD EN LA OPERATIVA						
		todos los cambios se deben controlar estrictamente.			LOTAIP	No Aplica
A.12.7 Consideraciones de las auditorias de los sistemas de información Objetivo: Minimizar el impacto de actividades de auditoría en los sistemas operacionales			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.12.7.1	Controles de auditoría de los sistemas de información	Control: Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.	**PARCIALMENTE IMPLEMENTADO**	Auditoría del sistema	NORMA RO	4.3.5.27, 22.8, 22.13
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	25-a
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-11 muestra el enunciado de aplicabilidad para el dominio de Seguridad en las Telecomunicaciones

Tabla 3-11: Enunciado de aplicabilidad - Seguridad en las telecomunicaciones

A.13 SEGURIDAD EN LAS TELECOMUNICACIONES						
A.13.1 Gestión en las seguridades en las redes. Objetivo: Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.13.1.1	Controles de red	Control: Se debe administrar y controlar las redes para proteger la información en sistemas y aplicaciones.	**IMPLEMENTADO**	Protección del cableado estructurado y suministros eléctricos	NORMA RO	4.3.4
					POLITICA SI	25,26
					REGLAMENTO SI	13-f
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	Control: Se debe identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se	**IMPLEMENTADO**	Protección del cableado estructurado y suministros eléctricos	NORMA RO	4.3.5.3, 4.3.5.4, 4.3.8.3, 4.3.8.4, 4.3.8.5
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	13-k, 21-c, 21-d, 21-e
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	8
					LOTAIP	No Aplica

A.13 SEGURIDAD EN LAS TELECOMUNICACIONES						
		entregan de manera interna o están externalizados.				
A.13.1.3	Segregación de redes	Control: En las redes se deben separar los grupos de servicios de información, usuarios y sistemas de información.	SELECCIONADO	Protección del cableado estructurado y suministros eléctricos	NORMA RO	4.3.7
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.13.2 Intercambio de información con partes externas Objetivo: Mantener la seguridad de la información que transfiere un organización internamente o con entidades externas.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.13.2.1	Políticas y procedimientos de intercambio de información	Control: Deben establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.	SELECCIONADO	Protección de las Comunicaciones	NORMA RO	4.3, 20.2.10
					POLITICA SI	27
					REGLAMENTO SI	14-g
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	No Aplica
A.13.2.2	Acuerdos de intercambio	Control: Deben establecerse acuerdos para el intercambio de información y del software entre la organización y los terceros.	SELECCIONADO	Protección de las Comunicaciones	NORMA RO	4.3
					POLITICA SI	28
					REGLAMENTO SI	14-g
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	9
					LOTAIP	No Aplica
A.13.2.3	Mensajería electrónica	Control: La información que sea objeto de mensajería electrónica debe estar adecuadamente protegida.	PARCIALMENTE IMPLEMENTADO	Protección de las Comunicaciones	NORMA RO	4.3.5
					POLITICA SI	27
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	No Aplica
A.13.2.4	Acuerdos de confidencialidad y secreto	Control: Se debe identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.	IMPLEMENTADO	Protección de las Comunicaciones	NORMA RO	20
					POLITICA SI	27
					REGLAMENTO SI	14-h
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-12 muestra el enunciado de aplicabilidad para el dominio de Seguridad en los Sistemas de Información

Tabla 3-12: Enunciado de aplicabilidad - Seguridad en los Sistemas de Información

A.14 SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN.						
A.14.1 Requisitos de seguridad de los sistemas de información Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para aquellos que proporcionan servicios en redes públicas			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.14.1.1	Análisis y especificación de los requisitos de seguridad	Control: En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad	**PARCIALMENTE IMPLEMENTADO**	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO	4.3.3.2, 4.3.5.28, 22.15
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes publicas	Control: La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.	**PARCIALMENTE IMPLEMENTADO**	Configuración de la seguridad en los sistemas tecnológicos de la información	NORMA RO	4.3.8,4.3.5, 20.2.10
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	13-f
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.1.3	Protección de las transacciones por redes telemáticas	Control: La información en transacciones de servicios de aplicación se debe proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.	**SELECCIONADO**	Protección de las Comunicaciones	NORMA RO	4.3.8, 4.3.7
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.2 Seguridad en los procesos de desarrollo y soporte Objetivo: Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.14.2.1	Política de	Control:	**SELECCIONADO**	Control de	NORMA RO	4.3.3.1

A.14 SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN.						
	desarrollo seguro de software	Se debe establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.		pruebas de integridad	POLITICA SI	Falta Incluir
					REGLAMENTO SI	15-d
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.2.2	Procedimientos de control de cambios en los sistemas	Control: En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.	**PARCIALMENTE IMPLEMENTADO**	Control de pruebas de integridad	NORMA RO	4.3.3.7 , 4.3.3.8
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	15-a, 15-b, 15-c
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Control: Las aplicaciones críticas para el negocio se deben revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.	**SELECCIONADO**	Control de pruebas de integridad	NORMA RO	4.3.3.3
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.2.4	Análisis y especificación de los requisitos de seguridad	Control: En las declaraciones de los requisitos de negocio para los nuevos sistemas de información, o para mejoras de los sistemas de información ya existentes, se deben especificar los requisitos de los controles de seguridad.	**SELECCIONADO**	Control de pruebas de integridad	NORMA RO	4.3.4.7, 4.3.6, 4.3.7
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	Control: Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.	**SELECCIONADO**	Control de pruebas de integridad	NORMA RO	4.3.3.5, 22.15
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.2.6	Seguridad en entornos de desarrollo	Control: Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e	**PARCIALMENTE IMPLEMENTADO**	Control de pruebas de integridad	NORMA RO	4.3.3.4
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	14-i
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica

