UOC – INSTITUTO INTERNACIONAL DE POSGRADO

ELABORACIÓN DE UN PLAN PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Trabajo de Fin del Máster Interuniversitario en Seguridad de las Tecnologías de la Información y las Comunicaciones.

Autor:
Jorge Cástulo Guerrón Eras

Tutor:
Antonio José Segovia Henares

Loja, Enero de 2013

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo del Plan del proyecto es definir claramente el propósito del proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), los documentos que se redactarán, los plazos y las funciones y responsabilidades del proyecto.

El Plan del proyecto se aplica en una primera etapa a los datos, sistemas de información, medios de enlace y redes de comunicación, infraestructura tecnológica, soportes de información, infraestructura física y funcionarios que apoyan la ejecución de los tres (3) primeros procesos identificados como críticos dentro del Banco de Loja, lo cual nos permitirá identificar de una implementar la metodología adecuada, para cada año adaptar los demás procesos críticos del negocio con el SGSI, hasta obtener un grado de madurez que luego nos permita gestionar de una manera adecuada todos los procesos en el Banco de Loja.

Los usuarios de este documento y los que tienen acceso son:

- Gerente General.
- Gerente de Negocios.
- Gerente Administrativo Financiero.
- Gerente de Planificación.
- Gerente de Sistemas.
- Gerente de Riesgos.
- Asesor Jurídico.
- Jefe de Recursos Humanos.
- Jefe de Operaciones.
- Auditor de Sistemas.
- Oficial de Seguridad de la Información.
- Los miembros para la ejecución del proyecto, que serán debidamente identificados y notificados por el Oficial de Seguridad de la Información.

Objetivos Específicos.

- Realizar un diagnóstico de la situación actual entorno al ambiente de Seguridad de la Información en el Banco de Loja.
- Analizar la reglamentación elaborada por las entidades de control respecto a riesgos y seguridad de la información.
- Implementar bajo normas, mejores prácticas, y requerimientos de entidades de control un Sistema de Gestión de Seguridad de la Información, que permita dar cumplimiento a la legislación en materia de seguridad de la información.
- Establecer la metodología y procedimientos necesarios para implementar la gestión de activos de información de los procesos del Banco de Loja.

- Establecer mediante los controles seleccionados del anexo de la norma ISO 27002, los pilares de seguridad de la información en los activos y los procesos que soportan los servicios del Banco de Loja.
- Mejorar e implementar nuevas medidas de seguridad sobre los activos de información, los procesos y los sistemas que permiten brindar los servicios del Banco de Loja.
- Establecer las normas necesarias que permitan incrementar el compromiso y entorno de seguridad de la información, de los funcionarios y directivos del Banco de Loja.
- Establecer la planificación necesaria para gestionar de mejor manera la implementación de los controles de seguridad de la información.
- Identificar los requerimientos de normativas, servicios o software que son necesarios implementar para mejorar y garantizar la confidencialidad, integridad y disponibilidad de la seguridad de la información.

1. Documentos de referencia

Para el desarrollo del presente plan y la implementación del mismo, se ha seleccionado a la serie de estándares ISO 27000 relacionados con seguridad de la información, los cuales contienen los términos y definiciones que nos permiten aplicar el estándar ISO, los requisitos para implementar un SGSI, los dominios y objetivos de control para la implementación, y una guía de auditoría útil en la fase de verificación.

Adicionalmente se ha seleccionado los siguientes documentos:

- Norma BS 25999-2.
- NTP-ISO/IEC 17799-2007.

Metodología:

- Arquitectura de Seguridad de Información en la Empresa, denominada EISA por sus siglas en inglés.

2. Proyecto de Implementación del SGSI.

2.1. Objetivo del proyecto.

Para implementar el Sistema de Gestión de Seguridad de la Información en conformidad con la norma ISO 27001, se realizará a más tardar, hasta finales de Noviembre del 2014, la implementación de los documentos necesarios que permitan gestionar de manera segura el flujo de información derivado de los diferentes procesos del Banco de Loja.

2.2. Resultados del proyecto.

Durante el proyecto de implementación del SGSI, se redactarán los siguientes documentos:

a. Situación actual
b. Políticas que incluyen controles para:
    1. Aspectos Organizativos de la seguridad de la información.
    2. Gestión de Activos.
    3. Seguridad relacionada al personal.
    4. Gestión de comunicaciones y operaciones.
    5. Control de Acceso.
    6. Adquisición, desarrollo, mantenimiento de sistemas informáticos.
    7. Gestión de los Incidentes de Seguridad.
    8. Gestión de la Continuidad del Negocio.
    9. Cumplimiento.
c. Compromiso firmado por parte de los miembros del Comité de Administración Integral de Riesgo (CAIR), de apoyar decididamente a la implementación del SGSI.
d. Enfoque de evaluación de riesgos cuya metodología debe contemplar inventario de activos, identificación de amenazas y vulnerabilidades, identificación de impactos, análisis y evaluación de riesgos, y tratamiento de riesgos.
e. Declaración de aplicabilidad SOA.
f. Estrategias para Formación y concienciación.
g. Planes de acción correctiva/preventiva.
h. Planes de monitoreo y revisión.
i. Revisión del SGSI por parte de la Dirección.
j. Planes de auditoría.

2.3. Plazos

El Sistema de Gestión de Seguridad de la Información tiene como fecha límite de implementación Noviembre del 2014, fecha en la cual se habrá pasado por las fases del ciclo de Deaming o PDCA (Plan - Do - Check - Act) que nos permitirá, como la mejor práctica, hacer una mejora continua de las facses que son necesarias a fin de llevar a cabo una satisfactoria implementación del SGSI.

2.4. Organización del Proyecto

2.4.1. Promotor del Proyecto.

El promotor y responsable del presente proyecto será el Oficial de Seguridad de la Información, quien deberá coordinar cada una de las fases, solicitar, organizar o generar la documentación que sea necesaria a fin de dar cumplimiento a la implementación satisfactoria del SGSI.

2.4.2. Gerente del Proyecto.

El Oficial de Seguridad de la Información informará de los avances en el desarrollo del presente proyecto al Gerente de la Unidad de Administración Integral de Riesgos.

2.4.3. Equipo del Proyecto.

Para el desarrollo del presente proyecto será necesario contar con la colaboración de un miembro de la Unidad de Planificación y Desarrollo Organizacional, Administrador de Seguridad de la Información, y el visto bueno de los Gerentes de cada Área con la finalidad de involucrar a sus colaboradores de una manera planificada mientras se desarrolla el presente plan.

2.5. Principales Riesgos del Plan

En cualquier proyecto, el recurso más importante son las personas. Idealmente un proyecto debería tener disponibles a un número adecuado de personas, con las habilidades y experiencia correctas, y comprometidos y motivados con el proyecto. Sin embargo, las cosas pueden ser diferentes, por lo que hemos identificado estos riesgos.

- ¿El personal del proyecto está comprometido con la entera duración para lo que son necesarios?
- ¿Todos los miembros del equipo están disponibles a tiempo completo?
- ¿El movimiento de personal de un mismo proyecto es suficientemente bajo como para permitir la continuidad del proyecto?
- ¿Se han establecido los mecanismos apropiados para permitir la comunicación entre los miembros del equipo?
- ¿El entorno de trabajo del equipo es el apropiado?

