MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA LAS ENTIDADES BANCARIAS

Rubio, Reyes Fabian Andrés.
Frubio8@hotmail.com
Universidad Piloto de Colombia

Resumen – La historia de la banca comienza con el primer prototipo de banco comercial con préstamos de granos para los agricultores y negociantes, con el pasar de los años y la inclusión de la tecnología, los bancos se han dedicado a proporcionar soluciones financieras con el más alto nivel de satisfacción y rentabilidad para los clientes, mejorando los productos por medio de metodologías móviles que permiten hacer transacciones en línea de una manera fácil y rápida, pero el mantener la información actualizada de los clientes, sus ahorros y sus futuros, han generado un interés particular en una serie de delincuentes informáticos que tienen como objetivo ingresar de manera no autorizada a esta información para obtener grandes beneficios.

Abstract - The history of banking begins with the first prototype commercial bank loans grain for farmers and traders, with the passing of the years and the inclusion of technology, banks have committed to providing financial solutions with the highest level satisfaction and profitability for customers, improving products through mobile methodologies to make online transactions easily and quickly. But keeping updated customer information, their savings and their futures, has developing a particular interest in a number of cybercriminals aim unauthorized manner enter to this information and get great benefits.

Índice de Términos - Implementación, lineamientos, modelo de Seguridad de la información, disponibilidad, confidencialidad, incidentes de seguridad, riesgo, gestión de riesgos, vulnerabilidad, integridad, no repudio, suplantación robo, ataques informáticos, contraseñas.

I. INTRODUCCIÓN

El diseño y la implementación de objetivos estratégicos y operacionales dentro del sector bancario para ser más competitivos, ofrecer el mayor número de soluciones transaccionales a sus clientes, incrementar su prestigio, alto nivel de satisfacción, calidad y rentabilidad, ha generado fallas en sus modelos de seguridad de la información, creando impactos en la reputación corporativa (productos y servicios), pérdida de confianza y retiro definitivos de los clientes de las entidades.

El hurto de dinero no es solo el objetivo principal de los ataques informáticos, de acuerdo a la motivación que puedan tener los atacantes, la información personal de los clientes, obtener el control de los ordenadores y aplicaciones del sistema bancario sin ser detectado, conocer y modificar los dispositivos físicos o lógicos para la protección de la información, denegación de servicios en línea, eliminación de reglas de seguridad configuradas en los cortafuegos (firewall) y la extracción de información confidencial, son algunas de las razones que generan inestabilidad en los modelos de seguridad de la información y que son conocidos y atacados por ciberdelincuentes, quienes desarrollan software malicioso (malware) para infiltrarse y causar el daño o un mal funcionamiento del sistema.

II. LAS AMENAZAS DE SEGURIDAD PARA EL SECTOR FINANCIERO

A continuación nombraremos y explicaremos algunos de los ataques más comunes a los que el sector bancario se enfrenta a diario.

A. Robo de identidad y contraseñas

Phishing. Por medio de un correo electrónico aparentemente enviado por el banco donde tiene sus cuentas de ahorro, solicitan una actualización de información y adicionan una URL que los direcciona a un sitio web con una interfaz similar a la que normalmente es usada para desarrollar las transacciones obteniendo: Nombre de usuario, contraseña, con esta información hacen la transacción del dinero a destinos desconocidos y cuando se identifica el robo, el banco notifica que no tiene responsabilidad alguna.

B. Robo por implementación de dispositivos a los cajeros electrónicos

Skimming. Este es un ataque que ha venido en aumento desde el momento en que se incluyen nuevos servicios a los cajeros, y es desarrolla con la adición de dispositivos físicos a los cajeros electrónicos, quienes por medio de la banda magnética de la tarjeta, capturan la información personal del cliente.