A.14 SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN.						
		integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.			LOTAIP	No Aplica
A.14.2.7	Externalización del desarrollo del software	Control: La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.	**PARCIALMENTE IMPLEMENTADO**	Control de pruebas de integridad	NORMA RO	20.1, 20.2, 4.3.3, 4.3.4.8, 4.3.6
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Control: Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.	**PARCIALMENTE IMPLEMENTADO**	Control de pruebas de integridad	NORMA RO	4.3.3.1
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.2.9	Pruebas de aceptación	Control: Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.	**PARCIALMENTE IMPLEMENTADO**	Control de pruebas de integridad	NORMA RO	4.3.3.6
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.14.3 Datos de prueba Objetivo: Proteger los datos que se utilizan para procesos de pruebas.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.14.3.1	Protección de los datos utilizados en pruebas	Control: Los datos de prueba se deben seleccionar con cuidado y deben estar protegidos y controlados.	**PARCIALMENTE IMPLEMENTADO**	Control de pruebas de integridad	NORMA RO	4.3.3.9, 4.3.5.19
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	14-i
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-13 muestra el enunciado de aplicabilidad para el dominio de Relaciones con Proveedores

Tabla 3-13: Enunciado de aplicabilidad - Relaciones con Proveedores

A.15 RELACIONES CON PROVEEDORES						
A.15.1 Seguridad de la información en las relaciones con proveedores Objetivo: Controlar el acceso de la información de la organización por parte de terceros que acceden a información sensible de la organización.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.15.1.1	Política de seguridad de la información para proveedores.	Control: Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.	**SELECCIONADO**	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	9 Falta Incluir 13-b No Aplica No Aplica No Aplica
A.15.1.2	Tratamiento del riesgo dentro de acuerdo de proveedores.	Control: Identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.	**SELECIONADO**	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	10 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	Control: Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.	**SELECCIONADO**	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	11 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.15.2 Gestión de la prestación del servicio por proveedores Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros. La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	

A.15 RELACIONES CON PROVEEDORES						
satisfacer todos los requerimientos acordados con terceras personas.						
A.15.2.1	Supervisión y revisión de los servicios por terceros	Control: Los servicios, informes y registros proporcionados por un tercero deben ser objeto de supervisión y revisión periódicas, y también deben llevarse a cabo auditorias periódicas.	SELECCIONADO	Revisión Periódica de Controles de Seguridad	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	10 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	Control: Se deben gestionar los cambios en la provisión de los servicios, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas del negocio afectados así como la reevaluación de los riesgos	SELECCIONADO	Revisión Periódica de Controles de Seguridad	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	11 Falta Incluir 17-a No Aplica No Aplica No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-14 muestra el enunciado de aplicabilidad para el dominio de Gestión de Incidentes en la Seguridad de la Información

Tabla 3-14: Enunciado de aplicabilidad - Gestión de Incidentes en la Seguridad de la Información

A.16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION						
A.16.1 Gestión de incidentes de seguridad de la información y mejoras **Objetivo:** Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.16.1.1	Responsabilidades y procedimientos	Control: Establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SELECCIONADO	Capacidad de respuesta a incidentes	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.16 21-a 25-c, 26-b No Aplica 53, 54, 55, 56, 57 No Aplica
A.16.1.2	Notificación de los eventos de seguridad de la	Control: Los eventos de	SELECCIONADO	Capacidad de respuesta a	NORMA RO POLITICA SI	22.16 20-c

A.16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION						
	información	seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.		incidentes	REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	24-e, 25-c, 26-c No Aplica No Aplica No Aplica
A.16.1.3	Notificación de puntos débiles de la seguridad	Control: Exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.	SELECCIONADO	Capacidad de respuesta a incidentes	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.16 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	Control: Valoración de eventos de seguridad de la información y toma de decisiones: Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.	SELECCIONADO	Capacidad de respuesta a incidentes	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.16 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.16.1.5	Respuesta a los incidentes de seguridad	Control: Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.	SELECCIONADO	Capacidad de respuesta a incidentes	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.16 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control: Existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.	SELECCIONADO	Capacidad de respuesta a incidentes	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO ELECTRÓNICO LOTAIP	22.16 Falta Incluir Falta Incluir No Aplica No Aplica No Aplica
A.16.1.7	Recopilación de evidencias	Control: Cuando una acción de seguimiento contra una persona u	SELECCIONADO	Capacidad de respuesta a incidentes	NORMA RO POLITICA SI REGLAMENTO SI LOSEP COMERCIO	22.16 Falta Incluir Falta Incluir No Aplica No Aplica

A.16 GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION						
		organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecida en la jurisdicción pertinente.			ELECTRÓNICO	
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-15 muestra el enunciado de aplicabilidad para el dominio de Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

Tabla 3-15: Enunciado de aplicabilidad - Aspectos de Seguridad de la Información en la Gestión de la Continuidad de Negocio.