2.6. Herramientas para implementación del proyecto y generación de informes.

Se ha evaluado varias herramientas, una de las mejores opciones de código abierto ha sido Securia SGSI es una herramienta integral que cubre el proceso automático de implantación, puesta en funcionamiento, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma internacional ISO 27001.

Otras herramientas evaluadas fueron:

- e-Pulpo.
- GCPGLOBAL.

- ORCA.

La herramienta seleccionada es actualizada periódicamente y cuenta con manuales de implementación y uso en español, adicional al uso de Securia, se usará hojas de cálculo lo cual permitirá llevar un control del avance de la implementación del SGSI.

3. Gestión de registros guardados en base a este documento.

Se realizará una revisión de los documentos de políticas y archivos generados del desarrollo e implementación del SGSI, se gestionará la implementación de un sistema de versionamiento que permita validar los cambios documentales y las versiones finales de adicionalmente se llevará el control de la documentación en las herramientas seleccionadas.

4. Validez y gestión de documentos.

Todos los documentos serán debatidos por los involucrados, recoger los comentarios ayudará a enriquecer las políticas que se definan, solo entrara en vigencia cuando se los apruebe por los canales establecidos en el Banco de Loja, y una vez que se tenga implementadas todas las correcciones solicitadas por los involucrados del SGSI.

5. Situación Actual.

5.1. Objetivos

- Verificar la implementación de una metodología que permita gestionar los riesgos del Banco, la identificación y valoración de activos y las amenazas sobre éstos.
- Verificar la administración de accesos lógicos a los servicios internos y externos.
- Verificar las configuraciones de los servicios y la documentación generada.
- Evaluación de la arquitectura de red implementada.
- Seleccionar los controles que nos van a permitir cubrir los distintos aspectos al implementar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Revisar las políticas, normas, procedimientos y documentos de control que nos permiten determinar el grado de cumplimiento en la implementación del SGSI.
- Validar el cumplimiento actual de la ISO:IEC 27002:2005

5.2. Metodología.

La metodología seleccionada para la implementación se basa en la metodología EISA la cual nos permitirá aplicar un método riguroso y comprensivo para describir el comportamiento de los procesos de seguridad del Banco, sistemas de seguridad de información y subunidades de personal y organizativas, para que se alineen con las metas comunes de la organización y la dirección estratégica.

Preguntas que responde la EISA

Un proceso de Arquitectura de Seguridad de Información en la Empresa ayuda a contestar preguntas básicas como:

- ¿Está la arquitectura actual apoyando y añadiendo valor a la seguridad de la organización?
- ¿Cómo podría una arquitectura de seguridad ser modificada para que añada más valor a la organización?
- Basándonos en lo que sabemos sobre lo que la organización quiere llevar a cabo en el futuro, ¿la arquitectura actual lo sustentará o lo entorpecerá?

Para implementar una arquitectura de seguridad de información en el Banco de Loja, mediante la cual la arquitectura se alinee con la estrategia de la organización y otros detalles necesarios tales como dónde y cómo opera, es necesario competencias esenciales, procesos de negocio, y cómo la organización interactúa consigo misma y con partes tales como clientes, proveedores, y entidades gubernamentales.

Estando establecida la estrategia y estructura de la organización, es necesario identificar cual es la actual arquitectura y como ésta soporta los procesos.

Requerimiento	Documentado	Actualizado
Cuadros de organización, actividades, y flujo de procesos sobre cómo TI de la organización opera.	Si	Si
Ciclos, periodos y distribución en el tiempo de la organización.	No	No
Proveedores de tecnología hardware, software y servicios.	No	No
Inventarios y diagramas de aplicaciones y software.	No	No
Interfaces entre aplicaciones; esto es: eventos, mensajes y flujo de datos.	No	No
Intranet, Extranet, Internet, comercio electrónico.	No	No
Clasificación de datos, bases de datos y modelos de datos soportados.	No	No
Hardware, plataformas, servidores, componentes de red y dispositivos de seguridad y dónde se conservan.	No	No
Redes de área local y abiertas, diagramas de conectividad a internet	No	No

Para el desarrollo del presente plan se utilizarán los siguientes procedimientos:

- Reuniones con los involucrados en el Plan de implementación del SGSI, que nos permitirá debatir y contar con la aceptación de los controles de la norma ISO 27002 a implementar en el Banco de Loja.
- Reunión para establecer el compromiso y delegados en el proceso de implementación del SGSI.

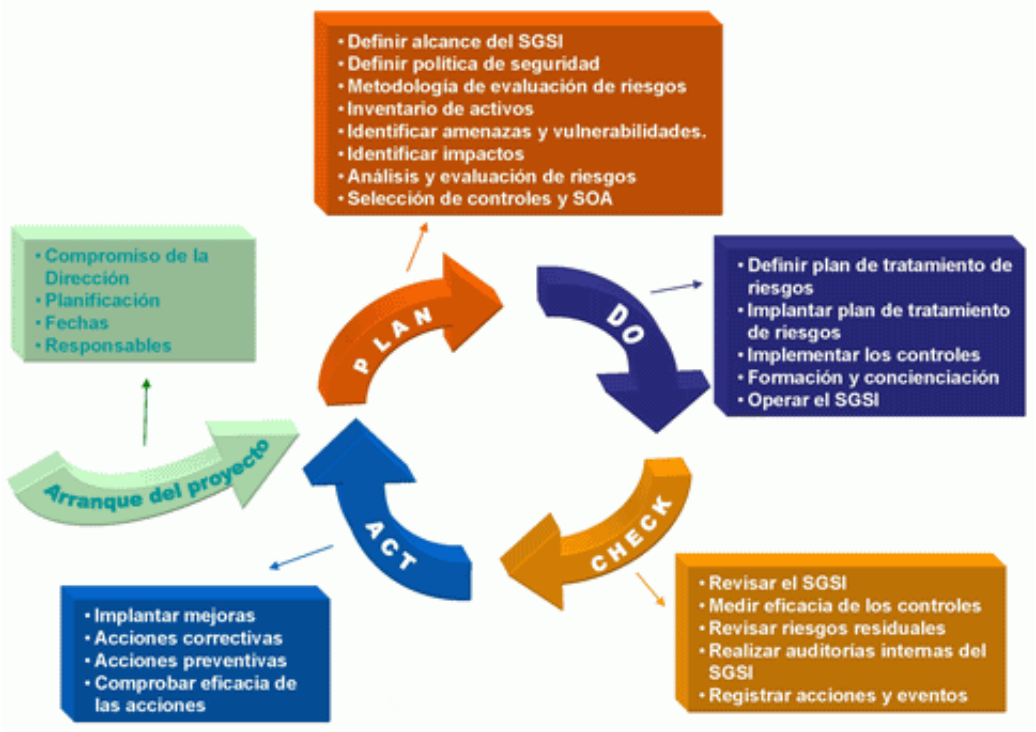
El objetivo de ésta etapa es sentar las bases del proceso de mejora continua en materia de seguridad, permitiendo al Banco de Loja conocer el estado del mismo y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

Para ello se abordarán las siguientes fases:

- Documentación normativa sobre las mejores prácticas en seguridad de la información.
- Identificación y valoración de los activos y amenazas sobre los activos del Banco de Loja
- Auditoría de cumplimiento de la ISO/IEC 27002:2005.
- Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- Presentación de resultados.

