

# Metodología Para Implantar Seguridad de la Información en una Empresa Financiera en El Salvador

(Enero 2015)

Carlos A. Najarro A., Ermides U. López, Linda J. Ibarra de Martínez  
[cnajarro05@gmail.com](mailto:cnajarro05@gmail.com), [ermides@gmail.com](mailto:ermides@gmail.com), [libarra04@gmail.com](mailto:libarra04@gmail.com)  
Universidad Don Bosco

Con formato: Posición: Horizontal:  
1.5 cm, Con relación a: Página, Ancho:  
Exacto 18.49 cm

Código de campo cambiado

Código de campo cambiado

Código de campo cambiado

## 1-1 Las Entidades Financieras en El Salvador registradas por la Superintendencia del Sistema Financiero

*Resumen - La Seguridad de la Información, reviste vital importancia para las entidades financieras, bancos, que debe adoptarse y para ello existen varias normas y/o estándares de aceptación internacional emitidas por organismos de sumo prestigio, pero que normalmente exponen lo que hay que hacer y no el cómo. Por otra parte siendo algo tan importante y delicado, que implica el involucramiento de toda la organización, se presenta la disyuntiva de cuál norma y/o estándar seleccionar cómo el más idóneo para la entidad. Presentamos una metodología para seleccionar la norma o estándar que mejor cubra los aspectos de Seguridad de la Información enfocados en una entidad financiera, banco, en El Salvador.*

### Palabras Clave:

Seguridad de la Información - SGSI

Gestión de Riesgos

Tecnología de la Información – TI

ISO/IEC 27002 (Normas Internacionales consideradas estándar)

COBIT 5 Objetivos de Control para la Información y

Tecnologías Relacionadas

ITIL v.3 Biblioteca de Infraestructura de Tecnologías de la Información.

Procesos (se refiere al procedimiento repetitivo de ejecutar un operación)

Servicios, los prestados a los usuarios de la entidades financieras

Controles Primarios o Relevantes, aquellos de mayor impacto al ser trastocados

Controles Secundarios, importantes pero en menor escala que los primarios

En El Salvador, el ente rector de las entidades financieras es la Superintendencia del Sistema Financiero – SSF, que en adelante consignaremos como SSF, quien tiene como objetivo preservar la estabilidad del sistema financiero, y velar por la eficiencia y transparencia del mismo; todo en concordancia con las mejores prácticas internacionales.

Vamos a centrarnos en las entidades Financieras, específicamente bancos, dado que tienen relación directa con aspectos de la operatividad de las cuentas de depósitos y cartera de préstamos, más otras transacciones relacionadas con la circulación del efectivo, lo cual implica manejar extensas y sensitivas bases de datos de las personas y cuentas que hacen uso de estos servicios, aún, cuando por la naturaleza de la transacción en sí, no se tipifiquen como clientes, tal es el caso de los usuarios de remesas familiares que representa un rubro importante en cuanto al ingreso y circulación de efectivo, parte significativa del ingreso para miles de personas, como se evidencia el cuadro del Anexo 1.<sup>1</sup>

Las entidades Financieras registradas por la SSF, que totalizan 39, las segrega en varios grupos, así; Bancos Privados, Bancos Cooperativos, Asociaciones de Ahorro y Crédito, Casas Corredoras de Bolsa que solo intermedian Valores, Casas Corredoras de Bolsa que Intermedian Valores y Administran Cartera, Aseguradoras Certificadas y nosotros hemos incluido un apartado de “No referidos por la SSF”, entidades existentes o en formación, pero de pleno conocimiento del público.

## 1-2 Servicios que prestan las Entidades Financieras en El Salvador y su interrelación entre diferentes entes

Con el propósito de hacer notar la importancia que se le debe dar a las entidades financieras, estimamos conveniente resaltar

## 1. EL ESTADO ACTUAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL SALVADOR Y LAS REGULACIONES LEGALES Y/O INTERVENCIÓN.

<sup>1</sup> <http://www.bcr.gob.sv/esp/>

los diferentes servicios que prestan, aun cuando no todas prestan la totalidad de dichos servicios.

En El Salvador de hoy día, con el auge que ha tenido la bancarización, en que el grueso de la población, independientemente de su nivel socio económico hace uso de los servicios bancarios, a diferencia del pasado, en la actualidad se estila pagar los sueldos y salarios con abono en una cuenta bancaria y la persona obtiene efectivo por medio de los cajeros automáticos de los correspondientes bancos. Esto es lo que ha llevado a distintas entidades financieras a prestar servicios cada vez menos tradicionales a los de captación y/o colocación de fondos, a la vez que se esgrime con mucha definición el concepto de servicio al cliente, evidenciado en los servicios mismos y/o en los horarios de atención en ventanilla, que en algunos casos es de lunes a domingo, también debemos hacer notar una alta competencia por la cercanía de los servicios ya sea en la modalidad de; Banca por Internet, Kioscos de autoservicio, Cajeros Automáticos (ATM's), Servicios de Call Center, Banca móvil (por teléfono) y últimamente con el apareamiento de los Corresponsales Financieros, que se complementan con las tradicionales Agencias, mini Agencias, etc., permitiendo con ello “llevar” hasta el cliente, los servicios que prestan dichas instituciones, en la mayoría de los casos sin limitaciones de horarios ni restricciones de fechas.

Lo anterior pone en evidencia que las entidades financieras hacen uso de potentes, extensos y complejos recursos tecnológicos para poder brindar el servicio las veinticuatro horas del día, siete días a la semana en forma presencial o virtual por medio de los llamados canales electrónicos, para lo que se necesita una infraestructura tecnológica que permita almacenar, transmitir o recibir datos e incluso el intercambio de datos entre instituciones de diferente índole en virtud de; disposiciones legales, reglamentos, normativas, convenios de negocios y por supuesto mantener un nivel de servicio acorde a las exigencias de los usuarios y en atención a la competencia que las otras entidades financieras representan.

Esta infraestructura que en muchos de los casos rebasa la interacción dentro de la entidad misma, permite funcionar los puntos de servicio (agencias, mini agencias, cajeros automáticos, kioscos de autoservicio, corresponsales financieros, etc.), también implica la conectividad necesaria para el intercambio de datos entre instituciones, en algunos de los casos por mandato de ley, como lo es la “Consulta Tributaria” de quienes están presentando una solicitud de crédito por montos ya especificados en la ley correspondiente. A continuación una gráfica que esboza dicha infraestructura, Anexo 2.

Igualmente se puede inferir que ello implica manejar bases de datos que contengan enormes cantidades de datos sensibles los cuales deben estar adecuadamente protegidos, entendemos que muchas de las entidades financieras han implantado ya sea por su propia iniciativa, atención a buenas prácticas o por instrucciones de sus respectivas casas matrices (filiales de transnacionales, que en su mayoría fueron bancos de El Salvador vendidos a esas transnacionales), medidas de

seguridad de la información, en ciertos casos en razón de cumplimiento, con entes internacionales, externos.

Además se prestan servicios de Tarjetas de Crédito de reconocidos Concesionarios de este tipo de franquicias a nivel internacional, en cuyo caso por una condición propia de este rubro de negocios, se ha implantado una normativa específica de Seguridad conocida como “PCI-DSS – Payment Card Industry Data Security Standards”. Vale comentar que dicha normativa se focaliza en aspectos propios del giro de Tarjetas de Crédito y/o Débito, tal como la seguridad del PIN, el enmascaramiento de los números de las tarjetas y el transporte seguro de los datos, que la mayoría de entidades ofrecen como producto y en otros casos se limita a servicio.

No obstante la normativa PCI-DSS, no es apta para ser tenida como una norma o estándar de seguridad aplicable a la Seguridad de la Información en forma integral y a todas las aplicaciones que utilizan las diferentes entidades financieras. Para clarificar un poco más sobre la diversidad de servicios de las entidades financieras, presentamos el siguiente cuadro en el que hemos incorporado los servicios que prestan las diferentes entidades, Anexo 3. Fuente [www.ssf.gob.sv](http://www.ssf.gob.sv) e información recaba por nosotros.

En el cuadro del Anexo 3, se destaca que en adición a los típicos servicios bancarios de captación y colocación de fondos, los bancos hoy día presentan una gama de servicios que facilitan al cliente y público en general acceder al banco por medio de canales electrónicos e incluso virtuales, tales como; Cajeros Automáticos, Kioscos de auto servicio, Banca por Internet, Aplicaciones para móviles (teléfonos celulares inteligentes), Centros de Llamados (Call Center), Corresponsales Financieros, Tarjetas de Créditos, Medios Electrónicos de Pagos (SICE), Tarjetas de Débito, etc.

### **1-3 Normas Prudenciales para Bancos emitidas por la Superintendencia del Sistema Financiero de El Salvador**

La Superintendencia del Sistema Financiero tiene como competencia cumplir y hacer cumplir las leyes, reglamentos, normas técnicas y demás disposiciones legales aplicables al sistema financiero, monitorear preventivamente los riesgos de las instituciones integrantes, propiciar el funcionamiento eficiente, transparente y ordenado del sistema financiero, vigilar que las instituciones supervisadas realicen sus negocios, actos y operaciones de acuerdo a lo establecido en la legislación vigente, dando continuidad a una supervisión y regulación que anteriormente realizaban las Superintendencias del Sistema Financiero, Pensiones y Valores.

La SSF, publica y hace del conocimiento de las entidades financieras las “NPB- Normas Prudenciales para Bancos”. Las cuales aplican a los Bancos Privados, los Bancos Cooperativos, Sociedades de Ahorro y Crédito, Casas Corredoras de Bolsa y Administración de Cartera, Aseguradoras, etc.

Para este trabajo, es de interés primordial, dos de estas NPB y son; la NPB4-47 Normas para la Gestión Integral de Riesgos de las Entidades Financieras y la NPB4-50 Normas para la Gestión del Riesgo Operacional de las Entidades Financieras.

En la NPB4-47 Normas para la Gestión Integral de Riesgos de las Entidades Financieras, no encontramos referencias puntuales relativas los riesgos que implican la Seguridad de la Información ni cómo administrarlos a pesar de su importancia directamente relacionada con la colocación de fondos y administración de cartera.

En la NPB4-50 Normas para la Gestión del Riesgo Operacional de las Entidades Financieras, encontramos menciones a recursos de tecnología de la información y procesos básicos propios de la Seguridad de la Información, aunque sin entrar en detalles sobre como implantarlos o hacer cumplir lo especificado ni de los exámenes sobre los mismos por parte de la SSF.