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO						
A.17.1 Continuidad de la seguridad de la información Objetivo: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: Desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	**SELECCIONADO**	Continuidad del negocio	NORMA RO	15.1, 15.2,15.3, 15.4
					POLITICA SI	29
					REGLAMENTO SI	18-a, 18-b, 18-c, 18-d
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.17.1.2	Implantación de la continuidad de la seguridad de la información	Control: Desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la	**SELECCIONADO**	Continuidad del negocio	NORMA RO	15.5,15.6,15.7 , 16.1 - 16.13
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DE NEGOCIO						
		información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.			LOTAIP	No Aplica
A.17.1.3	Verificación de la continuidad de la seguridad de la información	Control: Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.	SELECCIONADO	Continuidad del negocio	NORMA RO	15.2, 15.8
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.17.2 Redundancias Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de información.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	Control: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.	PARCIALMENTE IMPLEMENTADO	Mantener fuentes de energía alternas	NORMA RO	4.3.4.2, 4.3.4.12, 4.3.5
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

En la tabla 3-16 muestra el enunciado de aplicabilidad para el dominio de Cumplimiento

Tabla 3-16: Enunciado de aplicabilidad - Cumplimiento

A.18 CUMPLIMIENTO						
A.18.1 Cumplimiento de los requisitos legales y contractuales Objetivo: Evitar el incumplimiento de cualquier ley, obligaciones reglamentarias, estatales o contractuales y de cualquier requisito de seguridad.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.18.1.1	Identificación de la legislación aplicable	Control: Todos los requisitos legales, reglamentarios, estatales o contractuales, así	IMPLEMENTADO	Asignación de responsabilidades y separación de obligaciones para Seguridad de la	NORMA RO	22.17
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	TODO

A.18 CUMPLIMIENTO						
		como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización.		Información	COMERCIO ELECTRÓNICO	2,3,4, 45, 46, 47
					LOTAIP	TODO
A.18.1.2	Derechos de propiedad intelectual (DPI)	Control: Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.	NO SELECCIONADO	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO	22.17
					POLITICA SI	33, 34
					REGLAMENTO SI	Falta Incluir
					LOSEP	TODO
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	No Aplica
A.18.1.3	Protección de los registros de la organización	Control: Los registros importantes se deben proteger contra la pérdida, destrucción y falsificación, de acuerdo con los requisitos estatales, reglamentarios, contractuales y del negocio.	PARCIALMENTE IMPLEMENTADO	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO	22.17
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	TODO
					COMERCIO ELECTRÓNICO	No Aplica
					LOTAIP	TODO
A.18.1.4	Protección de datos y privacidad de la información personal	Control: Garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.	PARCIALMENTE IMPLEMENTADO	Asignación de responsabilidades y separación de obligaciones para Seguridad de la Información	NORMA RO	22.17
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	TODO
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	TODO
A.18.1.5	Regulación de los controles criptográficos	Control: Utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.	SELECCIONADO	Administración de claves criptográficas	NORMA RO	22.17
					POLITICA SI	Falta Incluir
					REGLAMENTO SI	Falta Incluir
					LOSEP	No Aplica
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	No Aplica
A.18.2 Revisiones de la seguridad de la información Objetivo: Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.			**DEFINICIÓN**	**JUSTIFICACION PARA LA SELECCIÓN DEL CONTROL**		
				CRITERIO DE SEGURIDAD	**LEGALES**	
A.18.2.1	Revisión independiente de la	Control: Los sistemas de	PARCIALMENTE IMPLEMENTADO	Revisión Periódica de	NORMA RO	22.18
					POLITICA SI	Falta Incluir

A.18 CUMPLIMIENTO						
	seguridad de la información	información se deben revisar periódicamente por un área independiente para determinar el cumplimiento y nivel de implementación de las normas de seguridad.		Controles de Seguridad	REGLAMENTO SI	25-d, 25-e
					LOSEP	TODO
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	TODO
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Control: Los sistemas de información deben evaluarse para determinar el cumplimiento con las normas y políticas vigentes de seguridad.	**PARCIALMENTE IMPLEMENTADO**	Revisión Periódica de Controles de Seguridad	NORMA RO	22.18
					POLITICA SI	37, 41
					REGLAMENTO SI	Falta Incluir
					LOSEP	TODO
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	TODO
A.18.2.3	Comprobación del cumplimiento	Control: Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de seguridad.	**PARCIALMENTE IMPLEMENTADO**	Revisión Periódica de Controles de Seguridad	NORMA RO	22.18
					POLITICA SI	20-b
					REGLAMENTO SI	Falta Incluir
					LOSEP	TODO
					COMERCIO ELECTRÓNICO	TODO
					LOTAIP	TODO

Fuente: Los autores. Se incluyó la lista de controles tomados del estándar ISO27001:2013, Enero/2015, http://www.iso27000.es/download/ControlesISO27001-2013.pdf. Último Acceso: Febrero 2015

3.4.1 Resumen del Enunciado de Aplicabilidad

En la tabla 3-17 se indica el resultado final de la selección de controles requeridos para la institución financiera.

Tabla 3-17: Tabla de Resumen del Enunciado de Aplicabilidad.

LITERAL	DETALLE	DEFINICION
5	**POLITICAS DE SEGURIDAD**	
5.1	***Directrices de la Dirección en Seguridad de la Información***	
5.1.1	Conjunto de políticas para la seguridad de la información	IMPLEMENTADO
5.1.2	Revisión de las políticas para la seguridad de la información	SELECCIONADO
6.	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION**	
6.1	***Organización interna***	
6.1.1	Asignación de responsabilidades para seguridad de la información	SELECCIONADO
6.1.2	Segregación de tareas	IMPLEMENTADO
6.1.3	Contacto con las autoridades	SELECCIONADO
6.1.4	Contacto con grupos de interés especial	IMPLEMENTADO
6.1.5	Seguridad de la información en la gestión de proyectos	SELECCIONADO
6.2	***Dispositivos para movilidad y teletrabajo***	