C. Infiltración de Software Malicioso

Malware para el Sistema bancario. Es un software desarrollado para infiltrarse en el sistema operativo utilizado por el banco y por medio de la adición de código fuente en las páginas web, generan pantallas adicionales a las normales para que el usuario genere un nuevo código de acceso y así capturan la información de la víctima.

D. Ingeniería Social

Clonación de tarjeta. Es una estrategia de manipulación a las personas que llegan a realizar una operación bancaria, y logran por medio de engaños generar confianza, conocer la clave de acceso al cajero y utilizando el método de skimming, completan el robo de dinero.

En la siguiente grafica se describen los sectores más afectados para Latinoamérica y su tendencia:

SECTORES	ATAQUES POR DIA	PORCENTAJE	TENDENCIA A FUTURO
FINANCIERO	6.600.000	75.29%	Aumentarán
GOBIERNO	925.600	10.56%	Aumentarán
COMUNICACION	737.200	8.41%	Se mantendrá
ENERGIA	325.347	3.71%	Descenderán
INDUSTRIA	173.900	1.98%	Aumentarán
COMERCIO	3.600	0.05%	Aumentarán
TOTAL	8.765.647	100%	

Figura 1. Sectores más Afectados de Seguridad en Latinoamérica.

III. ACTUALIDAD COLOMBIANA FRENTE AL CIBERATAQUE EN EL SECTOR BANCARIO

De los estudios realizados por las empresas especializadas en seguridad de la información para Latinoamérica, califican y resaltan a Colombia como un país de implementación y desarrollo tecnológico, capacidad de respuesta a incidentes de seguridad, adición de políticas a las leyes del Gobierno que incrementan la seguridad de los usuarios, y un mayor respaldo de inversión a la banca, sin embargo, Colombia es el tercer país con el mayor número de ataques informáticos 21,73% y el sector financiero registra el 14,34%, y es debido al desarrollo de aplicaciones móviles para transacciones en línea.

IV. ESFUERZOS DEL GOBIERNO COLOMBIADO FRENTE A LA SEGURIDAD DE LA INFORMACIÓN EN LOS ENTES BANCARIOS

La superintendencia financiera de Colombia continúa trabajando en la protección del consumidor financiero, y para esto incluye dentro de su sección de leyes la ley 1266 del 2008 que establece las condiciones generales del *habeas data* y regula el manejo de la información contenida en las bases de daos personales, en especial la financiera y crediticia que tienen los colombianos para conocer, actualizar y rectificar la información entregada a las entidades bancarias en cualquier momento.

Por su parte y esto debido al incremento de robo de la información, el Gobierno modificó el código penal e incluye la ley 1273 de 2009 llamada **de la protección de la información y de los datos**, que tiene como objetivo preservar la integridad de los sistemas que utilizan las tecnologías de la información y las comunicaciones. A continuación incluimos una tabla que describe los aspectos más importantes a tener en cuenta cuando se atenta contra la integridad – disponibilidad y confidencialidad de la información, incluyendo la sanción:

		SANCION	
ARTICULO	NOMBRE	PRISION	MULTA
269A	Acceso abusivo a un sistema informático	48 -96 MESES	100 A 1000 SML
269B	Obstaculización ilegítima de sistema informático o red de telecomunicación	48 -96 MESES	100 A 1000 SML
269C	Interceptación de datos informáticos	36 A 72 MESES	No Aplica
269D	Daño Informático	48 -96 MESES	100 A 1000 SML
269E	Uso de software malicioso	48 -96 MESES	100 A 1000 SML
269F	Violación de datos personales	48 -96 MESES	100 A 1000 SML
269G	Suplantación de sitios web para capturar datos personales	48 -96 MESES	100 A 1000 SML
269H	Circunstancias de agravación punitiva		

Figura 2. Ley 1273 De 2009.