Para ilustración del universo de las NPB, adjuntamos el siguiente cuadro del Anexo 4<sup>2</sup>

#### **1-4 Recursos de Tecnología de la Información enunciados en diferentes leyes de El Salvador**

En la legislación de El Salvador tenemos una serie de consignaciones relacionadas con el uso y aplicaciones de la Tecnología de la Información, sin llegar a establecer un marco regulatorio integrado aplicable al uso de los recursos de tecnología de la información.

Encontramos contenidos enunciados en leyes de El Salvador relativos a recursos de Tecnologías de la Información en los que el legislador aborda dicha temática con enfoques desde conceptualizaciones generales hasta algunas transacciones electrónicas y la forma como deben ejecutarse, sin profundizar en lo relativo a la seguridad de la Información, no obstante llega a tipificar ilícitos que puede generarse por el uso voluntario o no de dichos recursos sin entrar en detalles ni en un enfoque integral de seguridad.

Como caso extremo se llega a tipificar “Actos de Terrorismo” algunos usos genéricos de ciertos recursos de TI, sin ahondar en aspectos primordiales técnicos, asumiendo conocimiento de los mismos por parte de los individuos que aplican la ley.<sup>3</sup>

Se evidencia la no existencia de una metodología cierta sugerida por los entes rectores, para el caso la SSF, o mejor aún contenida en una ley de la República que comprenda la

seguridad de la información en términos generales para todo tipo de institución y no limitado a las entidades financieras.

Nuestro enfoque de una Metodología para seleccionar una norma o estándar para Implantar Seguridad de la Información en las Entidades Financieras en El Salvador, se explica por la trascendencia de lo sensitivo de los datos que reciben, almacenan, procesan, transmiten y distribuyen, que de no tener implantada una seguridad cierta, puede ser objeto de usos indebidos por parte de personas autorizadas o no para acceder a ellos dentro y fuera de las entidades financieras, lo que puede impactar negativamente en el usuario de los servicios financieros y puede repercutir incluso en acciones delincuenciales con impacto negativo directo en la imagen institucional, y en algunos casos afectar las utilidades del ejercicio.

En caso de sucederse un fraude, evidenciado ya sea por los controles internos o denunciado por el usuario, se procede, de acuerdo al marco legal vigente y la experiencia demuestra que en los casos que se judicializan, estos se ventilan como delitos comunes y no de acuerdo a su verdadera naturaleza, delitos cibernéticos.

Es importante tener en cuenta algunos aspectos básicos de la tecnología de la Información para con ello evidenciar vacíos en la legislación vigente en El Salvador y que de alguna forma, ya algunos recursos tecnológicos y/o transacciones, se han mencionado en ciertas leyes, aunque con un propósito específico, la recaudación de impuestos, estos aspectos primordiales son; almacenamiento de los datos, certificados y firmas digitales, no repudio, etc., que ante el alto crecimiento en el uso de recursos de tecnología de la información, y proliferación de aplicaciones móviles demandan un mayor esfuerzo por implantar seguridad de la información por la alta exposición a riesgos tecnológicos y pérdidas monetarias, algunos de estos aspectos son:

##### **1.4.1 Almacenamiento de Datos**

En El Salvador ya se discute entre los especialistas conceptos como “Big Data”, provocado por el crecimiento de las operaciones y servicios de las empresas o por regulaciones de carácter internacional como los Acuerdos de Basilea (aplicable a los bancos), pero no encontramos más que una alusión a base de datos en la Ley de Simplificación Aduanera, promulgada en 1999, que menciona en su artículo 8-b “Base de Datos de acceso privado”.<sup>4</sup>

También encontramos referencia a los medios de almacenamiento de información en la sección sexta del Código Procesal Civil y Mercantil en alusión a los medios de prueba en las diligencias judiciales.<sup>5</sup>

<sup>2</sup> <http://www.ssf.gob.sv/index.php/normativa/normas/513-normas-prudencia-bancos>

<sup>3</sup> Ley Especial contra Actos de Terrorismo  
Art. 12 Delito Informático y art. 46 Régimen de las Pruebas

<sup>4</sup> Ley de Simplificación Aduanera  
art.8-b Bases de Datos de acceso privado

<sup>5</sup> Código procesal civil y mercantil  
ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR  
18 de Septiembre de 2008

Figuras delictivas como fraude, robo de información, ventas de bases de datos y otros concretan su accionar mediante la modificación de datos en dichas bases por personas autorizadas o no para acceder a los datos, que lo hacen con dolo sin que el legislador se haya ocupado de dichas acciones y sus efectos.

Por otra parte, desde 1995, en El Salvador, el uso de las tecnologías de Internet ha venido creciendo de una forma acelerada demandando regulación para protección legal. El uso arbitrario de un banco de datos puede afectar derechos fundamentales, el problema es que no se sabe cuántos se habrán enterado de la divulgación de sus datos personales, y nadie sabe en qué momento van a ser utilizados y de qué manera, ante lo que surgen las siguientes preguntas:

-¿Quién vende esa base de datos?

-¿Cómo obtuvieron esa información personal?

#### 1.4.3 Certificados y firmas digitales

De igual forma la Ley de Simplificación Aduanera manda funcionar entidades Certificadoras que crearán y certificarán, certificados digitales y manda a los usuarios del sistema que implantó Teledespacho, el uso de firmas digitales públicas para que los usuarios del sistema puedan tramitar lo relativo a importación de mercancías, incorporando la figura de fehaciente a lo contenido en los registros electrónicos del sistema y la responsabilidad irrevocable de los usuarios mediante el uso del usuario y clave asignados para operar remotamente el sistema, y de esa forma agilizar los trámites de retiro de mercaderías de las aduanas.<sup>6</sup>

Este aspecto está reconocido a nivel país a tal grado que se ha presentado a la Asamblea Legislativa un anteproyecto de “Ley de la Firma Electrónica” para usos generalizados en la emisión de facturas electrónicas y el fondo, una vez aprobada dicha ley, se pueda garantizar la legalidad en la utilización de la tecnología para las relaciones entre los diversos actores de la sociedad, tanto a nivel local como internacional, que incluye, entre otros, un alto componente de negocios y gestiones gubernamentales. Más allá de la reducción de tiempos e la comunicación, la Firma Electrónica tiene la virtud de ser un mecanismo de transparencia proporcionando el máximo grado de confidencialidad y seguridad en internet.<sup>7</sup>

El Salvador, ya tiene en el Gobierno Central algún avance en este aspecto, aunque focalizado en la recolección de tributos y algunos Gobiernos municipales han incurrido en la atención a los ciudadanos por medio de redes informáticas

<sup>6</sup> Ley de Simplificación Aduanera

Art. 1-A Transición electrónica art. 6 Teledespacho art. 7 Uso de medios informáticos y de la vía electrónica art. 8 Entidades certificadoras Pareja de llaves, una pública y otra privada “Criptografía” art.8-a Funciones de las entidades Certificadoras.

<sup>7</sup> Secretaría para Asuntos Legislativos y Jurídicos de la Presidencia (2012).

“DOCUMENTO EXPLICATIVO DEL ANTEPROYECTO DE LEY DE FIRMA ELECTRÓNICA EL SALVADOR”

interconectadas electrónicamente entre sus diferentes sedes, que representan aspectos relacionados con el surgimiento del Gobierno Electrónico.

#### 1.4.4 Alto crecimiento en el uso de recursos de las tecnologías de la Información

El desarrollo tecnológico que se aplica a todos los recursos de la Tecnología de la Información, aunado a los esfuerzos de integrar la población estudiantil en el conocimiento y uso de dichos recursos, plantea una utilización masiva de dicha tecnología y por ende una mayor y urgente necesidad de que su uso esté legislado en forma integrada, para evidenciar dicha circunstancia hacemos referencia a tres leyes propias de la Tecnología de la información que exponen dicho crecimiento a nivel general, estas son:

- a) La Ley de Moore, la cual planteó en 1965 que aproximadamente cada dos años, se duplicaría la capacidad de los microprocesadores en una computadora, lo cual, haría caer el precio de las computadoras.
- b) Ley de Metcalfe, la cual establece que el valor de una red de comunicaciones aumenta proporcionalmente al cuadrado del número de usuarios del sistema. Es decir, que el valor de acceder a Internet aumenta cuando se incrementa el número de usuarios y de servicios conectados a la red.
- c) Ley de Gliddens, la cual dice que el ancho de banda de los sistemas de comunicación, se triplicará cada 12 meses, permitiendo así transferir o bajar archivos más grandes.<sup>8</sup>

Lo anterior denota la urgente necesidad de una adecuada regulación / legislación sobre el uso de los recursos de la Tecnología de la Información – TIC, y de la Seguridad de la Información, dada una realidad concreta de la proliferación de aplicaciones móviles, sobre todo que ambos aspectos están en su etapa de inicio y se espera un crecimiento sustancial, aspecto que igualmente no ha sido debidamente regulado ni legislado.

El legislador ha intentado tipificar desde la perspectiva jurídica y ante la realidad nacional, esperemos sea transitoria, la figura del delito informático, aunque tratado de una forma compleja para los propósitos de salvaguardar la seguridad de la información, porque dicho aspecto está contenido en la “Ley Especial contra Actos de Terrorismo”, que engloba como es de suponer otros aspectos delictivos relacionados o no

<sup>8</sup> Las TIC en la educación: caso de El Salvador

Extractado

de:  
<http://webquery.ujmd.edu.sv/siab/bvirtual/Fulltext/ADLI0000548/Capitulo%203.pdf>

Con formato: Sin subrayado

con el uso de las tecnologías de la Información y no se enfoca en la Seguridad de la información en sí.<sup>9</sup>

### **1-5 El Vice Ministerio de Ciencia y Tecnología, dependencia del Ministerio de Educación**

En El Salvador se cuenta a partir del año 2009, con el Vice Ministerio de Ciencia y Tecnología, en sustitución del anterior Vice ministerio de Tecnología y Educación, siempre dependiente del Ministerio de Educación y comprendiendo en su estructura organizacional al CONACYT.<sup>10</sup>

Entre las atribuciones, por mandato de ley del Vice Ministerio de Ciencia y Tecnología tenemos las enunciadas en el capítulo III de la Ley de Desarrollo Científico y Tecnológico, las que están enfocadas a la divulgación de diversas tecnologías y no focalizado en Tecnologías de la Información, con énfasis en el sector educacional público<sup>11</sup>.