LITERAL	DETALLE	DEFINICION
6.2.1	Políticas de uso de dispositivos para movilidad	SELECCIONADO
6.2.2	Teletrabajo	SELECCIONADO
7.	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**	
7.1	***Antes de la contratación***	
7.1.1	Investigación de antecedentes	PARCIALMENTE IMPLEMENTADO
7.1.2	Términos y condiciones de contratación	PARCIALMENTE IMPLEMENTADO
7.2	***Durante la contratación***	
7.2.1	Responsabilidad de gestión	PARCIALMENTE IMPLEMENTADO
7.2.2	Concienciación, educación y capacitación en SI	IMPLEMENTADO
7.2.3	Proceso disciplinario	SELECCIONADO
7.3	***Cese o cambio de puesto de trabajo***	
7.3.1	Cese o cambio de puesto de trabajo	PARCIALMENTE IMPLEMENTADO
8.	**GESTION DE ACTIVOS**	
8.1	***Responsabilidad sobres los activos***	
8.1.1	Inventarios de activos	PARCIALMENTE IMPLEMENTADO
8.1.2	Propiedad de los activos	PARCIALMENTE IMPLEMENTADO
8.1.3	Uso aceptable de los activos	SELECCIONADO
8.1.4	Devolución de activos	PARCIALMENTE IMPLEMENTADO
8.2	***Clasificación de la información***	
8.2.1	Directrices de clasificación	IMPLEMENTADO
8.2.2	Etiquetado y manipulado de la información	SELECCIONADO
8.2.3	Manipulación de activos	PARCIALMENTE IMPLEMENTADO
8.3	***Manejo de los soportes de almacenamiento***	
8.3.1	Gestión de soportes extraíbles	PARCIALMENTE IMPLEMENTADO
8.3.2	Eliminación de soportes	SELECCIONADO
8.3.3	Soportes físicos en tránsito	SELECCIONADO
9.	**CONTROLES DE ACCESOS**	
9.1	***Requisitos de negocio para el control de accesos***	
9.1.1	Políticas de control de accesos	PARCIALMENTE IMPLEMENTADO
9.1.2	Control de acceso a las redes y servicios asociados	PARCIALMENTE

LITERAL	DETALLE	DEFINICION
		IMPLEMENTADO
9.2	***Gestión de acceso de usuario***	
9.2.1	Gestión de altas/bajas en el registro de usuarios	PARCIALMENTE IMPLEMENTADO
9.2.2	Gestión de los derechos de accesos asignados a usuarios	PARCIALMENTE IMPLEMENTADO
9.2.3	Gestión de los derechos de acceso con privilegios especiales	SELECCIONADO
9.2.4	Gestión de información confidencial de autentificación de usuarios	PARCIALMENTE IMPLEMENTADO
9.2.5	Revisión de los derechos de acceso de los usuarios	PARCIALMENTE IMPLEMENTADO
9.2.6	Retirada o adaptación de los derechos de acceso	PARCIALMENTE IMPLEMENTADO
9.3	***Responsabilidades del usuario***	
9.3.1	Uso de la información confidencial para la autentificación	IMPLEMENTADO
9.4	***Control de acceso a sistemas y aplicaciones***	
9.4.1	Restricción del acceso a la información	PARCIALMENTE IMPLEMENTADO
9.4.2	Procedimientos seguros de inicio de sesión	IMPLEMENTADO
9.4.3	Gestión de contraseñas de usuario	IMPLEMENTADO
9.4.4	Uso de herramientas de administración de sistemas	IMPLEMENTADO
9.4.5	Control de acceso al código fuentes de los programas	PARCIALMENTE IMPLEMENTADO
10.	**CIFRADO**	
10.1	***Controles criptográficos***	
10.1.1	Política de uso de los controles criptográficos	SELECCIONADO
10.1.2	Gestión de claves	SELECCIONADO
11.	**SEGURIDAD FISICA Y AMBIENTAL**	
11.1	***Áreas seguras***	
11.1.1	Perímetro de seguridad física	NO SELECCIONADO
11.1.2	Controles físicos de entrada	PARCIALMENTE IMPLEMENTADO
11.1.3	Seguridad de oficinas, despachos y recursos	PARCIALMENTE IMPLEMENTADO
11.1.4	Protección contra las amenazas externas y ambientales	PARCIALMENTE IMPLEMENTADO
11.1.5	El trabajo en áreas seguras	NO SELECCIONADO
11.1.6	Áreas de acceso público, carga y descarga	NO SELECCIONADO

LITERAL	DETALLE	DEFINICION
11.2	***Seguridad de los equipos***	
11.2.1	Emplazamiento y protección de equipos	PARCIALMENTE IMPLEMENTADO
11.2.2	Instalación de suministros	IMPLEMENTADO
11.2.3	Seguridad del cableado	IMPLEMENTADO
11.2.4	Mantenimiento de los equipos	PARCIALMENTE IMPLEMENTADO
11.2.5	Salida de activos fuera de las dependencias de la empresa	SELECCIONADO
11.2.6	Seguridad de los equipos y activos fuera de las instituciones	SELECCIONADO
11.2.7	Reutilización o retirada segura de dispositivos de almacenamientos	SELECCIONADO
11.2.8	Equipo informático de usuario desatendido	SELECCIONADO
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	PARCIALMENTE IMPLEMENTADO
12.	**SEGURIDAD EN LA OPERATIVA**	
12.1	***Responsabilidades y procedimientos de operación***	
12.1.1	Documentación de procedimientos de operación	PARCIALMENTE IMPLEMENTADO
12.1.2	Gestión de cambios	PARCIALMENTE IMPLEMENTADO
12.1.3	Gestión de capacidades	PARCIALMENTE IMPLEMENTADO
12.1.4	Separación de entornos de desarrollo, prueba y producción	PARCIALMENTE IMPLEMENTADO
12.2	***Protección contra código maliciosa***	
12.2.1	Controles para el código malicioso	SELECCIONADO
12.3	***Copias de seguridad***	
12.3.1	Copias de seguridad de la información	PARCIALMENTE IMPLEMENTADO
12.4	***Registro de actividad y supervisión***	
12.4.1	Registro y gestión de eventos de actividad	PARCIALMENTE IMPLEMENTADO
12.4.2	Protección de los registros de información	PARCIALMENTE IMPLEMENTADO
12.4.3	Registros de actividades del administrador y operador del sistema	SELECCIONADO
12.4.4	Sincronización de relojes	IMPLEMENTADO
12.5	***Controles del software en explotación***	
12.5.1	Instalación del software en sistemas en producción	IMPLEMENTADO
12.6	***Gestión de las vulnerabilidades técnicas***	
12.6.1	Gestión de las vulnerabilidades técnicas	SELECCIONADO