V. COMO IMPLEMENTAR UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA SISTEMAS BANCARIOS

Como respuesta a los grandes y rápidos cambios tecnológicos, procesos de globalización y desarrollo económico, el diseñar e implementar un sistema de seguridad de la información para el sistema bancario, se convierte en una decisión estratégica que permite generar confianza a los clientes, continuidad en los procesos internos y aumentar la calidad de servicio.

El enlace de los objetivos específicos y estratégicos del banco, conocer su alcance, evaluar el modelo que actualmente es utilizado para proteger los activos tecnológicos entre otros, permitirá a los directivos tomar decisiones más acertadas sobre la necesidad de invertir en seguridad y así obtener el éxito dentro de la banca.

Para el autor del ciclo de deming2 (modelo para procesos de mejora continua) independiente del alcance que tenga el negocio, se deben monitorear y asegurar los mismos aspectos para controlar los riesgos de seguridad que tenga el banco. Este modelo es conformado por 4 fases: Planear – hacer – verificar - actuar y serán desarrolladas a continuación.

Pero antes de desarrollar las fases del ciclo de deming2, será incluida la norma internacional que describe la forma de gestionar la seguridad de la información ISO 27001.

VI. RESEÑA HISTÓRICA DE LA NORMA E IMPLEMENTACIÓN

Esta norma nace como fórmula de solución a la problemática del momento y a los reportes en pérdidas de los diferentes sectores, entre los que se encuentra el financiero por los ataques informativos de la época.

Preguntas como: ¿Cuánto pagaría su competencia por obtener la base de datos de sus clientes? ¿Está su empresa lista para afrontar un desastre natural y continuar entregando operaciones bancarias normalmente? ¿Los controles establecidos para proteger la información son efectivos?, han sido los interrogantes que hoy continúan siendo la base para seguir trabajando, mejorando e implementado la norma en los sistemas bancarios.

Dentro de las organizaciones, sin tener como base su objetivo comercial, se deben implementar mecanismos que permitan asegurar la confidencialidad, integridad, no repudio, el control de acceso y la disponibilidad de la información.

A. Confidencialidad

Asegura que la información no pueda estar disponible o ser conocida por personas ajenas a la empresa. Tiene como objetivo prevenir el acceso no autorizado de personas a la información.

B. Disponibilidad

Es el servicio que garantiza que la información para los usuarios autorizados que cuenta con acceso a los sistemas esté disponible y asegura que el sistema tenga los mecanismos de respaldo para una información precisa.

C. Integridad

Garantiza que la información no sea modificada, eliminada y que solo pueda ser consultada por el personal autorizado. Los datos siempre deben tener la información completa y con las características autorizadas por el dueño.

D. No Repudio
Es utilizado como evidencia por el emisor o receptor de los mensajes, para asegurar que la información si existe y si fue o no socializada.

E. Control de Acceso
Es un control que tiene como objetivo validar que el logueo a una aplicación sea hecha por el usuario dueño de este acceso y sea autenticado de manera correcta.

Luego de hacer una introducción sobre la norma, los pilares de la seguridad de la información, se inicia con la implementación del sistema de seguridad de la información, ¿Pero cómo es viable hacerlo?

La recolección de información con las diferentes áreas, una correcta evaluación de riesgos sobre los activos del banco, una asignando de criticidad a estos riesgos y la creación de mecanismos de control, podrán mitigar los problemas de seguridad de la información. Desafortunadamente ningún modelo de control asegurará un 100% de efectividad.

¿Por qué debemos implementar la norma?

El cumplimiento de los requerimientos legales, la obtención de un certificado que permita a la compañía está por encima de sus competidores, mitigar los incidentes de seguridad le permitirán evitar gastos adicionales en la remediación de problemas y una mejor organización en sus procesos, le permitirán estar más cerca de la excelencia.

PLANEACIÓN

A. Alcance
El alcance del proyecto será establecido por el banco de acuerdo a: Los objetivos, la proyección, necesidades, estrategias de expansión, la ubicación física de las sucursales y el apoyo administrativo, la clasificación de sus activos, los activos son todos aquellos elementos físicos o lógicos que hacen parte de un proceso, incluyendo los equipos de seguridad internos o externos, serán las bases para la asignación de los recursos económicos asignados a la implementación del sistema.