Es nuestro objetivo hacer conciencia de la situación o estado actual de la seguridad de la información que en El Salvador, por el momento, adolece de falta de una metodología para Implantar seguridad de la Información en términos generales, es decir empresas públicas y/o privadas sin diferenciar el giro del negocio ni la rama de industria a la que se dedican, pero nuestro esfuerzo se focaliza en aquellos aspectos puntuales que competen a las Entidades Financieras, bancos, dado que una incidencia en la Seguridad de la Información en una de estas entidades puede afectar a un gran número de usuarios y que existen entidades financieras cubriendo un amplio sector del mercado bancario de El Salvador, por lo que una falla grave a la seguridad de la información, podrá trascender en una situación de alto impacto negativo, para todos sus usuarios, accionistas, asociados de negocios, público en general e incluso en la imagen de las demás entidades financieras, pudiendo llegar a provocar una completa crisis económica a nivel país.

### **1-5 Seguridad de la Información implantada en Entidades Financieras en El Salvador**

<sup>9</sup> Ley Especial contra Actos de Terrorismo  
Art. 12 Delito Informático y art. 46 Régimen de las Pruebas

<sup>10</sup> Decreto No. 12, “Decreto de Creación del Viceministerio de Ciencia y Tecnología, Consejo de Ministros  
Recuperado de  
<http://www.cienciaytecnologia.edu.sv/index.php/programas.html>  
Redefinición de las funciones del “nuevo” CONACYT, unidad Organizacional del Viceministerio de Tecnología, dependencia del Ministerio de Educación.  
Recuperado de:  
[http://www.conacyt.gob.sv/index.php?option=com\\_k2&view=item&id=64:publicación-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77](http://www.conacyt.gob.sv/index.php?option=com_k2&view=item&id=64:publicación-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77)

<sup>11</sup> Diario Oficial Tomo No. 398 San Salvador, martes 19 de Febrero de 2013. Órgano Legislativo Decreto No. 234 – Ley de Desarrollo Científico y Tecnológico.

Recuperado de: [http://unctad.org/es/docs/dtlstict2011d4\\_sp.pdf](http://unctad.org/es/docs/dtlstict2011d4_sp.pdf)

En El Salvador algunas entidades financieras, especialmente las que forman parte de una transnacional, filial El Salvador, han por indicaciones de su casa matriz, implantado alguna norma o estándar de seguridad de la información.

Por otra parte en todas las entidades financieras encontramos diversas iniciativas organizacionales de cara al establecimiento de un Gobierno Corporativo, Código de Ética, Comité de Auditoría y otras formalidades administrativas, las cuales están consignadas en la “NBP4-48 NORMAS DE GOBIERNO CORPORATIVO PARA LAS ENTIDADES FINANCIERAS”, emitida por la SSF, para apoyar este aspecto presentamos a continuación, un cuadro que contiene la adopción de normas y/o estándares de seguridad de la información y algunas prácticas (las más relevantes) de su implantación, administración y seguimiento, que muestra las principales entidades financieras (Bancos) y algunos aspectos de administración y control (seguimiento) a la norma y/o estándar de seguridad de la información adoptado, Anexo 5.

Como puede inferirse fácilmente, existe conciencia de la importancia en las entidades financieras, filiales de una transnacional, con lo que se ha tomado conciencia del riesgo y adoptado medidas para administrarlo, no así, en las entidades típicas salvadoreñas a quienes al consultarles al respecto manifestaron que dicho aspecto es de carácter confidencial y que por lo tanto no pueden brindar información al respecto (N/D= no disponible), no obstante al ahondar sobre el particular con ejecutivos de algunas de esas entidades, en su gran mayoría mostraron desconocimiento del tema, lo cual permite deducir que dicho aspecto no está siendo debidamente atendido.

### **1-6 Consideraciones de la Gestión de Riesgos para la implantación de la Seguridad de la Información.**

Se necesita una aproximación sistemática de la gestión de los riesgos de la seguridad de la información que permita identificar las necesidades organizacionales congruentes con los requerimientos de la Seguridad de la Información y la creación de un Sistema de Gestión de la Seguridad de la Información (SGSI), efectivo.

Esta aproximación deberá elaborarse para el entorno particular de cada organización y particularmente deberá estar alineada con el enfoque integral de gestión de riesgos de la Organización. Las iniciativas de seguridad de la información deberán direccionar los riesgos en una forma efectiva y oportuna cuando y donde sea necesario.

Al igual que la Seguridad de la Información, la gestión de riesgos es un proceso continuo, debe establecer el contexto de los activos de riesgo y el tratamiento de los riesgos, usando un plan de tratamiento de riesgos para implantar las recomendaciones y decisiones que desarrollen las salvaguardas pertinentes, para mantenerlos a un nivel aceptable.

La gestión de riesgos de la seguridad de la información debe contribuir a:

- a) Identificar los riesgos
- b) Evaluar los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia
- c) La probabilidad y consecuencias de que estos riesgos hayan sido comunicados y entendidos.
- d) Determinar un orden de prioridad para el tratamiento de los riesgos
- e) Priorizar acciones para reducir la posible ocurrencia de los riesgos
- f) Involucrar a todas las partes interesadas en la toma de decisiones del tratamiento de riesgos y mantenerlos informados del estatus de dichos riesgos
- g) Hacer seguimiento a la efectividad del tratamiento de los riesgos
- h) Seguimiento y revisión periódica a los riesgos y a la gestión de los mismos
- i) Capturar información que permita mejorar la gestión de riesgos
- j) Los gerentes y personal ejecutivo deben ser educados sobre los riesgos y las acciones a tomar para mitigarlos

El proceso de gestión de riesgos de la seguridad de la información consiste en:

- a) Establecer el contexto organizacional al que se va aplicar
- b) La evaluación de riesgos
- c) El tratamiento de riesgos.
- d) La aceptación de riesgos
- e) La comunicación de riesgos
- f) Seguimiento y revisión de los riesgos

Para ilustrar el concepto de evaluación de riesgos, existen técnicas específicas las cuales permiten de forma sencilla o más elaborada, hacer una estimación de los riesgos en atención a su probabilidad de ocurrencia, impacto y magnitud.

### 1.7.1 Técnicas específicas para el establecimiento del Riesgo

La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

Sea la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- **MB:** Muy Bajo
- **B:** Bajo
- **M:** Medio
- **A:** Alto
- **MA:** Muy Alto

La estimación del impacto se puede calcular en base a tablas sencillas de doble entrada, aquellos activos que reciban una

calificación de impacto muy alto (**MA**) deberían ser objeto de atención inmediata.

Mientras el impacto mide el valor de la desgracia potencial, el riesgo pondera ese impacto con la frecuencia estimada de ocurrencia de la amenaza. El impacto es la medida del costo si ocurriera mientras que el riesgo mide la exposición en un determinado periodo de tiempo.<sup>12</sup>

### 1-8 Normas y Estándares para implantar Seguridad de la Información en las Entidades Financieras en El Salvador

Las empresas y los gobiernos dependen hoy en día de las tecnologías de información (TI) para su funcionamiento y desarrollo. Hacen enormes esfuerzos e inversiones en TI con el objetivo de ser más eficientes, seguras, cumplir con su misión y con los aspectos claves de su planeación estratégica. Infortunadamente muchas empresas funcionan como silos, aisladas unas de otras, las divisiones no se comunican entre sí y los esfuerzos de un área son a veces desconocidos o entorpecidos por otras. Una de las áreas claramente afectadas por este fenómeno es el área de TI, que muchas veces tiene objetivos claros pero estos no están necesariamente alineados con los objetivos del negocio.

Por otro lado aparecen nuevas tecnologías y procesos de negocio que hacen que las TI deban responder a otras necesidades u operar bajo otros esquemas, como por ejemplo los procesos de tercerización de TI a todos los niveles, la computación en la nube (Cloud Computing), etc. Estas nuevas tendencias marcan nuevos retos para el desarrollo de los procesos y servicios que debe proveer la unidad de TI dentro de una empresa. No importa cuál sea el modelo usado, las TI deben estar presentes para el apoyo de la organización.

#### *Algunas normas y estándares que apoyan el gobierno de TI*

Marcos de referencia con herramientas sólidas son esenciales para asegurar que los recursos de TI estén alineados con los objetivos del negocio y que los servicios y la información satisfagan los requisitos de calidad, financieros y de seguridad.

De acuerdo con los marcos de control disponibles se observa la presencia de estándares que apoyan el gobierno de TI en alguno de ellos, los que permiten materializar el “cómo” para diferentes controles de TI. Se podrían mencionar a ISO 27001, ISO 27002, ISO 20000, BS 25999, ITIL, PCI DSS..<sup>13</sup>

<sup>12</sup> MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información  
Libro III - Guía de Técnicas / ISO/IEC 27005:2008

<sup>13</sup> Chrissis, M. B., Konrad, M., & Shrum S. (2011). CMMI for development@:

Guidelines for process integration and product improvement (3a ed.). Upper Saddle River, NJ: Addison-Wesley Professional.

También tenemos la metodología definida e impulsada por el “ISACA – Information Systems Audit and Control Association”, COBIT, que tiene como Propósito Común proveer para la gestión de procesos de previsión y de negocios de tecnología de información (IT) un Modelo de gobierno, que es útil en la entrega de valor de TI y ayuda en comprensión y gestión de los riesgos asociados con TI.<sup>14</sup>

Además se cuenta con “ITIL – Biblioteca de la Infraestructura de Tecnología de Información” que hace un enfoque de servicios más allá de las necesarias implicaciones de la tecnología de la información y para conseguir este objetivo es imprescindible determinar en primera instancia qué servicios deben ser prestados y por qué han de ser prestados, desde la perspectiva del cliente y el mercado. Los servicios son definidos en ITIL, como un medio de aportar valor al cliente sin que éste deba asumir los riesgos y costos que implican.<sup>15</sup>

## **2 - MARCO TEORICO DE LA ISO 27001, ITIL Y COBIT**

### **2.1 Alcance**

Tomando en cuenta que el objetivo principal del presente trabajo está limitado a orientar a las instituciones financieras del país, en como seleccionar el o la combinación de estándares y/o marcos de trabajo que mejor se adapte a los procesos de negocio para la implantación de un SGSI, por lo tanto en este capítulo se abordara de forma general las características de los 3 marcos de trabajo que hemos seleccionado, y no entraremos a fondo en el proceso de implantación para cada uno de ellos, sino que más bien presentaremos sus características, objetivos de control, procesos, dominios de tal forma que permita obtener una mayor asociación de cada uno de ellos con los procesos de negocio en una institución financiera y determinar si solo es necesario adoptar uno, o si se necesitan los 2 ó los 3 estándares.