LITERAL	DETALLE	DEFINICION
12.6.2	Restricciones en la instalación del software	IMPLEMENTADO
12.7	***Consideraciones de las auditorias en los sistemas de información***	
12.7.1	Controles de auditoría de los sistemas de información	PARCIALMENTE IMPLEMENTADO
13.	**SEGURIDAD EN LAS TELECOMUNICACIONES**	
13.1	***Gestión de la seguridad en las redes***	
13.1.1	Controles de red	IMPLEMENTADO
13.1.2	Mecanismos de seguridad asociados a servicios en red	IMPLEMENTADO
13.1.3	Segregación de redes	SELECCIONADO
13.2	***Intercambio de información con partes externas***	
13.2.1	Políticas y procedimientos de intercambio de información	SELECCIONADO
13.2.2	Acuerdos de intercambio	SELECCIONADO
13.2.3	Mensajería electrónica	PARCIALMENTE IMPLEMENTADO
13.2.4	Acuerdos de confidencialidad y secreto	IMPLEMENTADO
14.	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION**	
14.1	***Requisitos de seguridad de los sistemas de información***	
14.1.1	Análisis y especificación de los requisitos de seguridad	PARCIALMENTE IMPLEMENTADO
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	PARCIALMENTE IMPLEMENTADO
14.1.3	Protección de las transacciones por redes telemáticas	SELECCIONADO
14.2	***Seguridad en los procesos de desarrollo y soporte***	
14.2.1	Política de desarrollo seguro de software	SELECCIONADO
14.2.2	Procedimientos de control de cambios en los sistemas	PARCIALMENTE IMPLEMENTADO
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SELECCIONADO
14.2.4	Restricciones a los cambios en los paquetes de software	SELECCIONADO
14.2.5	Uso de principio de ingeniería en protección de sistemas	SELECCIONADO
14.2.6	Seguridad en entornos de desarrollo	PARCIALMENTE IMPLEMENTADO
14.2.7	Externalización del desarrollo del software	PARCIALMENTE IMPLEMENTADO
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	PARCIALMENTE IMPLEMENTADO
14.2.9	Pruebas de aceptación	PARCIALMENTE IMPLEMENTADO
14.3	***Datos de prueba***	

LITERAL	DETALLE	DEFINICION
14.3.1	Protección de los datos utilizados en pruebas	PARCIALMENTE IMPLEMENTADO
15.	**RELACIONES CON SUMINISTRADORES**	
15.1	***Seguridad de la Información en las relaciones con suministradores***	
15.1.1	Política de seguridad de la información para proveedores	SELECCIONADO
15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	SELECCIONADO
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	SELECCIONADO
15.2	***Gestión de la prestación del servicio por suministradores***	
15.2.1	Supervisión y revisión de los servicios prestados por terceros	SELECCIONADO
15.2.2	Gestión de cambios en los servicios prestados por terceros	SELECCIONADO
16.	**GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION**	
16.1	***Gestión de incidentes de seguridad de la información y mejoras***	
16.1.1	Responsabilidad y procedimientos	SELECCIONADO
16.1.2	Notificación de los eventos de seguridad de la información	SELECCIONADO
16.1.3	Notificación de puntos débiles de la seguridad	SELECCIONADO
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	SELECCIONADO
16.1.5	Respuesta a los incidentes de seguridad	SELECCIONADO
16.1.6	Aprendizaje de los incidentes de seguridad de la información	SELECCIONADO
16.1.7	Recopilación de evidencias	SELECCIONADO
17.	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUDAD DEL NEGOCIO**	
17.1	***Continuidad de la seguridad de la información***	
17.1.1	Planificación de la continuidad de la seguridad de la información	SELECCIONADO
17.1.2	Implantación de la continuidad de la seguridad de la información	SELECCIONADO
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SELECCIONADO
17.2	***Redundancias***	
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	PARCIALMENTE IMPLEMENTADO
18.	**CUMPLIMIENTO**	
18.1	***Cumplimiento de los requisitos legales y contractuales***	
18.1.1	Identificación de la legislación aplicable	IMPLEMENTADO
18.1.2	Derechos de propiedad intelectual (DPI)	NO SELECCIONADO
18.1.3	Protección de los registros de la organización	PARCIALMENTE IMPLEMENTADO
18.1.4	Protección de datos y privacidad de la información personal	PARCIALMENTE IMPLEMENTADO
18.1.5	Regulación de los controles criptográficos	SELECCIONADO

LITERAL	DETALLE	DEFINICION
18.2	***Revisiones de la seguridad de la información***	
18.2.1	Revisión independiente de la seguridad	PARCIALMENTE IMPLEMENTADO
18.2.2	Cumplimiento de las políticas y normas de seguridad	PARCIALMENTE IMPLEMENTADO
18.2.3	Comprobación del cumplimiento	PARCIALMENTE IMPLEMENTADO

Fuente: Los autores.