Para adaptar el Sistema de Gestión de Seguridad de la Información será importante que el proyecto se ajuste a las 4 fases definidas por la serie de normas ISO 27000 como la mejor práctica para poder implementar el SGSI, en el siguiente esquema se presenta las etapas

en las cuales el SGSI será adaptado al Banco de Loja, las mismas etapas serán la guía para la presentación de avances.



5.3. Documentación normativa sobre las mejores prácticas en seguridad de la información.

Para la ejecución de la presente etapa se selecciona a Magerit V2 como metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, también es posible que para la consecución de los objetivos sea necesario implementar otras fuentes de buenas prácticas como ITIL.

5.4. Identificación y valoración de los activos y amenazas sobre los activos del Banco de Loja

5.4.1. Inventario de Activos.

Como primera actividad a ejecutar es necesario realizar la evaluación de los activos de información en los procesos seleccionados, considerando las dependencias entre éstos y realizando una valoración.

Definición de grupos de activos.

Inventario de Activos	Detalle

Instalaciones	Ubicación de equipos informáticos y de comunicaciones
Hardware (HW)	Equipos que alojan datos, aplicaciones y servicios
Aplicación(SW)	Aplicativos que permiten manejar los datos
Datos	El principal recurso, todos los demás activos se identifican alrededor de éste activo
Red	Equipamiento que permite intercambiar datos
Servicios	Que se brindan gracias a los datos y que se necesitan para gestionar los datos
Equipamiento Auxiliar	Todo aquello que complemente al material informático
Soportes de Información	Dispositivos que permiten el almacenamiento de datos (temporal)
Personal	Quienes explotan u operan todos los demás elementos

Activos proceso operaciones de caja:

Ámbito	Activo
Datos	Información personal cliente
	Transacción Cliente
Servicios	Depósito
	Retiro
	Pagos
	Operaciones Pólizas
	Recaudación
SW	FISA
	Sistema BP-BR (webservice)
HW	Servidor BBDD
	IBM Blade Server
	Servidor Formas
	Terminal de Usuario
Redes y comunicaciones	Red Lan
Soporte de Información	Papeletas
	Comprobantes
Equipamiento Auxiliar	
Instalaciones	Oficinas
	Data Center (Sala servidores)
Personal	Cajeros
	Supervisor de Caja / Oficial Operativo y Administrativo
	Supervisor de Front Operativo
	Jefe de Operaciones
	Terceros

Valoración de los activos

Dimensiones de Seguridad		
VA	Valor	Criterio
MA	10	Daño muy grave a la organización
A	7 - 9	Daño grave a la organización
MA	4 - 6	Daño importante a la organización
B	1 - 3	Daño menor a la organización
MB	0	Daño irrelevante para la organización

Ámbito	Activo	Valor	A	C	I	D	A
Datos	Información personal cliente	MA	8	9	10	9	7
	Transacción Cliente	M	6	8	9	6	7
Servicios	Depósito	MA	8	7	7	10	7
	Retiro	MA	8	7	7	10	7
	Pagos	M	8	7	7	6	7
	Operaciones Pólizas	M	8	7	7	6	7
	Recaudación	M	8	7	7	6	7
SW	FISA	MA	8	9	9	9	8
	Sistema BP-BR (webservice gestión independiente)	MA	6	6	5	3	1
HW	Servidor BBDD Principal - Oracle	MA	9	9	9	9	9
	IBM Blade Server	MA	7	9	8	9	6
	Servidor Formas - Oracle Forms 6	MA	7	9	8	9	6
	Terminal de Usuario	M	2	2	1	6	1
Redes y comunicaciones	Red Lan	MA	9	9	9	9	9
Soporte de Información	Papeletas	M	2	1	8	4	1
	Comprobantes	MB	8	2	6	4	2
Instalaciones	Oficinas	A	7	8	7	8	2
	Data Center (Sala servidores)	MA	9	10	10	10	9
Personal	Cajeros	M	7	9	9	5	4
	Supervisor de Caja / Oficial Operativo y Administrativo	M	7	9	9	8	6
	Supervisor de Front Operativo	B	7	9	9	3	4
	Jefe de Operaciones	B	7	9	9	3	4

5.4.4. Análisis de Amenazas.

Para el entendimiento de la presente etapa es necesario indicar que se establecen según Magerit V2, ciertas amenazas típicas identificadas y que reducen la utilización del activo en diferentes ámbitos de los pilares de la seguridad de la información, éstos activos están frecuentemente expuestos a las amenazas, por lo cual la frecuencia de ocurrencia se expresará como como tasa anual o incidencias por año; finalmente la frecuencia con la

que una amenaza se materialice sobre un activo hará que éste activo disminuya en un porcentaje de su valor.

Información personal cliente	Frecuencia	A	C	I	D	A
E.1 Errores de los usuarios	40			80%	60%	
E.2 Errores del Administrador	20	10%	80%	80%	100%	100%
E.3 Errores de monitorización (Log)	20		10%	10%	10%	100%
E.4 Errores de configuración	30	50%				100%
E.14 Escapes de Información (fuga accidental)	60		1%			
E.15 Alteración de la información	30			100%		
E.16 Introducción de información incorrecta	100			50%		
E.17 Degradación de la información	40			50%		
E.18 Destrucción de información	10				100%	
E.19 Divulgación de información (fuga)	50		10%			
A.4 Manipulación de la configuración	1	100%	100%	100%	100%	100%
A.11 Acceso no autorizado	1	50%	10%	100%		
A.14 Interceptación de información (escucha)	1		50%			
A.15 Modificación de la Información	10			100%		
A.16 Introducción de falsa información	10			80%		
A.17 Corrupción de la información	40			20%		
A.18 Destrucción la información	20				100%	
A.19 Divulgación de Información	40		1%			

Transacción Cliente	Frecuencia	A	C	I	D	A
E.1 Errores de los usuarios	60			30%	20%	
E.2 Errores del Administrador	10	10%	80%	80%	50%	10%
E.3 Errores de monitorización (Log)	10		10%	10%	10%	100%
E.4 Errores de configuración	50	50%				100%
E.14 Escapes de Información (fuga accidental)	1		1%			
E.15 Alteración de la información	10			100%		
E.16 Introducción de información incorrecta	10			50%		
E.17 Degradación de la información	1			50%		
E.18 Destrucción de información	1				100%	
E.19 Divulgación de información (fuga)	10		10%			
A.4 Manipulación de la configuración	1	100%	100%	100%	100%	100%
A.11 Acceso no autorizado	1	50%	10%	100%		
A.14 Interceptación de información (escucha)	1		50%			
A.15 Modificación de la información	1			100%		
A.16 Introducción de falsa información	10			80%		
A.17 Corrupción de la información	1			20%		
A.18 Destrucción la información	1				100%	
A.19 Divulgación de Información	80		1%			