B. Política de Seguridad
La política de la seguridad de la información estará liderada por la alta gerencia y tendrá la responsabilidad de expresar de una forma clara y concisa los objetivos de seguridad, la inclusión de compromisos y la socialización a toda la compañía permitirá que todos los empleados comiencen a tener en cuenta este factor dentro de los procesos.

C. Inventario de Activos
El Inventario de los Activos para una posterior asignación de impacto, serán todos los procesos y herramientas utilizadas para que la entidad bancaria entregue el más alto nivel de calidad a los clientes en sus productos, tomando como primicia que la información almacenada en las bases de datos de cada banco, se puede catalogar como el activo más importante para su funcionamiento, la forma como se actualiza, la forma como es protegida de terceros, podrá ser un factor definitivo contra las otras entidades bancarias.

D. Análisis de Riesgos
El análisis de riesgos dentro de una organización bancaria y de acuerdo a la criticidad entregada en la asignación de los activos del banco con la información como su activo más importante, tiene como fin asegurar que el sistema de seguridad de la información logre alcanzar los resultados previstos, logre minimizar los impactos que se puedan presentar al normal funcionamiento de los sistemas y puedan trabajar de manera preventiva contra los ataques informáticos. La identificación y clasificación de los riesgos de acuerdo a su: Vulnerabilidad y amenaza, permitirán una correcta creación y puesta en marcha de los controles.

E. Riesgo
El riesgo lo podemos enunciar como el alto porcentaje que tiene una amenaza para explotar una vulnerabilidad detectada en un activo, causando una pérdida a la entidad bancaria.

1. Amenaza

Las Amenazas son las causas potenciales de un incidente no deseado sobre los riesgos ya identificados.

2. Vulnerabilidad

Las vulnerabilidades las podemos expresar como las debilidades de los activos.

3. Impacto

El impacto lo definimos como la consecuencia de la explotación de una vulnerabilidad en un activo.

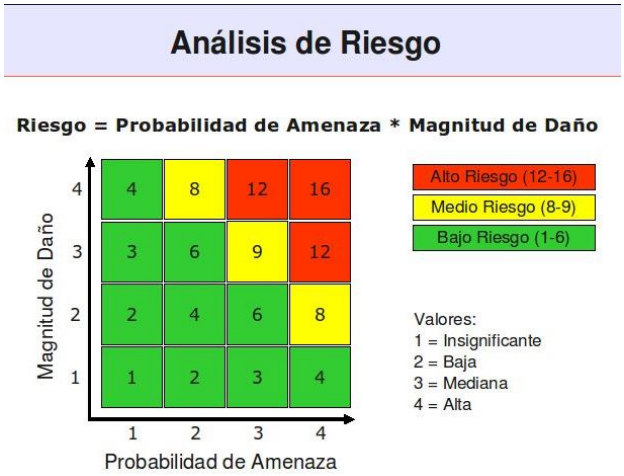

Figura 3. Análisis de riesgo.

4. Plan de Tratamiento de Riesgos

El plan de tratamiento de riesgos será definido de acuerdo a los resultados obtenidos en la clasificación de los riesgos y a la magnitud del daño, y tendrá como objetivo la creación de los controles para mitigar estos impactos al sistema bancario.

HACER

A. Ejecución: Tratamiento de Riesgos

Para ejecutar el plan de tratamientos de riesgos se tendrán en cuenta las siguientes características en la generación de controles:

1. Ser coherentes con las políticas de seguridad.
2. Deben ser medibles.
3. Tener una actualización de acuerdo a lo estipulado.
4. Asignación de responsables.
5. Documentación.
6. Descripción de cómo se evalúan los resultados.
7. Cuando finaliza y Forma de mostrar a la gerencia los resultados.
8. Implementación de mecanismos que aseguren que la vulnerabilidad no podrá ser explotada como (personas – herramientas de monitoreo).
9. Evitar el riesgo será una característica que podrá hacer la diferencia frente a la competencia.
10. Transferir el Riesgo a terceros. (proveedores Outsourcing de servicios tecnológico, compañías de seguros).
11. Implementación de recursos físicos.