3.5 PLAN DE ACCION CON RECOMENDACIONES PARA IMPLANTAR UN SGSI

En este capítulo se recogen claramente las responsabilidades de cada uno de los participantes en el proceso y establece los controles que permitan prevenir, detectar y responder a las amenazas priorizadas que están presentes en el sistema de la institución financiera.

3.5.1 PLAN DE ACCIÓN

Las actividades planteadas a realizar como parte del Plan de Acción correctivo en la institución financiera considera la criticidad relacionada al impacto para el negocio (alta, media o baja), así como la prioridad asignada para la realización de las actividades previstas.

La asignación de la prioridad se base en lo indicado en la tabla 3-18.

Tabla 3-18: Tabla de asignación de prioridad por tiempo

	**Actividad que deberían realizarse en forma inmediata – muy corto plazo (iniciar en un mes máximo)**
	Actividad que deberían realizarse en forma seguida – corto plazo. (iniciar entre uno y 3 meses)
	**Actividad que deberían realizarse en forma posterior – mediano plazo (iniciar en tres a seis meses)**

Fuente: Los autores. Quito. Enero/2015

En la tabla 3-19 se muestra el plan de acción del sistema de seguridad de la información.

Tabla 3-19: Tabla de Actividades del Plan de acción

PLAN DE ACCIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION						
ISO 27001:2013	**DEFICIENCIAS**	**OBJETIVOS A CUMPLIR**	**CRITICIDAD**	**PRIORIDAD**	**RESPONSABLE**	**TIEMPO**
A.5 Políticas de Seguridades	Falta de Lineamientos	Aprobar Manual	ALTO		Directorio	1 - 2 meses
A.6 Organización de seguridad de la información	Falta de Apoyo Gerencia	Definir Comité Seguridad	ALTO		Comité de Riesgos	1-2 meses
	Falta de Personal	Reforzar área de Seguridad			Jefatura de Seguridad	
	Falta de Presupuesto	Definir Presupuesto del área			Jefatura de Seguridad	
A.7 Seguridad en recursos humanos	Falta de Reglamento Disciplinario	Establecer procedimiento disciplinario	MEDIO		Talento Humano (TTHH)	3 - 5 meses
		Establecer control en el ingreso- salida del personal			Talento Humano	
		Curso de Inducción al Ingreso del Personal			TTHH y Jefe. de Seguridad	
		Establecer contratos y convenios de forma oportuna			Talento Humano	
A.8 Gestión de activos	Activos no Levantados	Actualización de activos	ALTO		Jefatura de Seguridad	2 - 3 meses
		Definir Responsables			Jefatura de Seguridad	
A.9 Control de acceso	Recursos y Administradores no definidos	Levantamiento de Recursos y responsables de Administración.	MEDIO		IT - Jefatura de Seguridad	3 - 5 meses
A.10 Cifrado	Establecer Controles	Política de Controles Criptográficos	BAJO		IT - Jefatura de Seguridad	6 - 8 meses
A.11 Seguridad física y ambiental	Falta de definición de funciones Seguridad Física	Control de acceso físico a la institución financiera	MEDIO		Seguridad Física	3 - 5 meses
		Política de escritorio limpio			Jefatura de Seguridad	
		Política para destrucción de documentación			Jefatura de Seguridad	
A.12 Seguridad Operativa	Falta de Controles de Información en movimiento	Adquisición Servidor de Archivos – Inactivación USB.	ALTO		IT - Jefatura de Seguridad	7 meses
A.13 Seguridad en Telecomunicaciones	Establecimiento de Procedimientos y Responsables	Depuración accesos a la red por personas y por equipos.	ALTO		IT - Jefatura de Seguridad	2 meses
		Definición de una política clara para uso de la red de invitados.			IT - Jefatura de Seguridad	

PLAN DE ACCIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION						
ISO 27001:2013	**DEFICIENCIAS**	**OBJETIVOS A CUMPLIR**	**CRITICIDAD**	**PRIORIDAD**	**RESPONSABLE**	**TIEMPO**
A.14 Adquisición, desarrollo y mantenimiento de sistemas	Segregación de Funciones y de áreas en TI	Definición de áreas y funciones específicas para realizar la segregación de accesos y ambientes. Faltan áreas independientes para la evaluación del requerimiento funcional y QA.	MEDIO		IT - Jefatura de Seguridad	12 meses
A.15 Relaciones con Proveedores	Establecer Proveedores Críticos	Levantamiento y evaluación proveedores críticos.	MEDIO		Negocio - Seguridad	8 meses
A.16 Gestión de incidentes de seguridad de la información	Falta de Manejo de Incidentes	Establecer un comité y procedimiento para manejo de incidentes de seguridad	ALTA		Jefatura de Seguridad	3 meses
A.17 Administración de continuidad del negocio	Falta de un plan de Contingencia operativo	Evaluar plan de Contingencia y establecer mejoras	BAJO		Riesgo Operativo	12 meses
	Falta de un Plan de Continuidad	Levantamiento de procesos críticos y crear BCP			Riesgo Operativo	
A.18 Cumplimiento	Falta de Responsable para Control por oposición	Generar obligatoriedad de auditoria de Sistemas y Seguridad de la Información con evaluación del alcance por año.	MEDIO		Auditoria - Jefatura de Seguridad	12 meses

Fuente: Los autores. Quito. Enero/2015

3.5.2. SEGUIMIENTO DEL PLAN

La institución financiera se compromete a realizar una revisión trimestral del Plan de Acción mediante la aplicación de una serie de indicadores que se han determinado y que se resumen en la tabla 3-20.