Depósito	Frecuencia	A	C	I	D	A
E.1 Errores de los usuarios	30			1%	1%	
E.2 Errores del Administrador	10	80%	30%	50%	100%	10%
E.3 Errores de monitorización (Log)	10					10%
E.4 Errores de configuración	20	10%	100%	100%	100%	100%
E.9 Errores de re-encaminamiento	1	10%	50%	80%		10%
E.10 Errores de secuencia	1			60%		
E.24 Caída del sistema por agotamiento de recursos	30				100%	
A.4 Manipulación de la configuración	1	30%	30%	50%	50%	80%
A.5 Suplantación de la identidad del usuario	1	10%	30%	50%		
A.6 Abuso de privilegios de acceso	20		60%	60%		
A.7 Uso no previsto	50				70%	
A.9 Re-encaminamiento de mensajes	1	10%	10%	30%		40%
A.10 Alteración de secuencia	1			20%		
A.11 Acceso no autorizado	1	50%	30%	30%		
A.13 Repudio	10					100%
A.24 Denegación de servicio	1				100%	

Retiro	Frecuencia	A	C	I	D	A
E.1 Errores de los usuarios	30			1%	1%	
E.2 Errores del Administrador	10	80%	30%	50%	100%	10%
E.3 Errores de monitorización (Log)	10					10%
E.4 Errores de configuración	20	10%	100%	100%	100%	100%
E.9 Errores de re-encaminamiento	1	10%	50%	80%		10%
E.10 Errores de secuencia	1			60%		
E.24 Caída del sistema por agotamiento de recursos	30				100%	
A.4 Manipulación de la configuración	1	30%	30%	50%	50%	80%
A.5 Suplantación de la identidad del usuario	1	10%	30%	50%		
A.6 Abuso de privilegios de acceso	20		60%	60%		
A.7 Uso no previsto	50				70%	
A.9 Re-encaminamiento de mensajes	1	10%	10%	30%		40%
A.10 Alteración de secuencia	1			20%		
A.11 Acceso no autorizado	1	50%	30%	30%		
A.13 Repudio	10					100%
A.24 Denegación de servicio	1				100%	

Pagos	Frecuencia	A	C	I	D	A
E.1 Errores de los usuarios	30			1%	1%	
E.2 Errores del Administrador	10	80%	30%	50%	100%	10%
E.3 Errores de monitorización (Log)	10					10%

E.4 Errores de configuración	20	10%	100%	100%	100%	100%
E.9 Errores de re-encaminamiento	1	10%	50%	80%		10%
E.10 Errores de secuencia	1			60%		
E.24 Caída del sistema por agotamiento de recursos	30				100%	
A.4 Manipulación de la configuración	1	30%	30%	50%	50%	80%
A.5 Suplantación de la identidad del usuario	1	10%	30%	50%		
A.6 Abuso de privilegios de acceso	20		60%	60%		
A.7 Uso no previsto	50				70%	
A.9 Re-encaminamiento de mensajes	1	10%	10%	30%		40%
A.10 Alteración de secuencia	1			20%		
A.11 Acceso no autorizado	1	50%	30%	30%		
A.13 Repudio	10					100%
A.24 Denegación de servicio	1				100%	

Operaciones Pólizas	Frecuencia	A	C	I	D	A
E.1 Errores de los usuarios	30			1%	1%	
E.2 Errores del Administrador	10	80%	30%	50%	100%	10%
E.3 Errores de monitorización (Log)	10					10%
E.4 Errores de configuración	20	10%	100%	100%	100%	100%
E.9 Errores de re-encaminamiento	1	10%	50%	80%		10%
E.10 Errores de secuencia	1			60%		
E.24 Caída del sistema por agotamiento de recursos	30				100%	
A.4 Manipulación de la configuración	1	30%	30%	50%	50%	80%
A.5 Suplantación de la identidad del usuario	1	10%	30%	50%		
A.6 Abuso de privilegios de acceso	20		60%	60%		
A.7 Uso no previsto	50				70%	
A.9 Re-encaminamiento de mensajes	1	10%	10%	30%		40%
A.10 Alteración de secuencia	1			20%		
A.11 Acceso no autorizado	1	50%	30%	30%		
A.13 Repudio	10					100%
A.24 Denegación de servicio	1				100%	

Recaudación	Frecuencia	A	C	I	D	A
E.1 Errores de los usuarios	30			1%	1%	
E.2 Errores del Administrador	10	80%	30%	50%	100%	10%
E.3 Errores de monitorización (Log)	10					10%
E.4 Errores de configuración	20	10%	100%	100%	100%	100%
E.9 Errores de re-encaminamiento	1	10%	50%	80%		10%
E.10 Errores de secuencia	1			60%		
E.24 Caída del sistema por agotamiento de recursos	30				100%	

A.4 Manipulación de la configuración	1	30%	30%	50%	50%	80%
A.5 Suplantación de la identidad del usuario	1	10%	30%	50%		
A.6 Abuso de privilegios de acceso	20		60%	60%		
A.7 Uso no previsto	50				70%	
A.9 Re-encaminamiento de mensajes	1	10%	10%	30%		40%
A.10 Alteración de secuencia	1			20%		
A.11 Acceso no autorizado	1	50%	30%	30%		
A.13 Repudio	10					100%
A.24 Denegación de servicio	1				100%	

FISA	Frecuencia	A	C	I	D	A
I.5 Avería de origen físico o lógico	10				100%	100%
E.1 Errores de los usuarios	10			1%	1%	
E.2 Errores del Administrador	20	50%	100%	100%	100%	20%
E.3 Errores de monitorización (Log)	1					20%
E.4 Errores de configuración	10	10%	50%	100%	100%	20%
E.8 Difusión de software dañino	1	1%	1%	1%	1%	1%
E.9 Errores de re-encaminamiento	1	1%	50%	50%		100%
E.10 Errores de secuencia	1			30%		
E.14 Escapes de información	20		30%			
E.20 Vulnerabilidades de los programas (software)	30		100%	100%	100%	
E.21 Errores de mantenimiento / Actualización de programas (software)	30			100%	100%	
A.4 Manipulación de la configuración	30	30%	100%	100%	100%	50%
A.5 Suplantación de la identidad del usuario	1	80%	80%	80%		
A.6 Abuso de privilegios de acceso	1		50%	50%		
A.7 Uso no previsto	20				50%	
A.8 Difusión de software dañino	1	100%	100%	100%	100%	100%
A.9 Re-encaminamiento de mensajes	1	10%	50%	50%		10%
A.10 Alteración de secuencia	1			50%		
A.11 Acceso no autorizado	1	100%	100%	100%		
A.14 Interceptación de información (escucha)	1		20%			
A.22 Manipulación de programas	1	100%	100%	100%		100%

Sistema BP-BR (webservice gestión independiente)	Frecuencia	A	C	I	D	A
I.5 Avería de origen físico o lógico	30				100%	100%
E.1 Errores de los usuarios	10			1%	1%	
E.2 Errores del Administrador	1	10%	10%	10%	10%	10%
E.3 Errores de monitorización (Log)	1					1%
E.4 Errores de configuración	1	1%	1%	1%	100%	2%
E.8 Difusión de software dañino	1	1%	1%	1%	1%	1%