B. Implementación de la Política de Seguridad

La implementación de las políticas de seguridad estarán ligadas a los objetivos del negocio, su visión, la concientización del personal del ente bancario y a los principios operativos, éticos y económicos que tienen como fin lograr el bien común, haciendo énfasis en la importancia de la seguridad.

Aspectos claves a tener en cuenta:

1. Debe ser redactada pensando en que será leída e interpretada por todo el personal del banco, incluyendo los objetivos generales y los objetivos de la dirección.
2. Debe ser de Dominio Público.
3. Debe incluir las reglas adoptadas por la empresa de acuerdo a las leyes del país.
4. Debe especificar las responsabilidades que cada empleado debe cumplir.
5. La forma como serán castigados estos incumplimientos (consecuencias).
6. Gestión de continuidad del negocio.
7. Requisitos que se debe cumplir para acceder a los sistemas de información de los clientes.

C. Plan de Concientización

El plan de concientización en seguridad de la información estará basado en las estrategias de sensibilización y divulgación de las policías de seguridad, generando un alto compromiso al interior del banco. Pero para poder implementar este

método de sensibilización debemos tener un punto de partida y conocer cómo está el banco a hoy en temas de seguridad, que otras compañas han sido ya desarrolladas, que resultados se tienen y así establecer cuál es la mejor forma de desarrollar la actividad. Un ejemplo práctico de cómo desarrollar una estrategia es SARLAFT (sistema de administración de riesgo de lavado de activos y de la financiación del terrorismo) desarrollado por la superintendencia financiera de Colombia, la cual por medio de imágenes, ayudas web y acompañamiento, explica lo que es y las consecuencias de incumplirlo. Esto permitirá comenzar a tener en cuenta los aspectos más importantes del SGSI que está siendo implementado.

D. Gestión de Recursos Humanos

La gestión de los recursos estará liderada por la dirección quien es la encargada de proveer los recursos necesarios para el establecimiento, implementación y mejora continua del modelo implementado de seguridad de la información, asegurando que cada uno de los asignados para un rol y un fin específico, cuenta con las capacidades técnicas y profesiones suficientes para saber cómo actuar en los diferentes escenarios de ataques informáticos que se puedan presentar, el monitoreo de alarmas, conocer su tratamiento y la forma de mitigar el daño al sistema bancario, permitirá reflejar en los reportes de calidad y seguimiento la efectividad del modelo.

E. Gestión de la Operación

La gestión de la operación estará ligada a las políticas de seguridad de la información y será la encargada de planear, implementar y controlar los procesos, tendrá la tarea de documentar todos los problemas a los que la seguridad se ve expuesta, y estará disponible para auditorías internas como externas. Todo cambio programado a la infraestructura tendrá una aprobación de la dirección, head de área y especialista de seguridad del ente bancario, con el objetivo evitar crear una vulnerabilidad a un activo o interrumpir de forma no controlada al normal funcionamiento de las aplicaciones. Al final de cada ejercicio de implementación, actualización o mejora tendrá una presentación de resultados, positivos o negativos que cumplirán las funciones de lecciones aprendidas.

VERIFICAR

El gran desarrollo tecnológico, la implementación de nuevas tecnologías con un mayor rendimiento económico para los clientes y la forma como estos pueden facilitar las transacciones bancarias, generan cambios significativos a lo ya planteado en la fase 1 y 2 del modelo, sin embargo, un plan de monitoreo podrá permitir identificar la efectividad, robustez y seguridad del sistema de gestión de seguridad implementado, a continuación los factores a validar.