Tabla 3-20: Tabla de Indicadores de Gestión de Seguridad

Indicadores - Gestión de la Seguridad					
Nombre	**Frecuencia**	**Fórmula**	**Meta**	**Descripción**	**Responsable**
Cantidad de Medidas de prioridad alta implementadas	Trimestral	Sumatoria	>= 4	Cantidad de medidas de seguridad implementadas como respuesta a amenazas de seguridad identificadas.	Jefatura de Seguridad de la información
Cantidad de Medidas de prioridad media implementadas	Trimestral	Sumatoria	>= 2	Cantidad de medidas de seguridad implementadas como respuesta a amenazas de seguridad identificadas.	Jefatura de Seguridad de la información

Fuente: Los autores.

CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES.

La entidad financiera mantiene un alto riesgo de que se materialicen eventos de seguridad de la información, lo cual puede conllevar a pérdidas financieras e incumplimiento de la normativa vigente en primera instancia.

Al ser una empresa gubernamental, existen cambios de la alta gerencia muy frecuentemente, generando cambio en los lineamientos y objetivos establecidos para la implementación del SGSI, ya que cada nueva administración maneja enfoques distintos.

Al momento la falta de un plan estratégico para la implementación de un SGSI dificulta la definición de controles adecuados acorde a las necesidades de la institución.

La política de seguridad no abarca todos los dominios de seguridad que la institución financiera requiere por lo que su alcance se ve limitado.

El reglamento de seguridad no está alineado a la política de seguridad lo que genera confusión y tergiversación sobre lineamientos puntuales.
Las contravenciones a la política de seguridad de la Institución Financiera no son sancionadas.

El departamento de Tecnología tiene como debilidad la falta de segregación de funciones y que en cada jefatura no se establezcan claramente sus funciones, limitaciones y responsabilidades, lo mismo aplica para el personal de estas jefaturas.

Los incidentes de seguridad no manejan un proceso adecuado de evaluación, cierre y seguimiento y por ende los controles requeridos no han sido establecidos.

En el diseño, desarrollo, implementación o compra de soluciones del negocio no se considera al área de Seguridad de la Información como parte del grupo de evaluación y control de forma obligatoria.

El diagnóstico y evaluación de riesgos, se estableció mediante la metodología de la NIST SP 800-30, sin embargo, estos parámetros de evaluación cuantificables pueden ser corroborados o rechazados bajo la visión del área de negocio y la persona designada para la evaluación, quién al final del proceso tiene la última palabra.

4.2 RECOMENDACIONES.

Para la implementación de SGSI en la entidad financiera, se detalla a continuación las siguientes recomendaciones.

Actualización y revisión de la política y Reglamento de Seguridad de la Información.

Establecer un presupuesto y un plan estratégico para la implementación del Sistema de Gestión de Seguridad que garantice su cumplimiento aun cuando exista cambio en la alta gerencia.

Implementar con prioridad alta el cumplimiento de la normativa vigente considerando no sólo la solución tecnológica sino la inclusión de procedimientos documentados y controles de medición.

Es prioritario que la institución financiera eleve la necesidad de establecer un área de Seguridad de la Información en el proveedor de la información fuente que garantice la confidencialidad, integridad y disponibilidad.

Para la implementación de un SGSI es necesario se contemple las dependencias que son la fuente de información, proveedores críticos y procesos de apoyo, los cuales no fueron parte del proceso de evaluación de este proyecto, ya que las debilidades que estos puedan tener se trasladan a la institución al no tener control sobre las mismas.

La institución deberá evaluar la creación de un área o funcionario que esté a cargo de establecer la estrategia para la implementación, control y mejoramiento permanente del plan de continuidad de la Institución Financiera, considerando los plazos establecidos por la Superintendencia de Bancos del Ecuador.

Establecer un proceso disciplinario en caso de incumplimiento a la normativa vigente de Seguridad de la Información.

Realizar cambios al orgánico funcional con objeto de establecer las funciones y responsabilidades del área de Tecnología.

Implementar un proceso de control para el paso a producción de cambios en la infraestructura, aplicativos desarrollados o adquiridos, que puedan afectar la información de la institución y sus clientes.

Establecer y evaluar a los proveedores críticos de la institución financiera, así como incluir controles a través de los contratos y acuerdos de nivel de servicio establecidos con estas empresas.

Crear un equipo interdisciplinario y procedimiento documentado para el manejo de incidentes de seguridad.

Es necesario que los riesgos levantados estén asociados a una perdida financiera, de modo que exista mayor compromiso para el cierre de los mismos.

GLOSARIO

- **Alta Gerencia:** La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que hagan su veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada.
- **Datos:** Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptibles de ser capturado, almacenado, procesado y distribuido.
- **Información:** Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de servicio.
- **Información crítica:** Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;
- **Tecnología de la Información:** Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros;
- **Integridad:** Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento.
- **Disponibilidad:** Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que o requieren a través de los medios adecuados que satisfagan sus necesidades.
- **Cumplimiento:** Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones contraladas están sujetos.
- **Pistas de auditoría:** Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el

propósito de mantener información histórica para fines de control, supervisión y auditoría.