### **2.2 Marco y Contexto Normativo – Estándares**

El marco normativo de los diferentes estándares que, de una u otra manera, están vinculados a un Sistema de Gestión de la Seguridad de la Información, en que se ven representados estándares internacionales de diferente naturaleza y con diferente cobertura. Algunos de ellos, como por ejemplo la serie ISO/IEC 27000, específico de la gestión de seguridad de la información, general y aplicable a cualquier sector de actividad, pero también deben tenerse en cuenta otros estándares y recomendaciones que son propios del sector, incluso puede existir la necesidad de alinear más de un estándar, como por ejemplo ITIL con la familia ISO/IEC 27000 y/o COBIT.

### **2.2 Evolución Histórica de los Marcos de Trabajo seleccionados**

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Desde el apareamiento de cada uno de estos marcos de trabajo que hemos seleccionado, encontramos una evolución constante en cada uno que en forma consistente denota una adaptación necesaria a la realidad existente y de esa forma responder a las necesidades del negocio y de la seguridad de la información en los mismos.

Ya sea enunciándolo en forma dedicada mediante uno de sus dominios (ITIL), o como parte de los controles desde la Planificación hasta el Seguimiento, siempre se hace referencia y destaca la importancia de la Mejora Continua. De la anterior se deduce que dicho aspecto no sólo se enuncia en las normas y/o estándares, sino que se trasluce en la constante revisión y actualización por parte de las entidades que los emiten.

#### **2.2.1 Ruta de Implantación de la norma ISO27001:2013**

A continuación presentamos en el Anexo 6, gráfica conceptual de la ruta de implantación de la ISO/IEC 27002

#### **2.2.2 COBIT 5**

Uno de los objetivos de la Asociación de Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Association, ISACA) es promover estándares aplicables internacionalmente para cumplir con su visión. Los recursos de COBIT deben utilizarse como fuente de asesoramiento con respecto a las mejores prácticas. El *Marco Referencial* de COBIT establece que: "es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para atender esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno. "COBIT proporciona un conjunto detallado de controles y de técnicas de control para el entorno de administración/gestión de sistemas de información".

COBIT 5 define una metodología y un marco de trabajo adecuado para la gestión de Tecnología de la Información (TI), orientado en el negocio y en procesos, y basado en controles. Para ello considera tres dimensiones:

- a) Los dominios, procesos y actividades de TI;
- b) Los requerimientos de la información del negocio; y
- c) Los recursos de TI.

<sup>14</sup> <http://www.isaca.org/Knowledge-Center/cobit/Pages/FAQ.aspx#1>

<sup>15</sup>

[http://itilv3.osiatis.es/estrategia\\_servicios\\_TI/introduccion\\_objetivos\\_creacion\\_valor.php](http://itilv3.osiatis.es/estrategia_servicios_TI/introduccion_objetivos_creacion_valor.php)

Define cinco dominios, con sus procesos (37) que a su vez describen actividades concretas, y especifican una serie de prácticas de control (210).

Estos dominios son: Evaluar, Orientar y Supervisar (EDM); Alinear, Planificar y Organizar (APO); Construir, Adquirir e Implantar (BAI); Entregar, Dar Servicio y Soporte (DSS); y Supervisar, Evaluar y Valorar (MEA).

### 2.2.2.1 Procesos COBIT 5

Presentamos en el Anexo 7, una gráfica con el detalle de los Dominios y Controles de COBIT 5, para mayor ilustración.

Tal como se define en el *Marco Referencial* de COBIT, cada uno de los elementos está organizado de acuerdo con el proceso de administración/gestión de TI. COBIT está destinado para ser utilizado por la gerencia de la empresa y por la gerencia de TI, así como por los auditores de TI; por lo tanto, su utilización permite la comprensión de los objetivos del negocio, la comunicación de las mejores prácticas y las recomendaciones que deben hacerse, basándose en una referencia de estándares comúnmente comprendida y bien respetada.

### 2.2.2.2 Ruta Implantación de COBIT

La implantación de COBIT 5 en una institución financiera puede ser fácil y efectiva siempre y cuando se ejecute siguiendo las mejores prácticas y, de forma general algunos de los pasos más importantes se describen a continuación.

- Evaluar las normas de auditoría y prácticas actuales de seguridad de la información
- Es importante aceptar los principios del modelo COBIT 5, pero más importante aún es que la organización los evalúe y acepte para que los pueda impulsar de forma holística.
- Si ya se ha decidido adoptar dichos principios, lo que sigue en importancia es conocer COBIT 5 a fondo, es determinante estar bien familiarizado con todos sus dominios y controles para poder adaptarlos a los procesos y a los requerimientos del negocio.
- Para cumplir con el paso anterior es necesario capacitarse y capacitar a todos los funcionarios relacionados a todos los niveles de tal forma que la implantación sea parte de la estrategia institucional.
- Luego es necesario dar el primer paso, el cual consiste en la evaluación de riesgo de los procesos de negocio involucrados.

El proceso de implantación COBIT deberá ser planeado desde sus inicios cumpliendo con la metodología recomendada, iniciando por el proceso APO (Alinear, Planear y Organizar). Para ejemplificar este concepto se utiliza la siguiente gráfica enfocada de forma específica en este dominio, donde se mapean los procesos de COBIT 5 con los criterios y los recursos que la organización ha definido y con los que ya cuenta, para luego identificar que controles COBIT tienen mayor relevancia para la organización y permitiendo

determinar prioridades y un punto de partida. Este ejercicio se deberá llevar a cabo con todos los dominios y procesos de COBIT para determinar en todos los dominios y procesos cuales son los que más se adaptan a las necesidades del negocio, para ilustrarlo presentamos en el anexo 7 el concepto de Navegación COBIT 5

### 2.2.2.3 Herramientas complementarias.

COBIT se apoya de herramientas externas o internas, de hecho COBIT 5 parte de COBIT 4.1 pero incorpora de forma interna herramientas que antes eran externas, como ValIT, RiskIT, BCS (Balanced Scorecard), RACI, etc., que en la versión 5 ya son parte de los procesos de implantación y se encuentran dentro de los procedimientos como un elemento más de COBIT. A continuación se ejemplifican algunas de esas herramientas con procesos genéricos de una organización genérica, lo que permitirá comprender mejor la utilización de cada herramienta y así valernos de ellas para poder diseñar un método de implantación en una entidad financiera.

RACI (Matriz de la asignación de responsabilidades), es determinante a la hora de identificar los roles dentro de la estrategia y planeación de un SGSI y para ello se basa en una tabla de codificación de roles, esbozada en la matriz de responsabilidades y sus respectivos designaciones en la Organización, ver Anexo 8.

La siguiente figura muestra un ejemplo de lo que sería la utilización de esta herramienta para el proceso EDM01 (Evaluar, Dirigir y Monitorear), en donde para la implantación del SGSI, se designan los roles que cada unidad de la organización deberá asumir según sus competencias y niveles jerárquicos. Ver Anexo 9

### BSC – Balanced ScoreCard.

Las necesidades de las partes interesadas en la implantación de un SGSI, tienen objetivos que pueden estar relacionados con objetivos empresariales genéricos, esos objetivos han sido desarrollados utilizando dimensiones de BSC, por lo general son una lista de objetivos comúnmente utilizados y definidos para sí mismo, Aunque esta lista no es exhaustiva, para la mayoría de metas específicas institucionales se puede hacer un mapa, fácilmente en uno o más de los objetivos genéricos de la empresa.

- La cascada de metas no es "nuevo" a COBIT fue introducido en COBIT 4.0 en 2005 .
- Aquellos usuarios de COBIT que lo han aplicado pensando que sus empresas han encontrado valor.
- Pero no todo el mundo ha reconocido este valor.
- La cascada de objetivos soporta a COBIT 5
- Las partes interesadas en principio es fundamental para COBIT y por lo tanto es un buen punto de partida.
- La cascada de metas ha sido revisado y actualizado para la versión de COBIT 5



Presentamos en el Anexo 10, el mapa de Objetivos del Negocio versus los Objetivos de Gobierno.

### Mapa de Procesos

Además COBIT 5 propone iniciar el análisis del entorno de los objetivos de gobierno relacionándolos con TI, esto por medio de un mapa de los procesos corporativos de COBIT 5 con los objetivos de TI para lo cual se marca con (P) Primario o (S) secundario según aplique. Ver Anexo 11. Lo que implica que se debe hacer un mapa entre los procesos de COBIT 5 con los objetivos relacionados con TI, esto para determinar si el proceso aplica y el nivel de prioridad que tiene para TI.

## 2.3 ITIL V3

La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés “Information Technology Infrastructure Library”), es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

### 2.3.1 Procesos.

De acuerdo al ciclo de vida de los servicios se identifican 4 cuadrantes en los cuales encajan cada uno de los procesos relacionados con el ciclo de vida en que se aplican, complementándose con el quinto proceso aplicable a cada uno de ellos. Ver anexo 12 Cuadrantes de ITIL V.3

Para una mejor comprensión del rol que debería ocupar ITIL dentro de la organización y cuál sería el enfoque que se le debería dar se presenta el siguiente diagrama comparativo con el rol o enfoque de otros marcos de referencia o conjunto de mejores prácticas. Ver Anexo 13, Gobierno de TI.

Bajo la perspectiva de ITIL en su definición de proceso no se aleja mucho de los otros estándares, cuyo concepto sería así:

- Un proceso es un conjunto estructurado de actividades designadas a cumplir un objetivo específico.
- Los procesos toman entradas, procesan y adicionan valor y producen una salida en respuesta a necesidades.

Algunos ejemplos son:

- Gestión de Incidentes
- Gestión de Cambios
- Gestión de Eventos

Para una mayor comprensión el siguiente diagrama ilustra mejor el concepto del modelo de proceso para ITIL, ver figura 16 en el Anexo 14.

Los procesos deben cumplir con características específicas:

- **Medible** = Proporcionar las métricas adecuadas para determinar el grado de madurez.
- **Responder a eventos** = Cambios, Incidentes, Requerimientos, Etc.
- **Resultados Específicos** = Número de Incidentes, Incidentes abiertos, Incidentes cerrados, Incidentes escalados, etc.