A. Verificación de controles

La verificación de los controles implementados por medio la forma como son monitoreados, la estructura que se tiene para una correcta actualización, el proceso de notificación de cambios o de errores identificados, la comunicación de eventos a la gerencia por medio de reportes mensuales, el correcto nivel de criticidad asignado a los activos del banco y la actualización de los activos en momentos en que se adicionen nuevos productos a los clientes, permitirán conocer la eficiencia y eficacia que se tiene en el modelo y generara una gran tranquilidad a sus clientes.

B. Reportes a la Alta Gerencia

Los reportes a la dirección o alta gerencia con los resultados de los controles desarrollados, explicando su periodicidad, su distribución por niveles de impacto y la forma como fueron mitigados, permitirán aprender de las experiencias, la divulgación a todo el equipo de trabajo sobre los resultados de la sensibilización, los métodos utilizados y las proyecciones esperadas, permitirán dar tranquilidad al negocio. Esto también aplica para los bancos que no solo tienen sucursales en Colombia, estos reportes con un alto número de efectividad, son adaptados a sus casas matrices.

C. Auditoría al Sistema

Las auditorías al SGSI brindan una gran oportunidad de mejora al modelo y tienen como fin detectar por medio de hallazgos sobre las evidencias entregadas de los monitores a los procesos, si los controles están siendo desarrollados de manera correcta y cumplen con las políticas de seguridad creadas para el ente bancario. Estas auditorías están divididas como internas, las cuales son desarrolladas por un grupo de auditores certificados en la norma, certificación respaldada por la compañía y permiten a la alta gerencia conocer el estado actual de la seguridad de sus activos, también es desarrollado por algunos bancos auditorías con entes externos y tienen como fin la certificación del modelo, esto genera un mayor grado de tranquilidad a los clientes.

Como ejemplo: El 17 de Febrero del 2015 BANCOOMEVA por medio del líder mundial en servicios de certificación y auditoría BUREAU VERITAS, obtuvo el certificado de su sistema de gestión de seguridad de la información (SGSI), bajo la norma ISO 27001-2013 y este fue el mensaje publicado en sus medios de comunicación:

“El certificado demuestra que el banco ha tomado las precauciones necesarias para proteger la información sensible contra riesgos potenciales, accesos y cambios no autorizados”

ACTUAR

Como cierre de la implementación de este modelo de SGSI a los sistemas bancarios y con el objetivo de no perder lo ya desarrollado en cada fase, el actuar se basa en la implementación, mejora y seguimiento a las acciones correctivas- preventivas identificadas en las auditorías, reportes a gerencia y experiencias con los empleados del banco, la socialización de los resultados obtenidos con los empleados, el seguimiento a los cambios hechos a los activos del banco, permitirán tener una política cada vez mejor y más competitiva frente a los otros bancos establecidos en Colombia.

VII. DISCUSIÓN

La implementación de la seguridad de la información en los entes bancarios es ahora una prioridad, el proteger la información de los clientes de actos delictivos, generar confianza por medio de ejemplos como el expresado con el banco COOMEVA, demuestran la forma de ver el futuro que tendrán las entidades financieras.

Pero la exposición a nuevos riesgos que actualmente tienen los bancos es mayor por el desarrollo de las tecnologías, el incremento de almacenamiento, la generación de páginas web para ofrecer sus productos, los servicios móviles actuales que son utilizados como zonas transaccionales, la disminución de dispositivos de autenticación asignados por el banco, y la instalación de estos métodos de autenticación desde el celular a los productos, crean modificaciones constantes a las configuraciones ya preinstaladas por los directores de la seguridad en las compañías llamados BISO o TISO.

Pero la problemática que podríamos tener hoy en día seria: ¿Deberían todas las entidades financieras estar certificadas en un SGSI por un líder mundial en servicios de certificación y auditoría como BUREAU VERITAS?