- **Encriptación:** Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino.
- **Plan de continuidad:** Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución.
- **Administración de la continuidad:** Es un proceso permanente que garantiza la continuidad de las operaciones del negocio de las instituciones financiero, a través de la efectividad del mantenimiento del plan de continuidad.
- **Responsable de la Información:** Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; se deben tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades;
- **Seguridad de la información:** Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.
- **Confidencialidad:** Es la garantía de que sólo el personal autorizado accede a la información preestablecida.
- **Transacción:** Se refiere a las acciones realizadas por los clientes a través de canales electrónicos, tales como consultas, transferencias, depósitos, retiros, pagos, cambios de clave, actualización de dato y otras relacionadas.
- **Banca Electrónica:** Son los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda.

- **Incidente de Seguridad de la Información:** Evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Institución Pública:** Institución perteneciente al estado que brinda servicios al público en general.
- **Registro Oficial:** El Registro Oficial es el órgano de difusión del Gobierno Nacional, se encarga de que la ley entre en vigencia a partir de su publicación y difusión
- **Títulos de Renta Fija:** Un título de renta fija es aquél que entrega una remuneración cierta, pactada de antemano, independientemente del desempeño de la empresa que lo emite, en tanto que uno de renta variable es aquél cuya remuneración es incierta, al estar sujeta al desempeño de ésta
- **Títulos de Renta Variable:** Los títulos de renta variable, los más importantes son las acciones, las cuales otorgan una retribución (dividendos en efectivo o en acciones liberadas) sólo cuando la empresa obtiene ganancias, previa aprobación de su junta de accionistas
- **Bolsas de Valores:** La bolsa de valores es una organización privada que brinda las facilidades necesarias para que sus miembros, atendiendo los mandatos de sus clientes, introduzcan órdenes y realicen negociaciones de compra y venta de valores, tales como acciones de sociedades o compañías anónimas, bonos públicos y privados, certificados, títulos de participación y una amplia variedad de instrumentos de inversión.
- **Listas de la OFAC:** Es una oficina del Departamento del Tesoro de los Estados Unidos que identifica países, terroristas y narcotraficantes sancionables de acuerdo con las leyes de EEUU. Emite la lista OFAC también conocida como lista Clinton
- **ISO 17799:** Es un estándar para la seguridad de la información publicado por la International Organization for Standardization y

la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013

- **NIST-800:** Son una serie de documentos de interés general sobre Seguridad de la Información. Estas publicaciones comenzaron en 1990 y son un esfuerzo de industrias, gobiernos y organizaciones académicas para todos los interesados en la seguridad.
- **BRP:** Perfil de Riesgo del Negocio y su medida del riesgo al que está expuesto una compañía.
- **AoAs:** Áreas de análisis que son la Infraestructura, las operaciones, aplicaciones y las personas.
- **MSAT:** La Herramienta de Evaluación de Seguridad de Microsoft es una herramienta gratuita diseñada para ayudar a las organizaciones de menos de 1.000 empleados a evaluar los puntos débiles de su entorno de seguridad de TI. Presenta un listado de cuestiones ordenadas por prioridad así como orientación específica para minimizar esos riesgos.
- **Autenticación Multi factor:** Es un sistema de seguridad que requiere más de una forma de autenticación para verificar la legitimidad de una transacción.
- **NIDS:** Sistema de detección de intrusos en una Red. Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneado de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real.
- **HIDS:** Es un programa de detección de accesos no autorizados a un computador o a una red.
- **COBIT:** Es un conjunto de herramientas de soporte que permite a los gestores poder cerrar la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio.

BIBLIOGRAFIA

- **Comité de Organizaciones Patrocinadoras de la Comisión de Normas**.
  http://www.coso.org/documents/. Último acceso: Marzo 2015.
- **Portal de la Superintendencia del Ecuador**.
  http://www.sbs.gob.ec/practg/p_index. Último acceso: Febrero 2015.
- **Portal del Proveedor.**
  Sitio web del proveedor. Último acceso: Enero 2015.
- **Portal de la institución financiera.**
  Sitio Web Institución Financiera Último acceso: Diciembre 2014.
- **Registro Oficial del Ecuador**.
  https://www.registroficial.gob.ec/. Último acceso: Diciembre 2014
- **Ministerio de Relaciones Laborales**
  http://www.trabajo.gob.ec/. Último acceso: Diciembre 2014.
- **Instituto Nacional de Estándares y Tecnología**.
  http://www.nist.gov/. Último acceso: Diciembre 2014
- **La Asociación Española de Normalización y Certificación.**
  http://www.aenor.es/aenor/inicio/home/home.asp. Último acceso: Marzo 2015.
- **El anexo de ISO 27001 en español**.
  https://iso27002.wiki.zoho.com/. Último acceso: Marzo 2015.
- **El portal de ISO 27002 en Español.**
  http://iso27000.es/. Último acceso: Marzo 2015.

ANEXOS

En la raíz del CD se encuentra ubicada la carpeta llamada Anexos donde constan los mencionados en este trabajo.

- **Anexo 1-A:** Informe Completo de resultados MSAT.
- **Anexo 2-A**: Justificación para Selección de la metodología NITS800-30.
- **Anexo 3-A:** Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- **Anexo 3-B:** Ley de Propiedad Intelectual.
- **Anexo 3-C:** Ley Orgánica del Sector Público (LOSEP).
- **Anexo 3-D:** Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).
- **Anexo 3-E:** Norma de Riesgo Operativo.
- **Anexo 3-F:** Código Orgánico Integral Penal.