### 2.3.4 Ruta de Implantación.

La implantación de ITIL v3 implica una gran cantidad de actividades que de alguna forma pueden ser bastante confusas si no se tiene la experiencia necesaria, así que para comenzar hay que adquirir los conocimientos suficientes u obtener asesoría de expertos externos a la organización, aunque lo recomendable es capacitar a alguien interno, quien conoce el negocio y apoyarlo con un consultor externo quien tiene la experiencia en la implantación.

Como un resumen de la ruta de implantación de ITIL V3, a continuación se describen algunos pasos de alto nivel, que representan la ruta a seguir para una implantación de este estándar en una organización.

#### 1. Preparación del Proyecto.

Como preparación para cualquier proyecto ITIL o ISO 20000, es esencial que los actores clave dentro de la organización de TI conozcan los principios de ITIL, las maneras de aplicarlos, y los beneficios que ofrecen.

#### 2. Definición de la estructura de servicios

Se sabe que la razón principal para implantar ITIL en una organización es hacer que TI, logre un mayor enfoque en los servicios, por lo tanto esta fase es el punto de partida indiscutible. En esta fase se deben identificar los servicios de negocio y de soporte, y a la vez crear la estructura de servicios determinando la interdependencia entre servicios de negocio y de soporte

#### 3. Selección de roles ITIL y los propietarios de los roles.

Consiste en la identificación de los individuos responsables por los nuevos procesos ITIL, determinar los roles y quien asumirá dicho rol dentro de la organización. El manejo de esta cuestión en la etapa inicial es de vital importancia para el éxito del proyecto. La persona que luego será responsable de determinado proceso también debe participar en su

Código de campo cambiado

Código de campo cambiado

Código de campo cambiado

diseño. Esto asegurará que la mayor experiencia posible fluya en la definición del proceso, y que los propietarios de roles se identifiquen muy de cerca con cualquier cambio a las prácticas de trabajo existentes.

La identificación de los roles necesarios para ITIL se deriva directamente de las disciplinas ITIL que se introducirán. Por ejemplo, si Gestión de Problemas está por implantarse, se debe nombrar un Gestor de Problemas.

Dentro de las empresas más grandes y donde se considere necesario, la determinación de los roles no es tan sencilla; puede ser necesaria una subdivisión de tareas, resultando en una subdivisión de roles. Si el Gestor de Problemas, por ejemplo, no puede manejar todas la tareas en Gestión de Problemas, se puede considerar el crear roles tales como "Analista de Problemas", "Gestor de Errores", etc.

#### **4. Análisis de procesos existentes.**

Realizar una evaluación de ITIL y luego una autoevaluación de ITIL en la organización, para determinar que procesos existen y que se puedan encaminar más fácilmente hacia las mejores prácticas además de identificar que procesos necesitan una intervención urgente para alinearlo, recomendamos evaluar los procesos existentes usando una serie de criterios objetivos, para identificar los puntos débiles y oportunidades sin un esfuerzo laborioso de documentación de procesos. La **Autoevaluación ITIL** es ideal para esta tarea.

#### **5. Definición de la estructura de procesos ITIL**

El desglose estructurado de procesos y subprocesos es el resultado de un correcto análisis de la situación actual y la determinación a detalle de cuál será el enfoque del proyecto y que procesos actuales y nuevos se deben incluir.

#### **6. Definición de Interfaces de procesos ITIL.**

A menudo, la importancia de las interfaces de procesos para el diseño de un trabajo óptimo se hace patente durante el análisis de los procesos existentes, los puntos débiles en los procesos aparecen, con frecuencia, en las interfaces, allí donde termina un proceso y empieza otro y en muchos casos, se producen interrupciones en el flujo de información o en los medios, lo que no permite intercambiar la información deseada.

#### **7. Establecer los controles de cada proceso ITIL.**

Una vez definida la estructura y las interfaces de los procesos se deben definir las métricas o controles que

nos ayuden a determinar si los procesos corren según las expectativas.

Una estrategia coherente para el control de los procesos no solamente ayuda a evaluar si se logran los objetivos que se buscan con la implantación de ITIL; también tiene beneficios a largo plazo, ya que presenta los datos necesarios para un proceso de mejoramiento continuo. Es importante en esta fase determinar los propietarios de los procesos y definir las métricas y procedimientos de medición o KPI's

### **8. Diseñando los procesos en detalle.**

Determinar las secuencias de actividades individuales dentro de cada proceso es relativamente laborioso. Por eso es muy importante concentrarse en las áreas que realmente cuentan. Las actividades detalladas dentro de cada proceso se deben discutir con todas las partes relevantes, para poder incluir en su diseño toda la experiencia y los conocimientos posibles. El propietario del proceso es responsable por esta tarea. Como resultado, se llega a un consenso, el cual se documenta en un diagrama de flujo ó flujograma.

#### **8.1. Selección, implantación y mejora de los sistemas de aplicación.**

Determinar si para lograr los objetivos se requieren aplicaciones nuevas o modificar las existentes para cumplir con lo establecido. Los requisitos funcionales de los sistemas de aplicaciones se derivan mayormente de las descripciones detalladas de los procesos, éstos ilustran qué actividades apoyará el sistema de aplicación.

Las definiciones de las salidas de procesos describen qué datos son procesados dentro del sistema. Por ejemplo, el proceso "Registro y Categorización de Incidentes" genera un "Registro de Incidente". El sistema debe poder manejar una estructura de estos datos, y ofrecer interfaces adecuadas para que los usuarios los puedan ver y editar.

### **9. Implantación de procesos ITIL y adiestramiento.**

Ante todo, los participantes se deben familiarizar con los nuevos procesos. La guía de implantación asegura en varios puntos que estos participantes estén involucrados en el diseño del proceso desde fases tempranas, de modo que, en la mayoría de los casos, no sea necesario explicar cómo cambiarán los procesos.

### **3 - MAPEO DE LOS SERVICIOS DE LAS ENTIDADES FINANCIERAS VERSUS LOS DOMINIOS Y CONTROLES EN LAS NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN**

### 3.1 Las Normas y/o Estándares para la implantación de Seguridad de la Información

Como se ha evidenciado en los dos capítulos anteriores, todas las organizaciones y por ende las entidades financieras, cuyo campo de acción comprende un ambiente de riesgo, desde cualquier ámbito del mismo, y que por lo tanto se acentúan la necesidad e importancia de implantar Seguridad de la Información para gestionar adecuadamente los riesgos inherentes al mismo, dado que su actuación es en el mercado del dinero, es decir, sirviendo como intermediario entre los depositantes y demandantes de soporte de crédito a distintos volúmenes para sus operaciones habituales y extraordinarias de inversión o gasto.

#### 3.1.1 COBIT 5 un enfoque Holístico

COBIT es un marco de gobierno de las tecnologías de la información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio, permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías de la información en toda la organización.

Enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías de la información, y permite su alineamiento con los objetivos del negocio.

Además, proporciona las mejores prácticas y herramientas para el monitoreo y mapeo de procesos de TI, mientras que ITIL tiene como objetivo organizar servicios de TI a nivel de gestión e ISO 27002 proporciona directrices para la implantación de un marco de seguridad de información estandarizada.

COBIT 5 proporciona un marco integral que ayuda a las Organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de las Tecnologías de la Información, para cubrir las necesidades de los interesados y alinearse a las actuales tendencias sobre técnicas de gobierno y administración relacionadas con la Tecnología de la Información.

#### 3.1.2 ISO/IEC 27002

Existe una relación de la norma ISO/IEC 27001 con la norma ISO/IEC 27002. La primera define formalmente los requisitos obligatorios para un Sistema de Gestión de Seguridad de la Información (SGSI). En cambio la norma ISO/IEC 27002, se utiliza para indicar los controles más idóneos de seguridad de la información dentro del SGSI, pero como ISO/IEC 27002 es más que un código de prácticas / directrices en lugar de una norma de certificación, las Organizaciones pueden optar en seleccionar e implantar otros controles, o incluso adoptar alternativas completas de controles de seguridad de la Información como mejor corresponda al giro del negocio de su Organización.

#### 3.1.3 ITIL v.3

ITIL se perfila como un conjunto de directrices de “mejores prácticas” que apoyan la Planificación, seguimiento y control

de los servicios de Tecnología de la Información. Define el conjunto de procesos necesarios para la prestación de servicios de TI y proporciona reglas de buenas prácticas. ITIL tiene vocación para establecer un vocabulario común para el conjunto de actores de la industria de TI y proponer una medida estándar de ejecución de los servicios de TI en las Organizaciones. También se presenta como un marco general, para que las organizaciones o sus dependencias puedan contar con una estructura dentro de la cual sea factible diseñar e implantar sus propios procedimientos.

La estructura de ITIL es en la forma de un ciclo de vida, iterativa y multidimensional. Asegura que las organizaciones estén preparadas para ejecutar sus capacidades en algunas áreas y para aprender y mejorar en otras. ITIL provee estructura, estabilidad y fuerza a las capacidades de la administración de los servicios aportando principios duraderos, métodos y herramientas, lo cual sirve para proteger las inversiones y para proveer las bases necesarias para las mediciones o métricas y para el aprendizaje y la mejora continua.

ITIL no es prescriptivo, no hay una rigidez en su aplicación que indique que las pruebas de cumplimiento son apropiadas, es la organización misma la que debe establecer dicha condición.

### 3.2 La importancia de la Seguridad de la Información como carta de presentación de los Servicios de las Entidades Financieras

La Seguridad de la Información en las Entidades Financieras es de vital importancia, dadas las características de dicho negocio de intermediar entre los depositantes y los usuarios de créditos como una forma de apoyar la gestión individual de cada usuario cualquiera que sea su actividad lícita, generadora de ingresos.

Para concretar la seguridad de la información, debemos hacer realidad algunos aspectos básicos propios de la seguridad, tales como; Confidencialidad, Integridad y Disponibilidad.

Por seguridad de la Información podemos entender, la gestión de todos los riesgos relativos a la información. Esto implica identificar tanto a usuarios autorizados y los no autorizados, así como la alteración, destrucción, o divulgación de la información, de tal forma que sólo los usuarios autorizados puedan almacenarla y consultarla en el momento que lo requieran con oportunos y adecuados niveles de seguridad. Esto se logra a través del establecimiento de un Sistema de Seguridad de la Información.

