UOC – INSTITUTO INTERNACIONAL DE POSGRADO

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

RESUMEN EJECUTIVO

Autor:

Jorge Cástulo Guerrón Eras

Tutor:

Antonio José Segovia Henares

Loja, Enero de 2013

Tabla de contenidos

Resumen Ejecutivo

1. Introducción

El Banco de Loja consiente de la responsabilidad de entregar servicios financieros eficientes y de calidad a sus clientes; adaptándose a los innovadores y constantes cambios tecnológicos ha buscado siempre innovar y entregar servicios de calidad, sin dejar de lado la administración correcta de la información.

Hace más de una década el manejo de la seguridad estaba limitada y fácilmente administrada mediante el resguardo de documentos importantes a accesos físicos controlados, hoy es más difícil; la información no solo se almacena en documentos físicos, es cambiante en el tiempo gracias a la introducción de sistemas informáticos que nos acercan a la información pero que también la hacen más sensible.

El uso actual de servicios globales como el internet ha obligado a los sistemas de seguridad a evolucionar de tal manera que no solo se enfoquen en la protección de la información, hoy los sistemas de seguridad deben ser capaces de gestionar y reducir incidentes para evitar delitos, que permitan cuantificar gastos y pérdidas, minimizar impactos de riesgo.

Debemos ser conscientes que no son las computadoras o elementos autónomos los que atacan a las empresas; son las personas que desde un lugar en el mundo intentan obtener un beneficio, son de manera creciente los ex-empleados o empleados inconformes los que de una u otra manera intentan hacer que los sistemas de seguridad fallen como un objetivo propio de venganza o simplemente por el daño derivado de su inconformidad.

El presente plan no pretende asegurar que se resolverá los incidentes de seguridad en un 100%, el presente plan pretende de un modo objetivo y pro-activo, constituirse en la piedra angular de la "cultura de seguridad", de tal manera que nos ayude a sobrevivir en los escenarios más exigentes, permitiendo que sean los empleados quienes entiendan como reconocer, responder e informar un incidente.

"Las empresas pueden invertir miles de dólares en reforzar la seguridad física

y su infraestructura tecnológica; mientras no se concientice a los usuarios

la inversión será un gasto; las personas son

la vulnerabilidad más grave en cualquier empresa"

El Autor.

2. Proceso y ámbito de autoevaluación

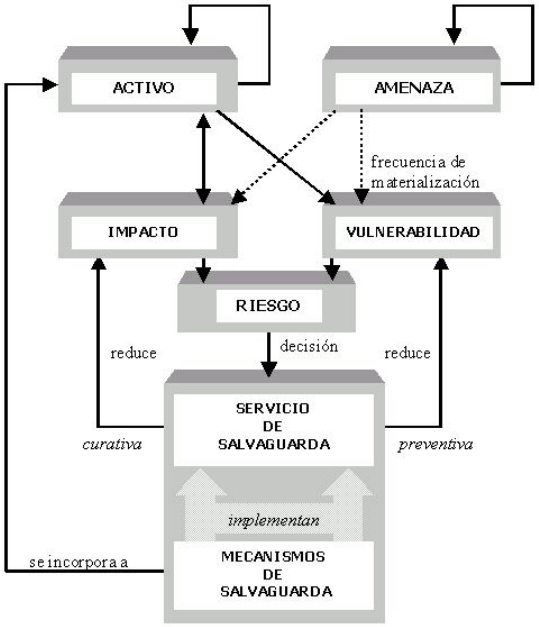
El Análisis de Riesgos se ha diseñado para identificar los activos y las medidas de seguridad utilizadas para mitigar los riesgos a los que se encuentra expuesto un activo. A partir de los problemas más comunes las empresas, se han visto en la necesidad de desarrollar una evaluación que permita validar los elementos que forman parte de los procesos y que son utilizados por el personal de la empresa. La valoración del riesgo al que la empresa está expuesta conforme al modelo y metodología seleccionados, permiten plantear una serie de preguntas para comprender como las medidas de seguridad que su empresa ha ido implantado a lo largo del tiempo, han formado capas de defensa, lo que proporciona una mayor protección frente a los riesgos de seguridad y las vulnerabilidades específicas. Cada capa contribuye a una estrategia combinada de defensa en profundidad (DiDI).

Para desarrollar la autoevaluación es esencial el desarrollo de un Plan Director de Seguridad, el mismo que se constituye en la herramienta que permite al Responsable de Seguridad gestionar de una forma adecuada la seguridad, al ejecutar ésta actividad no únicamente sabremos el estado de la empresa entorno a la seguridad, nos permitirá escalar a mejores prácticas y a un mejor ambiente de seguridad si nos enfocamos en estándares conocidos, en nuestro caso empleamos el conjunto de normas ISO 27000, y MAGERIT como metodología para la gestión de riesgo, si éstas poderosas herramientas las fusionamos con el modelo de mejora continua conocido como Deming o PDCA(Plan-Do-Check-Act).