E.9 Errores de re-encaminamiento	1	1%	50%	50%		100%
E.10 Errores de secuencia	1			30%		
E.14 Escapes de información	20		30%			
E.20 Vulnerabilidades de los programas (software)	10		10%	10%	10%	
E.21 Errores de mantenimiento / Actualización de programas (software)	10			100%	100%	
A.4 Manipulación de la configuración	10	10%	10%	10%	10%	10%
A.5 Suplantación de la identidad del usuario	1	1%	10%	10%		
A.6 Abuso de privilegios de acceso	1		1%	10%		
A.7 Uso no previsto	20				10%	
A.8 Difusión de software dañino	1	10%	10%	10%	10%	10%
A.9 Re-encaminamiento de mensajes	1	10%	50%	50%		10%
A.10 Alteración de secuencia	1			50%		
A.11 Acceso no autorizado	1	10%	10%	10%		
A.14 Interceptación de información (escucha)	1		20%			
A.22 Manipulación de programas	1	1%	1%	1%		1%

Servidor BBDD Principal - Oracle	Frecuencia	A	C	I	D	A
N.1 Fuego	0				100%	100%
N.2 Daños por Agua	1				100%	100%
N.* Desastres Naturales	0				100%	100%
I.1 Fuego	0				100%	100%
I.2 Daños por agua	1				100%	100%
I.* Desastres Industriales	0				100%	100%
I.3 Contaminación Mecánica	0				10%	10%
I.4 Contaminación Electromagnética	1				10%	10%
I.5 Avería de origen físico o lógico	10				100%	100%
I.6 Corte de suministro eléctrico	10				100%	100%
I.7 Condiciones inadecuadas de temperatura y/o humedad	1				50%	50%
I.11 Emanaciones electromagnéticas	1		10%			
E.2 Errores del Administrador	10	50%	100%	100%	100%	10%
E.4 Errores de configuración	1	10%	100%	100%	100%	10%
E.23 Errores de mantenimiento /actualización de equipos (hardware)	1				100%	
E.24 Caída del sistema por agotamiento de recursos	10				100%	
A.4 Manipulación de la configuración	1	10%	100%	100%	100%	10%
A.6 Abuso de privilegios de acceso	1		50%	50%		
A.7 Uso no previsto	1			30%		
A.11 Acceso no autorizado	1		30%	30%		
A.14 Interceptación de información (escucha)	0		20%			

A.24 Denegación de servicio	0				100%	
A.25 Robo	0		50%		50%	
A.26 Ataque destructivo	0				100%	
A.27 Ocupación enemiga	0		50%		50%	

IBM Blade Server	Frecuencia	A	C	I	D	A
N.1 Fuego	0				100%	100%
N.2 Daños por Agua	1				100%	100%
N.* Desastres Naturales	0				100%	100%
I.1 Fuego	0				100%	100%
I.2 Daños por agua	1				100%	100%
I.* Desastres Industriales	0				100%	100%
I.3 Contaminación Mecánica	0				10%	10%
I.4 Contaminación Electromagnética	1				10%	10%
I.5 Avería de origen físico o lógico	10				100%	100%
I.6 Corte de suministro eléctrico	10				100%	100%
I.7 Condiciones inadecuadas de temperatura y/o humedad	1				50%	50%
I.11 Emanaciones electromagnéticas	1		10%			
E.2 Errores del Administrador	10	50%	100%	100%	100%	10%
E.4 Errores de configuración	1	10%	100%	100%	100%	10%
E.23 Errores de mantenimiento /actualización de equipos (hardware)	1				100%	
E.24 Caída del sistema por agotamiento de recursos	10				100%	
A.4 Manipulación de la configuración	1	10%	100%	100%	100%	10%
A.6 Abuso de privilegios de acceso	1		50%	50%		
A.7 Uso no previsto	1			30%		
A.11 Acceso no autorizado	1		30%	30%		
A.14 Interceptación de información (escucha)	0		20%			
A.24 Denegación de servicio	0				100%	
A.25 Robo	0		50%		50%	
A.26 Ataque destructivo	0				100%	
A.27 Ocupación enemiga	0		50%		50%	

Servidor Formas - Oracle Forms 6	Frecuencia	A	C	I	D	A
N.1 Fuego	0				100%	100%
N.2 Daños por Agua	1				100%	100%
N.* Desastres Naturales	0				100%	100%
I.1 Fuego	0				100%	100%
I.2 Daños por agua	1				100%	100%
I.* Desastres Industriales	0				100%	100%
I.3 Contaminación Mecánica	0				10%	10%

I.4 Contaminación Electromagnética	1				10%	10%
I.5 Avería de origen físico o lógico	10				100%	100%
I.6 Corte de suministro eléctrico	10				100%	100%
I.7 Condiciones inadecuadas de temperatura y/o humedad	1				50%	50%
I.11 Emanaciones electromagnéticas	1		10%			
E.2 Errores del Administrador	10	50%	100%	100%	100%	10%
E.4 Errores de configuración	1	10%	100%	100%	100%	10%
E.23 Errores de mantenimiento /actualización de equipos (hardware)	1				100%	
E.24 Caída del sistema por agotamiento de recursos	10				100%	
A.4 Manipulación de la configuración	1	10%	100%	100%	100%	10%
A.6 Abuso de privilegios de acceso	1		50%	50%		
A.7 Uso no previsto	1			30%		
A.11 Acceso no autorizado	1		30%	30%		
A.14 Interceptación de información (escucha)	0		20%			
A.24 Denegación de servicio	0				100%	
A.25 Robo	0		50%		50%	
A.26 Ataque destructivo	0				100%	
A.27 Ocupación enemiga	0		50%		50%	

Terminal de Usuario	Frecuencia	A	C	I	D	A
N.1 Fuego	0				10%	10%
N.2 Daños por Agua	1				10%	10%
N.* Desastres Naturales	0				10%	10%
I.1 Fuego	0				10%	10%
I.2 Daños por agua	1				10%	10%
I.* Desastres Industriales	0				1%	1%
I.3 Contaminación Mecánica	0				1%	1%
I.4 Contaminación Electromagnética	1				10%	10%
I.5 Avería de origen físico o lógico	10				1%	1%
I.6 Corte de suministro eléctrico	10				1%	1%
I.7 Condiciones inadecuadas de temperatura y/o humedad	1				50%	50%
I.11 Emanaciones electromagnéticas	1		10%			
E.2 Errores del Administrador	10	10%	10%	10%	10%	10%
E.4 Errores de configuración	1	10%	10%	10%	10%	10%
E.23 Errores de mantenimiento /actualización de equipos (hardware)	1				10%	
E.24 Caída del sistema por agotamiento de recursos	10				10%	
A.4 Manipulación de la configuración	1	10%	10%	10%	10%	10%
A.6 Abuso de privilegios de acceso	1		1%	1%		

A.7 Uso no previsto	1			1%		
A.11 Acceso no autorizado	1		1%	1%		
A.14 Interceptación de información (escucha)	0		1%			
A.24 Denegación de servicio	0				1%	
A.25 Robo	0		50%		50%	
A.26 Ataque destructivo	0				50%	
A.27 Ocupación enemiga	0		50%		50%	