Los conceptos de Integridad, Confidencialidad y Disponibilidad están consignados en el estándar FIPS-199, publicación número 199 del NIST de los Estándares de Procesamiento de Información Federal (Federal Information Processing Standards), la cual se titula “Standards for Security Categorization of Federal Information Systems” y tiene como objetivo dar cumplimiento a lo establecido en la Ley FISMA de 2002, Estados Unidos de Norte América.

Las Categorías de seguridad que establece el estándar están basadas en el impacto potencial que tendría una organización si ocurriera un evento que ponga en peligro la información y los sistemas de información necesarios para cumplir con su misión. Para ello establece tres objetivos de seguridad, conocidos como la tríada de la Seguridad de la Información que son:

**Confidencialidad (Confidentiality).** Preservar restricciones autorizadas en el acceso y revelación de información, incluyendo los medios para la protección de la privacidad de datos personales y la propiedad de información. Define la pérdida de confidencialidad como la revelación no autorizada de Información. En El Salvador este aspecto está consignado, para las Entidades Financieras (Bancos), en el artículo 232 de la Ley de Bancos.

**Integridad (Integrity).** Proteger contra la modificación o destrucción indebida de información, e incluye el aseguramiento de no repudio y autenticidad de información. Una pérdida de integridad es la modificación o destrucción no autorizada de la información.

**Disponibilidad (Availability).** Asegurar el acceso y el uso de información en tiempo y de manera confiable. La pérdida de disponibilidad es la interrupción del acceso o uso de la información o de un sistema de información.

FIPS-199 indica tres niveles de impacto potencial, para los cuales debe existir una brecha de seguridad (pérdida de confidencialidad, integridad o disponibilidad).

Impacto potencial **BAJO** si, se espera que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso **limitado** en las operaciones, activos o en los individuos de la organización.

Impacto potencial **MODERADO** si, se espera que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso **serio** en las operaciones, activos o en los individuos de la organización.

Impacto potencial **ALTO** si, se espera que la pérdida de confidencialidad, integridad o disponibilidad tenga un efecto adverso **severo** o **catastrófico** en las operaciones, activos o en los individuos de la organización.

El formato general que se utiliza para realizar la categorización (SC) de seguridad en un tipo de información o tipo de sistema de información es el siguiente:

SC<sub>Information type or Information system type</sub> = {(confidentiality, impact), (integrity, impact), (availability, impact)}

Con estas consideraciones previas, haremos un análisis de las relaciones entre los servicios que en términos generales prestan las entidades Financieras, Bancos, con los dominios, controles y prácticas de control de la norma y/o estándares COBIT 5, ISO /IEC 27002 e ITIL v.3.

### 3.3 Los servicios de las entidades Financieras versus los controles de las normas y/o estándares de la Seguridad de la Información

Las Entidades Financieras (Bancos), son típicamente organizaciones de Servicios en el mercado del dinero mediante la intermediación entre los depositantes y los usuarios de créditos en todas las modalidades explotadas por ellos, y para lo cual tienen un portafolio de servicios que comprenden la totalidad de los mismos y en cada caso diferentes modalidades, acordes a la segmentación del mercado objetivo según el momento, plaza y tipo de cliente potencial al que pretenden cautivar y mantenerse en su preferencia.

El mapeo realizado de los servicios de las entidades financieras, bancos, versus los dominios, controles, prácticas de control y/o servicios, según el caso, evidencia que para este tipo de organizaciones tienen fuerte aplicabilidad COBIT e ITIL v.3, vale la pena aclarar que no son excluyentes sino más bien complementarios. El caso de la norma ISO/IEC 27001, que se implanta con la ISO/IEC 27002, contra la cual se han mapeado los servicios, encontramos algunos dominios que no tienen aplicabilidad, por ser esta norma de carácter general para todo tipo de organizaciones y que quien la implante deberá adecuarla a las características, giro de negocio o ramo de industria de la organización en si.

En todo caso, el mapeo que hacemos de los servicios que prestan las entidades financieras, bancos, no tiene por objetivo una comparación o relación de correspondencia entre ellos, sino que hacemos una enumeración de sus respectivos dominios, controles y prácticas de control aplicables al servicio en función de establecer y salvaguardar la seguridad de la información.

Para ello, elaboramos un cuadro con el mapa de controles aplicables a los servicios típicos de una entidad financiera y de los cuales por razón de volumen adjuntamos cuatro en los anexos, estos son los Anexos 15 al 30.

#### 3.3.1 Atención en Agencias

Las agencias son la modalidad y punto de servicio típico de las entidades financieras, independientemente del portafolio de servicio que tengan en un momento dado, se proyectan para atender a los clientes actuales y potenciales, dado que una buena parte de los servicios requieren de aspectos formales como los contratos, la captura de las firmas e instrucciones de uso de firmas, designación de beneficiarios, presentación de documentación de respaldo, la negociación de tasas y plazos y muchos otros aspectos que requieren una atención personalizada la cual se brinda en las agencias.

Todos los servicios desarrollados por la institución financiera se brindan también en las agencias en las cuales además de la plataforma secretarial y ejecutiva están dotadas de servicios de ventanilla y muchas veces incluso de dispositivos de canales electrónicos que las complementan para comodidad de los clientes y usuarios en general, el enfoque de la seguridad de la

información, en agencias lo detallamos en el siguiente figura presentada en el anexo 15.

### 3.3.2 Servicios por medio de Cajeros automáticos (ATM's)

Actualmente no se concibe una entidad Financiera (Banco), que no preste servicio por medio de los Cajeros Automáticos, conocidos como ATM's, aunque en la realidad actual de nuestro El Salvador, se encuentra casi en un 100%, este tipo de dispositivos pero con funciones limitadas, conocidos como "Cash Dispenser" o dispensadores de efectivo. La experiencia ha marcado la pauta para ello y en general los clientes de los bancos, utilizan estos dispositivos para obtener efectivo y hacer uso de él, en forma gradual minimizando así la pérdida accidental de la totalidad del mismo ó en cantidades mayores.

Estos dispositivos operan con base en las tarjetas de crédito y/o débito en poder de los clientes de las entidades financieras y prestan servicios en forma constante, independientemente de la fecha y hora, es decir, todos los días, a todas las horas, aunque en algunos casos con límite de usos por unidad de tiempo y límite de efectivo a retirar por transacción y/o unidad de tiempo, ampliando de esa forma los servicios en agencias y muchas veces la cercanía del servicio, dado que están instalados en diversos puntos del país.

No obstante, requieren de consideraciones propias de seguridad de la información por la naturaleza de los mismos, y el servicio que prestan y con mucha más razón cuando atienden tarjetas de débito y/o crédito de uso internacional, tales como seguridad de la red y cifrar la información que transmiten/reciben, y por estar ubicados, la gran mayoría de ellos, fuera de las instalaciones bien resguardadas de los locales físicos de las entidades financieras. Para salvaguardar su seguridad física la Superintendencia del Sistema Financiero emitió una normativa específica conocida como la "NPB4-45 Normas para la seguridad física de los cajeros automáticos" para protección contra el vandalismo, la delincuencia común (nacional e importada), y en forma complementaria para salvaguardar la seguridad física de los usuarios de los mismos, incorporando cámaras de video vigilancia como elemento disuasivo al fraude y/o delincuencia.

Lo anterior denota que los Servicios por ATM's, requieren, desde la perspectiva de la seguridad, un mayor énfasis en seguridad de la información por estar expuestos a riesgos adicionales, propios de los mismos, situación que se materializa por contener en su interior una caja fuerte con dinero para atender los requerimientos y uso de los clientes del banco, además requieren consideraciones de continuidad del servicio.

En el siguiente cuadro se hace una enunciación de los controles de seguridad de la información aplicables a los ATM's, desde los enfoque de COBIT 5, ISO/IEC 27002 e ITIL, presentado en el Anexo 16.

### 3.3.3 Los Kioscos de autoservicio

Estos dispositivos, los kioscos de autoservicio, operados por los clientes con base en la información de sus respectivas

tarjetas de crédito y/o débito, complementan conjuntamente con los Cajeros Automáticos (ATM's), los servicios que en un momento dado los clientes puedan demandar de las entidades financieras en las que tienen sus cuentas, pero por razones de horarios de servicio, las agencias no están disponibles o estando disponibles, les resulta más cómodo y oportuno auto servirse en un kiosco.

En términos generales, en estos dispositivos, se puede realizar una gran cantidad de transacciones que no involucren recibir ni entregar efectivo y facilita, entre otros, hacer los pagos de servicios varios, tales como; energía eléctrica, servicios de teléfono, agua potable, colegiaturas y en muchos casos pagos a proveedores de otros servicios no masivos, solicitudes de chequeras, etc.

Igualmente que los Cajeros Automáticos (ATM's), se les encuentra instalados en las agencias y fuera de ellas, en lugares de fácil accesos al público, brindando con ello la comodidad y oportunidad de hacer una amplia gama de transacciones sin tener que "ir" al banco. Igualmente pueden hacerse transacciones típicas bancarias como abono a obligaciones, y otros servicios bancarios.

Los Kioscos de autoservicio requieren de medidas de seguridad de la información de protección de la red, y por operarse con base en tarjetas de crédito y/o débito, la información transmitida/recibida debe estar en formato cifrado, como en el caso de los Cajeros Automáticos, igualmente requieren consideraciones de continuidad del servicio.

A continuación el mapeo de este servicio contra las normas y/o estándares ya referidos, que presentamos en el anexo 17.

### 3.3.4 Corresponsales Financieros

Esta modalidad de servicio, de reciente puesta en marcha, sirve para mantener los servicios de las entidades financieras cerca del lugar de residencia de los clientes, generalmente se ubican en negocios ya establecidos de particulares, es decir, no son instalaciones físicas de la entidad financiera, aunque ésta provee la infraestructura, hardware y software necesarios para que la aplicación bancaria funcione. Permiten realizar una serie de transacciones monetarias de pagos y/o retiro, estos últimos sujeto a la disponibilidad y riesgo del establecimiento en el que funciona el corresponsal financiero, generalmente son pequeños negocios ubicados en sitios donde la entidad financiera no tiene presencia.

Requieren medidas de seguridad de la información propias de este servicio en adición a la seguridad de la red, cifrado de la información que transmiten/reciben, cifrado de la información almacenada en el disco duro de la pc facilitada por la entidad financiera para la aplicación, y al operador(es) de la aplicación que designa el establecimiento mercantil, la entidad financiera les crea y administra cuentas de usuarios, las cuales cumplen con los requerimientos de seguridad de las mismas en un nivel que proporcione una condición de seguridad apropiada.