Al no estar mi banco certificado en este modelo de seguridad, ¿Debo estar tranquilo de la información proporcionada cuando inicie con los productos ofrecidos?

Con el objetivo de responder a las preguntas previamente realizadas, es importante aclarar que un SGSI eficiente dentro de un ente bancario, siempre va a estar expuesto a riesgos que pueden ser explotados, y que lo importante del modelo ya este certificado o no, es tener la forma de minimizar las consecuencias del daño y trabajar en conjunto con los clientes para evitar que se vuelvan a presentar.

VIII. CONCLUSIONES

Este artículo tiene como meta crear una conciencia de seguridad a los sistemas bancarios que actualmente ofrecen sus servicios en Colombia. Este modelo de seguridad de la información se basa en la normativa creada por la ISO 27001, y desarrolla de una manera clara y precisa las fases de implementación. El desarrollo y adición de nuevas tecnologías para generar daño a las entidades bancarias, incrementan el riesgo de seguridad para sus clientes, las amenazas ya detectadas por los controles implementados en cada organización pueden llegar a no ser suficientes y un impacto de reputación sobre niveles de confianza que manejan los entes bancarios, podría ser el fin de las operaciones.

Teniendo como prioridad los pilares de la seguridad de la información arriba descritos, los sistemas bancarios tienen la responsabilidad y obligación de proteger la información personal de sus clientes, la implementación de nuevas herramientas web para acceder a los servicios transaccionales y la facultad de crear controles de seguridad de acuerdo a sus activos tecnológicos de una manera acertada, contando con el respaldo de la alta gerencia, la sensibilización de todo el equipo de trabajo y siempre cumpliendo los estándares de seguridad registrados en las políticas de seguridad, aseguran el éxito del sistema de gestión de la seguridad de la información y como se explicó en algunos apartes del artículo, el objetivo de este SGSI no será evitar que se presenten incidentes de seguridad, la prioridad es aprender a actuar de una manera preventiva y tener definido los planes de mitigación para que las interrupciones a los sistemas o el daños que logren vulnerar un control, buscando que no se generen interrupción al correcto funcionamiento de los sistemas y que de las lecciones aprendidas identifique las falencias que actualmente se pueden tener y continuar trabajando en fortalecer los controles para evitar que se vuelva a presentar. Esta es una de las muchas ventajas que podrá tener el sistema bancario que observe la seguridad como plus adicional ante la competencia.

REFERENCIAS

[1]. “Tecnología de la Información. Técnicas de Seguridad”, ISO 27001, 2013. Disponible: http://www.iso.org/iso/home/search.htm?qt=iso+27001&sort=rel&type=simple&published=on

[2]. The Cyber Threat to Banking, “A global Industry Challenge”, (2014, Noviembre). Disponible en: https://www.bba.org.uk/.../the-cyber-threat-to-banking-a-global-i.

[3]. “Advancing Technology for Humany”, IEEE, (2013, Noviembre). Disponible: http://www.ieee.org/index.html

[4]. Antonio Huerta. “Introducción al análisis de Riesgos”. 30 de Marzo 2012. Disponible en: http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

[5].Ley 1273 Del 2009. República de Colombia. 5 de Enero del 2009. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[6]. Superintendencia Financiera de Colombia, la ley 1266 del 2008 disponible en: https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=19166

FIGURAS

[Figura 1]. Sectores más Afectados de Seguridad en Latinoamérica. Disponible en: https://blogaxon.com/2015/09/25/en-el-ultimo-ano-el-sector-financiero-paso-a-ser-el-mas-atacado-en-seguridad-informatica/

[Figura 2]. Ley 1273 De 2009. Código Penal. República de Colombia. 5 de Enero del 2009 Disponible:http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[Figura 3]. Markus Erb, M. (2008). Análisis de riesgo. Disponible: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/