Las actividades que se ejecutaron para alcanzar el Plan Director de Seguridad fueron:

- Analizar los procesos críticos del Banco, para obtener el inventario de activos.
- Valorar los activos de información y estudiar las amenazas a las que están expuestos.
- Calcular el impacto potencial de las amenazas sobre los activos.
- Analizar las salvaguardas y proponer un plan para minimizar el impacto de dichas amenazas.
- Valorar el nivel de cumplimiento de los controles de la norma ISO 27002.
- Luego de aplicar las salvaguardas, cálculo del riesgo residual.
- Iniciar nuevamente con el proceso para aplicar la mejora continua.

2.1.Gestión de Riesgos según MAGERIT



3. Resultados.

A continuación presento el resumen de las actividades realizadas.

3.1. Inventario y Valoración de Activos.

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

3.2. Impacto Potencial.

Anexo 1: Cálculo del Riesgo Actual.

3.3.Riesgo Actual.

Anexo 1: Cálculo del Riesgo Actual.

3.4.Selección de Salvaguardas.

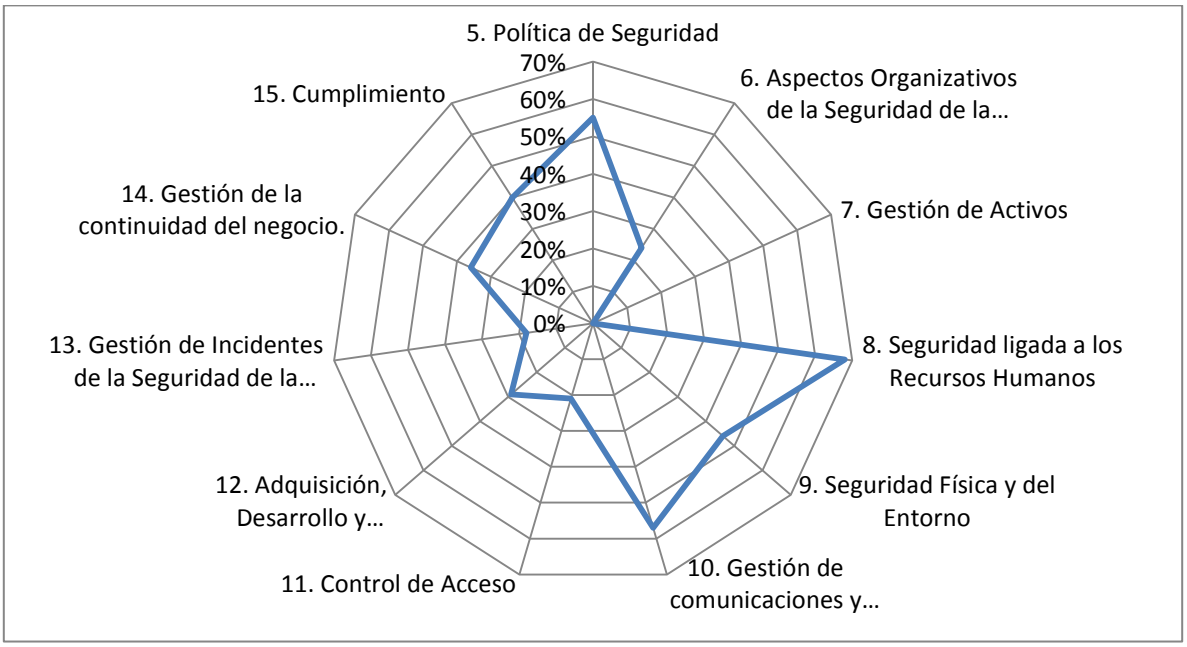
Anexo 2: Selección de Salvaguardas.

3.5.Riesgo Residual.

Anexo 3: Cálculo de Riesgo Residual.

3.6.Nivel de Cumplimiento ISO/IEC 27002:2005.

En el siguiente gráfico de radar presentamos el estado actual de cumplimiento, para más detalles ver Anexo 4: Cumplimiento ISO/IEC 27002:2005.



3.7.Cumplimiento Modelo de Mejora Continua.

Anexo 5: Cumplimiento PDCA.

4. Recomendaciones

- Recomendamos ejecutar de manera inmediata el proyecto de clasificación de activos, lo cual permitirá comprender de mejor manera como se están comportando los activos de información en los diferentes procesos del Banco de Loja.
- Recomendamos implementar controles que permitan mantener actualizado el inventario de hardware y software.
- Recomendamos implementar controles que permitan monitorear el estado de los elementos que conforman la red.
- Recomendamos implementar controles que permitan monitorear los eventos o posibles ataques a la infraestructura del Banco de Loja.
- Recomendamos implementar controles que permitan garantizar la integridad de los archivos de configuración de sistemas y servicios.
- Recomendamos implementar controles que permitan garantizar que los empleados que trabajan en las áreas de producción no tienen acceso a configuraciones y sistemas.
- Recomendamos implementar controles que permitan garantizar que los accesos o modificaciones de información en la base de datos principal del Banco de Loja, se encuentran debidamente sustentados.
- Recomendamos implementar en las áreas de Desarrollo y Pre- producción controles que eviten que los empleados del Banco de Loja tienen acceso directo a información sensible de los clientes.
- Recomendamos mejorar las medidas de control implementadas alrededor de los métodos de encriptación empleados que en algunos casos son muy básicos en otros se evidencio que son inexistentes.