Se establecen y funcionan con base en un contrato de servicio específico entre la entidad financiera y el establecimiento comercial en sí, en el que se delimitan, además de los niveles de servicio, las responsabilidades de cada una de las partes y los riesgos correspondientes, asumiendo el negocio el riesgo de la custodia del efectivo producto de sus transacciones habituales y de las realizadas mediante el servicio de corresponsal financiero.

A continuación el mapeo de este servicio versus las normas y/o estándar ya referidos, presentado en la figura del anexo 18.

### 3.3.5 Captación de Fondos

Uno de los pilares fuertes del negocio de las entidades financieras es la captación de fondos del público, mediante el cual adquieren una relación bilateral de clientes, y la entidad financiera en sí, los fondos que le permitirán ofrecer soporte crediticio a los mismos depositantes y también a los no depositantes.

El hecho mismo que captar fondos del público, para lo cual las entidades financieras deben contar con la autorización correspondiente, les permite operar como intermediarios del dinero entre los depositantes y los demandantes del mismo, sujetos a las regulaciones pertinentes, tanto de reserva de fondos que en el caso de El Salvador lo regula y le da seguimiento a diario el Banco Central de Reserva de El Salvador, independientemente que sea una filial de una transnacional en virtud de la figura conocida como “Encaje Bancario” o “Reserva de Liquidez” que permite a los clientes y público en general tener la confianza que en caso necesite hacer uso de sus fondos, no tendrá inconveniente para disponer de ellos, incluso existe otra entidad rectora conocida como “Instituto de Garantía de los Depósitos” la cual fue creada para garantizar un mínimo de recuperación de los fondos depositados en caso que la entidad financiera quebrara.

La operatividad de captación de fondos, en principio se concreta en las agencias de las entidades financieras, sin perjuicio de los servicios que estas puedan brindar a los grandes clientes, conocidos como clientes corporativos, esto último dependerá de la relación de negocios entre ambos.

A continuación presentamos el mapeo de este servicio contra los controles de seguridad de la información consignados por COBIT 5, ISO 27002 e ITIL v.3, en la figura 28 del anexo 19.

### 3.3.6 Colocación de Fondos

La actividad económica de un país está determinada en gran medida por el apoyo crediticio que puedan brindar las entidades financieras establecidas en el mismo e incluso, en algunos casos el apoyo crediticio que puedan brindar entidades financieras internacionales dependiendo de la cuantía de las inversiones a realizar y de la capacidad o liquidez que tengan dichas entidades financieras, ello conlleva igualmente un aspecto de riesgo crediticio.

Por la naturaleza de este tipo de transacciones, desde el crédito de consumo hasta el de inversión familiar e incluso empresarial, y las formalidades contractuales y legales que

implican, típicamente es una operación que se realiza en las agencias físicas de las entidades financieras.

Como es fácil de inferir, este servicio, requiere, al igual que el de captación de fondos un cuidado sustancial en lo referente a la seguridad de la información, en todos los casos, pero con mayor énfasis en las inversiones empresariales que regularmente implican proyectos de inversión que las empresas quieren mantener confidenciales de la competencia como elemento de oportunidad para el éxito de la inversión misma, y además de las consideraciones operacionales que conlleva este tipo de transacción para las entidades financieras, ya que se ven obligadas a implementar ciertas medidas de control que garanticen la recuperación de dichos fondos.

Se presenta un análisis de este servicio contra los dominios y controles de las normas y estándares considerados para este propósito, en la figura del anexo 20.

### 3.3.7 Banca por Internet

Para mantener una presencia significativa en el mercado del dinero, las entidades financieras han desarrollado iniciativas que les permitan ofrecer servicios en la web a sus clientes, tanto en el ámbito de las personas naturales como en el mundo empresarial.

Lo anterior tiene fuertes implicaciones desde la perspectiva de la seguridad de la información, dado que por la naturaleza de este servicio, estando en el ambiente conocido como Internet, el mismo puede ser accedido por los clientes de la entidad financiera o por terceros que sin ser clientes, pretenden acceder al mismo con el objetivo de obtener beneficios no lícitos, es decir, robo de información, interrumpir parcial o totalmente dichos servicios, en diferentes formas, concretando lo que se conocen como ataques cibernéticos que tienen varias formas y que en todo caso atentan contra la entidad financiera y/o sus clientes, exponiendo a la entidad financiera a pérdidas monetarias y lo más grave aún, impacto negativo e incluso pérdida de imagen.

Por lo tanto la entidad financiera debe hacer fuertes inversiones en seguridad de la información y fomentar una conducta de constante monitoreo de la misma, para mantener en un nivel aceptable los riesgos que implican las amenazas, identificar y corregir las vulnerabilidades en cuanto se logren detectar. Implica por lo tanto fuertes inversiones en infraestructura y un fuerte esfuerzo en desarrollar, probar y mantener un efectivo plan de continuidad del negocio, que le permita mantener el servicio disponible y en un nivel aceptable.

Presentamos el análisis de este servicio contra los dominios y/o controles de las normas y estándares seleccionados, en la figura del anexo 21.

### 3.3.8 Banca por Teléfono

Las exigentes demandas de los clientes por tener servicios de las entidades financieras cada vez, más acordes a la tecnología de la información de actualidad y poder hacer sus transacciones en una forma más expedita, llevan a establecer

una serie de servicios que los clientes de las entidades financieras puedan realizar mediante el uso del teléfono para asegurar la fiabilidad de una transacción, como por ejemplo, asegurar los fondos de un cheque que recién reciben o sencillamente pedir a su entidad financiera el bloqueo de Tarjetas de Crédito y/o Débito que se les han perdido, o han sido objeto de robo, dan al cliente la confianza de que su entidad financiera les protegerá adecuada y oportunamente en momentos que así se requiera independientemente de la fecha y hora..

Presentamos a continuación el mapeo de este servicio versus los dominios, controles y prácticas de control de las normas y/o estándar antes referidos, en la figura del anexo 22.

### **3.3.9 Banca Móvil**

El agitado mundial actual y el advenimiento de las tecnologías de la información, aunadas a las exigentes demandas de servicios por parte de los clientes y público en general, aparte del esfuerzo por mantenerse en un sitio preferencial, con lo cual procuran cimentar e incrementar la lealtad de sus clientes y atraer nuevos, en la Banca Móvil, que permite a los usuarios de la misma hacer transacciones monetarias y no monetarias desde un teléfono celular con el propósito de ser oportunos y efectivos en el manejo de sus respectivas transacciones.

Lo anterior implica mayor uso de recursos de tecnología de la información para las entidades financieras y además un incremento en el riesgo y mayor atención en preservar la seguridad de la información para seguridad de los clientes, y de la entidad misma. Se requieren medidas adicionales de seguridad tanto a nivel de control de accesos como de seguridad de la red y de la transmisión/recepción de la información por los riesgos inherentes a los que están expuestos los teléfonos celulares inteligentes que permiten la navegación en este tipo de aplicaciones. De igual forma se requiere dar alguna capacitación a los clientes desde la perspectiva de la seguridad con la que deben manejar sus dispositivos móviles para evitar que sean objetos de contaminación por malware y/o “hackeo” de dichos dispositivos móviles.

Presentamos una mapeo de este servicio “Banca Móvil” contra los dominios, controles y prácticas de control aplicable según lo consignado en las normas y/o estándares ya referidos, en la figura del anexo 23.

### **3.3.10 Centro de Llamadas (Call Center)**

El mercado de los servicios Bancarios y no bancarios ha tenido auge y aceptación gracias a la incorporación de los Centros de Llamados o “Call Center”, que normalmente son provistos por terceros quienes se han especializado en este rubro. Los centros de llamados tienen la característica de prestar sus servicios en idioma español e incluso en otros idiomas, generalmente Inglés y en horario continuos independientemente de la fecha, es decir, su servicio se entiende 24 horas al día si la entidad a quien se lo prestan así lo requiere.

Al ser una tercera parte entre los clientes y la entidad financiera, banco, se hace necesario exista una coordinación clara y completa entre ambas instituciones de forma que los

clientes no perciban dicha tercerización del servicio, Claro que demanda un cuidado especial de parte de la entidad financiera en cuanto a la seguridad de la información, dado que por intervenir con sus clientes una tercera parte, se deben cuidar con mayor celo y hacer seguimiento a los aspectos de Seguridad del personal, control de accesos, seguridad de la red, continuidad del servicio y monitorearlo de forma que se garantice que el cliente recibe un servicio de calidad en todos sus aspectos. Dado que la Ley de Bancos regula en el “secreto Bancario”, que aquellos aspectos que tengan relación con información sensitiva no deben ser atendidos por personas, sino que debe manejarse por medio de un medio idóneo de confidencialidad, este es un aspecto sujeto de examen por parte de las auditorías de las entidades financieras e incluso por el ente rector, entiéndase, SSF.

A continuación presentamos el mapeo de este servicio contra los dominios, controles y prácticas de control de las normas y estándares ya referidos, en la figura del anexo 24.

### **3.3.11 Tarjetas de Crédito**

En El Salvador, a mediados de la década de los 70’s, surge y rápidamente cobra auge el uso del dinero plástico o electrónico, como se le ha dado en llamar, materializado en las Tarjetas de Crédito, cuyas franquicias las comercializan emisores internacionales como VISA International, Master Card, etc. y su uso, inicialmente restringido a cierto mercado objetivo, por capacidad de pago, fue mediante la expedición de tarjetas de uso internacional, cuyo uso por parte de la Entidad Financiera y de los usuarios se regula mediante reglas operativas, de seguridad y transaccionalidad expedidas con el concesionario de la franquicia.

Posteriormente, algunas entidades financieras comenzaron a emitir Tarjetas de Crédito de uso restringido, nacional y en algunos casos a nivel centroamericano, hoy día este medio de pago y/o crédito ha alcanzado una penetración desde los niveles salariales de tipo obrero hasta los niveles de muchísima más capacidad económica.