Red Lan	Frecuencia	A	C	I	D	A
N.1 Fuego	0				100%	100%
N.2 Daños por Agua	1				100%	100%
N.* Desastres Naturales	0				100%	100%
I.1 Fuego	0				100%	100%
I.2 Daños por agua	1				100%	100%
I.* Desastres Industriales	0				100%	100%
I.3 Contaminación Mecánica	0				10%	10%
I.4 Contaminación Electromagnética	1				50%	50%
I.5 Avería de origen físico o lógico	10				100%	100%
I.6 Corte de suministro eléctrico	10				100%	100%
I.7 Condiciones inadecuadas de temperatura y/o humedad	1				80%	80%
I.8 Fallo de servicio de comunicaciones	1				100%	
I.11 Emanaciones electromagnéticas	0		50%			
E.2 Errores del Administrador	10	50%	100%	100%	100%	10%
E.4 Errores de configuración	1	10%	100%	100%	100%	10%
E.9 Errores de re-encaminamiento	0	10%	50%	50%		50%
E.10 Errores de secuencia	0			50%		
E.14 Escapes de información	1		50%			
E.24 Caída del sistema por agotamiento de recursos	1				100%	
A.4 Manipulación de la configuración	1	50%	100%	100%	100%	10%
A.5 Suplantación de la identidad del usuario	0	50%	50%	50%		
A.6 Abuso de privilegios de acceso	0		80%	80%		
A.7 Uso no previsto	1				50%	
A.9 Re-encaminamiento de mansajes	0	10%	100%	100%		10%
A.10 Alteración de Secuencia	0			50%		
A.11 Acceso no autorizado	0	10%	50%	50%		
A.12 Análisis de tráfico	0		20%			
A.14 Interceptación de información (escucha)	0		20%			
A.24 Denegación de servicio	0				100%	
A.25 Robo	0		10%		100%	
A.26 Ataque destructivo	0				100%	
A.27 Ocupación enemiga	0				100%	

Papeletas	Frecuencia	A	C	I	D	A
N.1 Fuego	0				100%	100%
N.2 Daños por Agua	30				100%	100%
N.* Desastres Naturales	0				100%	100%
I.1 Fuego	0				100%	100%
I.2 Daños por agua	30				100%	100%
I.* Desastres Industriales	0				100%	100%
I.3 Contaminación Mecánica	0				50%	50%
I.4 Contaminación Electromagnética	0				0%	0%
I.5 Avería de origen físico o lógico	10				100%	100%
I.6 Corte de suministro eléctrico	0				0%	0%
I.7 Condiciones inadecuadas de temperatura y/o humedad	30				100%	100%
I.10 Degradación de los soportes de almacenamiento de la información	30				100%	100%
A.7 Uso no previsto	10				1%	
A.11 Acceso no autorizado	1	50%	50%	50%		
A.25 Robo	0		100%		100%	
A.26 Ataque destructivo	0				100%	
A.27 Ocupación enemiga	0		10%		10%	

Comprobantes	Frecuencia	A	C	I	D	A
N.1 Fuego	0				100%	100%
N.2 Daños por Agua	50				100%	100%
N.* Desastres Naturales	0				100%	100%
I.1 Fuego	0				100%	100%
I.2 Daños por agua	50				100%	100%
I.* Desastres Industriales	0				100%	100%
I.3 Contaminación Mecánica	0				50%	50%
I.4 Contaminación Electromagnética	0				0%	0%
I.5 Avería de origen físico o lógico	10				100%	100%
I.6 Corte de suministro eléctrico	0				0%	0%
I.7 Condiciones inadecuadas de temperatura y/o humedad	50				100%	100%
I.10 Degradación de los soportes de almacenamiento de la información	50				100%	100%
A.7 Uso no previsto	10				1%	
A.11 Acceso no autorizado	1	50%	50%	50%		
A.25 Robo	0		100%		100%	
A.26 Ataque destructivo	0				100%	
A.27 Ocupación enemiga	0		10%		10%	

Oficinas	Frecuencia	A	C	I	D	A
N.1 Fuego	0				60%	60%
N.2 Daños por Agua	10				60%	60%
N.* Desastres Naturales	0				80%	80%
I.1 Fuego	0				60%	60%
I.2 Daños por agua	10				60%	60%
I.* Desastres Industriales	0				60%	60%
I.11 Emanaciones Electromagnéticas	0				30%	30%
A.7 Uso no previsto	0				10%	
A.11 Acceso no autorizado	20	20%	20%	20%		
A.26 Ataque destructivo	0				60%	
A.27 Ocupación enemiga	0		20%		20%	

Data Center (Sala servidores)	Frecuencia	A	C	I	D	A
N.1 Fuego	0				100%	100%
N.2 Daños por Agua	20				80%	80%
N.* Desastres Naturales	0				80%	80%
I.1 Fuego	0				100%	100%
I.2 Daños por agua	20				80%	80%
I.* Desastres Industriales	0				60%	60%
I.11 Emanaciones Electromagnéticas	0				50%	50%
A.7 Uso no previsto	0				10%	
A.11 Acceso no autorizado	20	50%	50%	50%		
A.26 Ataque destructivo	0				100%	
A.27 Ocupación enemiga	0		50%		50%	

Cajeros	Frecuencia	A	C	I	D	A
E.7 Deficiencias en la organización	30				20%	
E.28 Indisponibilidad del personal	40				1%	
A.28 Indisponibilidad del personal	0				1%	
A.29 Extorsión	0	1%	1%	1%		1%
A.30 Ingeniería Social	20	1%	1%	1%		1%

Supervisor de Caja / Oficial Operativo y Administrativo	Frecuencia	A	C	I	D	A
E.7 Deficiencias en la organización	20				20%	
E.28 Indisponibilidad del personal	10				20%	
A.28 Indisponibilidad del personal	0				20%	
A.29 Extorsión	0	20%	20%	20%		20%
A.30 Ingeniería Social	10	20%	20%	20%		20%

Supervisor de Front Operativo	Frecuencia	A	C	I	D	A

E.7 Deficiencias en la organización	10				10%	
E.28 Indisponibilidad del personal	1				30%	
A.28 Indisponibilidad del personal	0				30%	
A.29 Extorsión	0	30%	30%	30%		30%
A.30 Ingeniería Social	10	30%	30%	30%		30%

Jefe de Operaciones	Frecuencia	A	C	I	D	A
E.7 Deficiencias en la organización	1				1%	
E.28 Indisponibilidad del personal	1				50%	
A.28 Indisponibilidad del personal	0				50%	
A.29 Extorsión	0	50%	50%	50%		50%
A.30 Ingeniería Social	1	50%	50%	50%		50%

5.4.5. Cálculo del Riesgo.

El cálculo del riesgo actual es una valoración en la que interviene el valor que le hemos dado a los activos en cada una de las dimensiones, la frecuencia con la que una amenaza puede degradar a aun activo, y el impacto de daño o disminución que la amenaza puede causarle al activo, en el ***Anexo 1. Cálculo del Riesgo Actual***; se identifica y se calculan los diferentes valores de riesgo para los activos.

5.4.6. Selección de controles/salvaguardas.

Para ejecutar la actividad de selección de salvaguardas, debemos tomar en consideración los elementos de protección actual que tienen nuestros activos, y los posibles elementos de control de los que podemos dotar a nuestros, activos, es decir a los grupos de activos que hemos definido, validar los controles del Anexo a la Norma UNE-ISO/IEC 27001:2005 son aplicables en el contexto de nuestras capacidades, para ésto se ha considerado 2 ámbitos esenciales con los que debemos trabajar las salvaguardas, los aspectos de y el tipo de protección de las salvaguardas que vamos a implementar, los cuales resumimos en los siguientes cuadros.

Aspecto de las salvaguardas	
PR	Procedimientos
PP	Política Personal
SW	Aplicaciones
HW	Dispositivos Físicos
SF	Seguridad Física

Tipo de protección	
PTG	Protección de Tipo General
PdS	Protección de Servicios
PDI	Protección de Datos/Información
PSW	Protección de Aplicaciones
PHW	Protección de Equipos
PdC	Protección de Comunicaciones
PSF	Seguridad Física
PRP	Relativas al Personal

En el ***Anexo 2. Selección de Salvaguardas***; hemos identificado los controles actuales y los posibles controles que podemos aplicar.

5.4.7. Cálculo del Riesgo Residual.

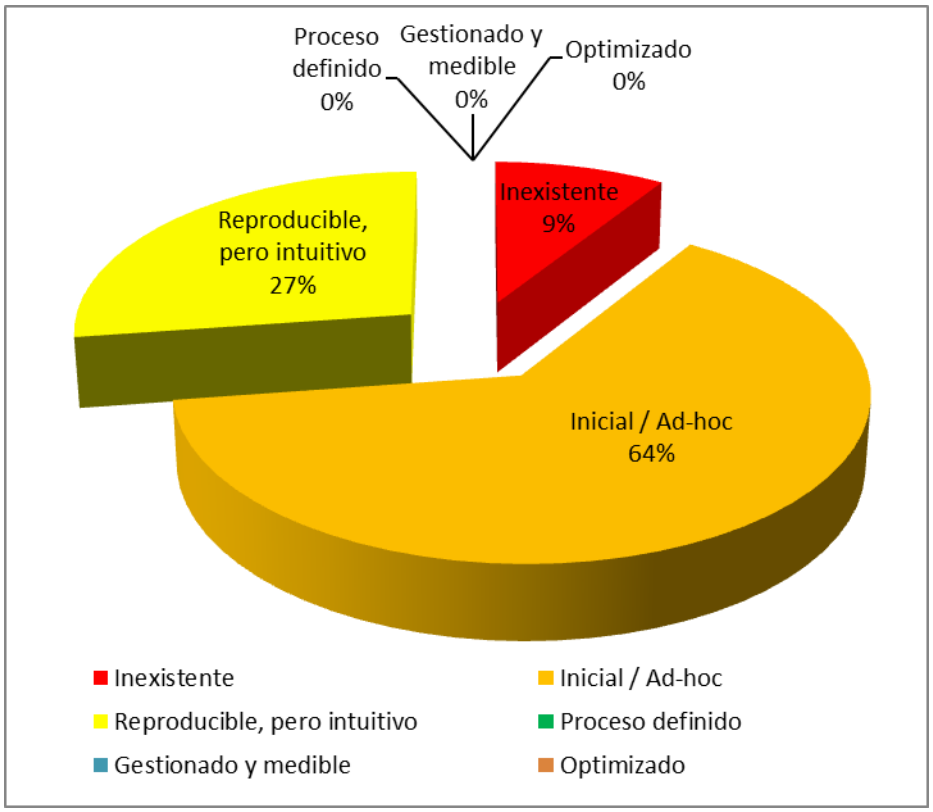
Luego de identificados los controles o salvaguardas que debemos aplicar a los diferentes activos, debemos volver a calcular el riesgo al que están expuestos nuestros activos pero ésta vez disminuido en los casos en los que hemos adoptado la implementación de salvaguardas, es decir que el riesgo analizado en el Literal 5.4.5, está disminuido gracias a la actividad realizada en el literal 5.4.6, en el ***Anexo 3. Cálculo del Riesgo Residual***; se detallan los diferentes valores de riesgo para los activos, luego de implementadas las salvaguardas.

5.5. Auditoría de cumplimiento de la ISO/IEC 27002:2005.

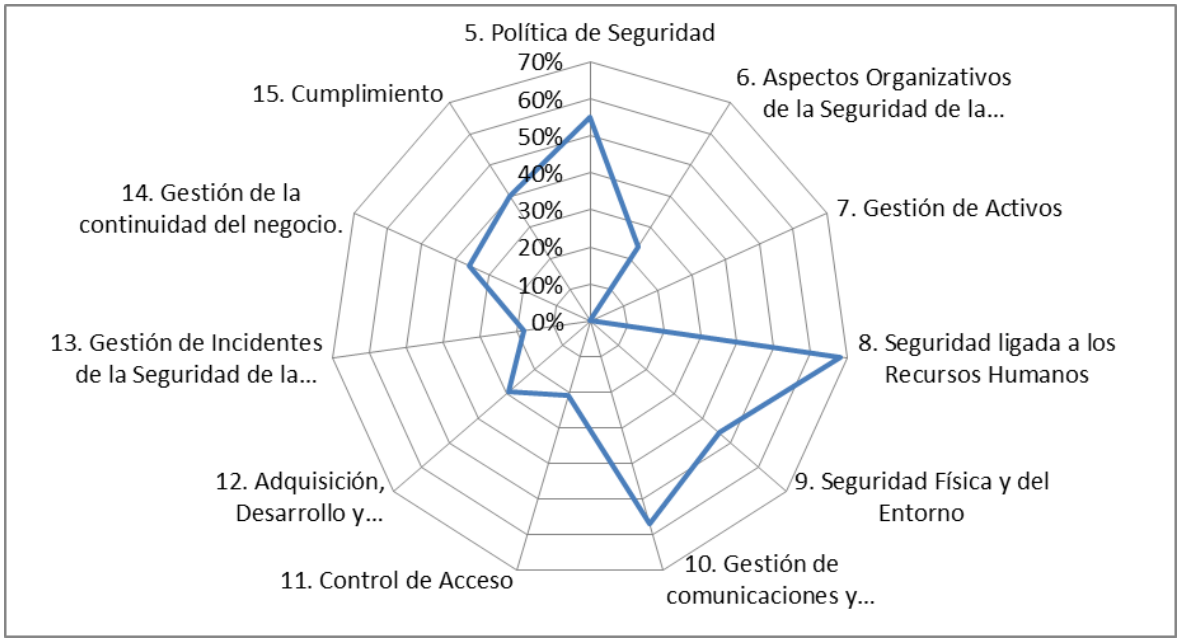
Con el propósito de proteger la información del Banco, y como futura guía para implementar o mejorar las medidas de seguridad, ésta etapa nos va a permitir obtener una radiografía de la situación actual entorno a la Seguridad del Banco de Loja.

*NOTA: En el **Anexo 4. Tabla de Cumplimiento de la ISO/IEC 27002:2005**, se detalla el estado actual de la seguridad implementada indicando el porcentaje de cumplimiento por cada control.*

5.5.1. Modelo de Madurez de la Capacidad



5.5.2. Diagrama de Radar



6. Propuestas de Proyectos

El primer acercamiento para realizar la implementación del SGSI es el desarrollo del presente plan, el mismo que es un instrumento imprescindible en cualquier organización, las propuestas de los proyectos que se ejecutarán ayudarán a mejorar el entorno de Seguridad de la Información en el Banco de Loja, los proyectos que se recomiendan estudiar y que ayudarán a mitigar el riesgo y dar cumplimiento a la norma UNE ISO/IEC 27002:2005, en todos los casos se deberá establecer el costo beneficio, para validar la cuantificación económica contra el tiempo de implementación y la factibilidad de uso, algunos de los proyectos que se propone validar serán:

Proyecto 1.-

Clasificación de activos de información.

Recursos Personal.-

- Oficial de Seguridad de la Información
- Oficial de Planificación
- Oficial de Procesos
- Jefe de Centro de Cómputo
- Jefe de Operaciones

Recursos Hardware.-

- Terminales del personal involucrado en el proyecto.

Recursos Software.-

- Software procesador de ofimática
- Gantt project.

Planificación de actividades.-

- Especificado en Anexo N° 6.

Presupuesto.- 40.000

Proyecto 2.-

Implementación de SIEM

Recursos Personal.-

- Oficial de Seguridad de la Información
- Gerente de Sistemas
- Jefe de Centro de Cómputo
- Técnico de Infraestructura
- Técnico de Telecomunicaciones

Recursos Hardware.-

- IBM Blade.
- Terminales de usuarios
- Equipamiento auxiliar de almacenamiento

Recursos Software.-
- OSSIM AlienVault
- Active Directory

Planificación de actividades.-
- Especificado en Anexo N° 7.

Presupuesto 80.000

Proyecto 3.-

Control de Accesos

Recursos Personal.-
- Oficial de Seguridad de la Información
- Gerente de Sistemas
- Jefe de Centro de Cómputo
- Técnico de Infraestructura
- Técnico de Telecomunicaciones
- Administrador de Base de Datos
- Administrador de Seguridad de la Información
- Personal Técnico de Proveedor

Recursos Hardware.-
- Appliance de Herramienta

Recursos Software.-
- Software de ofimática

Planificación de actividades.-
- Especificado en Anexo N° 8.

Presupuesto 35.000

Proyecto 4.-

Validación de transacciones de Base de Datos

Recursos Personal.-
- Oficial de Seguridad de la Información
- Auditor de Sistemas

- Gerente de Sistemas
- Administrador de Base de Datos
- Personal Técnico de Proveedor

Recursos Hardware.-
- Servidor de Base de Datos
- Appliance firewall de Base de Datos.

Recursos Software.-
- Software de Ofimática.

Planificación de actividades.-
- Especificado en Anexo N° 9.

Presupuesto 75.000

Proyecto 5.-

Implementación de TDM

Recursos Personal.-
- Oficial de Seguridad de la Información
- Gerente de Sistemas
- Jefe de Desarrollo
- Técnico de Infraestructura
- Técnico de Telecomunicaciones
- Administrador de Base de Datos
- Personal Técnico de Proveedor

Recursos Hardware.-
- Servidores de Base de Datos (ambiente desarrollo)

Recursos Software.-
- Software de Ofimática
- Herramientas para Test Data Management (Licuado de Datos)

Planificación de actividades.-
- Especificado en Anexo N° 10.

Presupuesto 60.000

Proyecto 6.-

Implementación de medidas de Encriptación.

Recursos Personal.-

- Oficial de Seguridad de la Información
- Gerente de Sistemas
- Jefe de Centro de Cómputo
- Técnico de Infraestructura
- Técnico de Telecomunicaciones
- Personal Técnico de Proveedor

Recursos Hardware.-

- Routers de Red

Recursos Software.-

- Software de Ofimática

Planificación de actividades.-

- Especificado en Anexo N° 11.

Presupuesto 15.000

7. Bibliografía.

7.1. Publicaciones de Normas.

1. UNE-ISO/IEC 27001, *Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad de la Información (SGSI). Especificaciones (ISO/IEC 27001:2005)*. España: AENOR, 2007. 35 Páginas.
2. NTP-ISO/IEC 17799, *EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª* Edición. Perú: INDECOPI, 2007. 174 páginas.

7.2. Otras Publicaciones

1. MAGERIT, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, I – Método.* Versión 2. España, 2006. 154 páginas
2. MAGERIT, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, II – Catálogo de Elementos.* Versión 2. España, 2006. 154 páginas
3. MAGERIT, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, III – Guía de Técnicas.* Versión 2. España, 2006. 154 páginas
4. HARRIS, Shon. *ALL IN ONE CISSP.* 6th Edition, USA: McGraw-Hill, 2012. 1430 pages. ISBN 978-0-07-178171-8
5. CÓRDOVA RODRIGUEZ, Norma Edith. *Plan de Seguridad Informática para una Entidad Financiera.* Argentina: Biblioteca Central UNMSM, 2007. 171 páginas.
6. INTECO-CERT. *Curso De Sistemas De Gestión De La Seguridad De La Información Según La Norma UNE-ISO/IEC 27000.* España: INTECO-CERT, 2010. 91 páginas.
7. CRESSON WOOD, Charles. *Políticas de Seguridad Informática - Mejores Prácticas Internacionales*, Version 9.0. Texas: NetIQ, Inc., 2002. 758 páginas. ISBN 1-881585-09-3
8. ANDRÉS, Ana y GÓMEZ, Luis, *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* España: AENOR, 2009. ISBN 978-84-8143-602-0.

7.3. Sitios Web.

1. Information Technology Security for Managers – IBM Global Service. http://www.ibm.com/services/securite
2. Information Security & Business Continuity Academy, Dejan Kosutic. http://www.iso27001standard.com/en
3. Lista de verificación para una auditoría a la seguridad Informática, Cristian Borghello. http://www.segu-info.com.ar/
4. El Portal de Iso 27001 en español. http://www.iso27000.es/
5. El Anexo de ISO 27001 en español. http://www.iso27002.es/

8. Glosario de Términos.

Mejor Práctica: Es la aplicación de controles o costumbres que han sido comunes o analizados e implementados en otras empresas de la misma naturaleza a la nuestra.
Ciclo de Deming: es conocido como el ciclo de mejora continua, es decir cada vez que el ciclo es completado, éste vuelve a iniciar; con el objetivo de aprender y mejorar sobre las actividades que ejecutamos al final.
Sistema de Gestión de Seguridad de Información (SGSI): es un conjunto de políticas de administración de la información, es el término utilizado principalmente en la Norma ISO/IEC27001, el concepto clave de un SGSI es gestionar eficientemente la información, buscando asegurar las dimensiones de Seguridad en los activos de información.
Activo de Información: Son los elementos, que pueden ser tanto físicos como lógicos y son gestionados por un SGSI.
Dimensión de Seguridad: Son conocidas como dimensiones de seguridad a la "triada" formada por los conceptos de Integridad, Confidencialidad, y Disponibilidad de la información
Valoración de Activos: Es la estimación cuantitativa o cualitativa de la importancia de un activo en un SGSI.
Amenaza: es todo aquello que puede causar daño o disminuir el valor de un activo para una empresa.
Vulnerabilidad: son todas las debilidades que puede tener un activo.