Típicamente es un negocio de grandes riesgos para la entidad financiera que las emite y para los usuarios, no obstante por las múltiples ventajas que representa y los grandes volúmenes de ingreso que les genera a las entidades financieras que las emiten, éstas han aceptado adecuar sus procedimientos operativos, sus sistemas de información e incorporado las medidas de seguridad que dictan las concesionarias, tales como la norma “PCI-DSS”, en adición a las normas y/o estándares de seguridad de la información referidas en este trabajo, para mantener en un nivel aceptable de riesgo la operatividad de las mismas, las cuales son usadas para adquirir bienes y/o servicios, pagar obligaciones, obtener efectivo contra su límite de crédito autorizado en la misma y hoy día las entidades financieras han extendido su uso para disponer de efectivo de sus cuentas de depósitos mediante los dispositivos conocidos como cajeros automáticos o ATM’s.

Se requiere, para su funcionamiento, Seguridad en la red, cifrado de la información transmitida / recibida, educación al usuario de la misma para salvaguardar su Tarjeta de Crédito de los múltiples riesgos a los que está expuesta.

Presentamos una mapeo de este servicio contra los dominios, controles y prácticas de control de ya referidos, en la figura del anexo 25.

### 3.3.12 Tarjetas de Débito

El servicio de las tarjetas de crédito, evoluciono con el apareamiento de la Tarjeta de débito que, como su nombre indica, se usa para disponer de efectivo que ha sido previamente depositado en una cuenta de depósitos bancario y se utiliza para hacer compras, retiro de efectivo de los cajeros automáticos ATM's y pagos varios. Existe igualmente que la tarjeta de crédito, en las modalidades Internacional y Nacional y como ventaja permite a su poseedor, un uso gradual de su efectivo. Desde la perspectiva del riesgo, para el tenedor o usuario es similar a los riesgos de la tarjeta de crédito con límite del valor de los fondos a retirar por transacción o por fecha, en caso de pérdida o extravío.

Requiere de medidas de seguridad de la información y de cuidados personalmente de su titular muy acuciosos, dado que representa un medio de pago, y que puede ser objeto de fraude, por lo tanto las entidades financieras que las emiten, hacen grandes esfuerzos para salvaguardar la seguridad de la información de las mismas y llevar con ello confianza y tranquilidad a sus usuarios.

Es necesario mantener una red segura e incluso cifrar la información recibida / transmitida, además usar medidas discrecionales de identificación del titular mediante procedimiento de resguardo de la información del mismo, conocidas como "enmascaramiento", para garantizar la confidencialidad.

Presentamos el mapeo de este servicio contra las normas y/o estándares ya referidos, en la figura del anexo 26.

### 3.3.13 Comercio Exterior

Los servicios de Comercio Exterior de las entidades financieras, bancos, son los que permiten materializar la relación interbancaria de los bancos de El Salvador con los bancos del resto del mundo. Ello implica además de facilidades para sus clientes ya sean importadores, exportadores o dedicados a ambas actividades, poder tener la facilidad de realizar sus transacciones de una forma segura, ágil y dentro de un ámbito de seriedad que inyecta a sus operaciones internacionales la imagen de ser serios, profesionales y además lícitos.

Las modalidades más usadas para el comercio exterior son los créditos documentarios ó cartas de crédito documentario que amparan importaciones y/o exportaciones de todo tipo de bienes, además se acostumbran realizar pagos a los compromisos adquiridos, mediante transferencias internacionales lo cual aplica al sector privado y gubernamental en sus relaciones crediticias con las entidades internacionales correspondientes.

Lo expuesto anteriormente permite inferir con facilidad que el aspecto de seguridad de la información en este servicio es vital, dado que se está actuando ante entidades de otras partes del mundo en los que muchas veces las horas de servicio no coinciden con las nuestras e incluso las fechas calendarios

pueden ser diferentes a la nuestra, además del idioma lo que se supera mediante el uso de un idioma común, Inglés, independientemente del idioma oficial del país donde esté radicada la entidad financiera con la que se está operando.

Por supuesto que deben tomarse todas las medidas que garanticen la seguridad de la información de forma interna y además, vigilar porque la transmisión de datos y/o comunicaciones sean seguras, correctas y oportunas, para evitar pérdidas monetarias por errores que el usuario de la entidad financiera no asume, sino que es la entidad financiera en la que recaen dichos gastos, siempre que el error haya sido cometido por la entidad financiera y no se deba a instrucciones imprecisas del cliente.

Este tipo de servicio es de vital importancia a nivel país dado que de su comportamiento se establecen indicadores de índice macroeconómico que a su vez dan la pauta para el estado de la economía del país. Por lo tanto la importancia de asegurar la seguridad de la información es tanta como el valor comercial de las transacciones que se efectúen por medio del comercio exterior. Igualmente se ha realizado el análisis de este servicio contra los dominios, controles y/o prácticas de control enunciados, en cada una de las normas y estándares ya referidos, así, en la figura del anexo 27.

### 3.3.14 Fianzas, Aavales y Garantías Bancarias

Las Entidades financieras, bancos prestan una gama de servicios en adición o complemento a los históricos servicios de captación y colocación de fondos que sirven de soporte a personas naturales y/o jurídicas para poder respaldar una gama de obligaciones civiles y mercantiles cuando las circunstancias así lo requieren, se trata de las Fianzas, Aavales y Garantías, bancarias todas, mediante las cuales, cada una en su caso específico sirven a un propósito puntual. Por ejemplo, alguien obtiene la concesión de un contrato de trabajo con el gobierno, para un proyecto dado, y éste le condiciona la concesión del mismo a que presente una Garantía Bancaria de Fiel cumplimiento por el valor del contrato a conceder, o una Fianza para gestionar licencia de conducir para un menor de edad habilitado.

Las Entidades Financieras, mediante la prestación de este servicio, asumen la responsabilidad del contratante o solicitante lo que implica asumir el riesgo de responder monetariamente por el valor, en nombre del concesionario de la fianza y/o garantía, ante la autoridad a quien se le presente. Dado que este servicio implica asumir responsabilidad ante el cliente y ante tercero, es importante velar por una seguridad de la información que no permite margen para errores. Presentamos a continuación el mapeo de este servicio, Fianzas, Aavales y Garantías Bancarias contra las normas y estándares ya referidos, en la figura del anexo 28.

### 3.3.15 Mercado Bursátil

El mercado del dinero tiene diferentes modalidades y en este servicio nos estamos refiriendo a aquellas transacciones que aún representando fuertes cantidades de dinero, como tal, no se materializan en numerario o efectivo en forma directa sino que mediante documentos conocidos como títulos valores, que pueden representar acciones de una "X" entidad, LETES –



Letras del Tesoro, Bonos o cualquier otro título valor. Ciertamente el volumen de transacciones en sí no es alto, pero si lo es el volumen en términos monetarios y aunque puede concretarse en el país, algunas de las Entidades Financieras de El Salvador ofrecen operar en bolsas de valores internacionales lo que conlleva una responsabilidad aun mayor y con el consiguiente riesgo por la naturaleza de las operaciones. Las entidades Financieras concretizan este servicio por intermedio de ejecutivos especializados conocidos como corredores de bolsa que operan en representación de la entidad financiera ante el cliente.

A pesar que el horario de servicio, en este caso es restringido, las implicaciones de seguridad son fuertes, dados los volúmenes monetarios de las transacciones a nivel individual y global que demandan, a juicio de la entidad financiera, la conveniencia y necesidad de grabar las conversaciones telefónicas, para efecto de respaldo ante una incidencia o mal entendido entre el ejecutivo del banco y el cliente. También algunas entidades financieras han comenzado a usar servicios de correo electrónico seguro (si, comprendido dentro de las normas y/o estándares de seguridad de la información), no así la grabación de las conversaciones telefónicas, pero de lo cual se le advierte al cliente para su conocimiento y satisfacción o que renuncie a realizar dicha transacción.

En este servicio, no hemos hecho consideraciones de continuidad del negocio, dado que la entidad financiera no opera la bolsa o bolsas de valores sino que sirve de intermediario entre el cliente y la bolsa en la que él decide hacer sus transacciones.

Presentamos a continuación el mapeo de este servicio versus las normas y estándares ya referidos para ilustración de la necesidad de implantarle seguridad de la información, en la figura del anexo 29.

### 3.3.16 Medios de Pagos

El servicio de medios de pago, de reciente aparición en El Salvador, conocido como “SICE – Sistema Interbancario de Compensación Electrónica”, surge producto de una iniciativa privada de algunos bancos que estiman conveniente facilitar a sus clientes las operaciones bancarias, haciendo uso del banco de su preferencia para realizar transacciones con otros bancos, mediante los conocidos créditos y débitos electrónicos.

En este tipo de servicio, el cliente de una entidad financiera puede honrar sus obligaciones con un proveedor, usando los servicios de su banco, aunque el proveedor tenga cuenta en otro diferente. Igualmente, las organizaciones podrán, usando los servicios de su banco, pagar los sueldos y demás prestaciones monetarias a sus empleados independientemente de en qué banco diferente tiene el empleado su cuenta.

Téngase presente que por razones de control de las entidades rectoras del sistema financiero este servicio opera, en términos de completar la operación de cargo/abono, bajo el término de tiempo “N+1”, es decir, que si hoy se ordena una de estas transacciones, ésta estará aplicada en el banco destinatario al siguiente día hábil.

No obstante lo anterior, como ya se habrá inferido, representa mucha ventajas en el sentido de evitar ir a más de un banco para concretar una transacción y debemos agregarle que el servicio de medios de pago se concreta desde las oficinas del cliente, es decir, de forma electrónica lo que representa una ventaja adicional en términos de comodidad, oportunidad y poder hacer previamente las verificaciones y controles correspondientes antes de “enviar” la transacción al banco. Lógicamente, en las oficinas del cliente, debe observarse todas las medidas de seguridad de la información recomendadas algunas, y exigidas otras por el banco.

Presentamos a continuación el mapeo realizado de este servicio contra las normas y estándares ya referidos, así, en la figura del anexo 30.

### 3.3.17 Conclusion

En los 16 servicios que en términos generales prestan las entidades financieras, bancos, enunciados en los numerales 3.3.1 al 3.3.16, hemos realizado una descripción genérica de los mismos y presentado en cada caso el mapeo de los dominios, controles y prácticas de control que aplican de los consignados en COBIT 5, ISO/IEC 27002 (que sirve para implantar la seguridad de la Información y que una vez implantada es factible de certificar usando la norma ISO/IEC 27001, que sólo contiene 11 dominios y no 14 como la ISO/IEC 27002), e ITIL v.3

De lo expuesto anteriormente, podemos inferir que siendo las entidades financieras, bancos, instituciones típicamente de servicios, la aplicabilidad de buenas prácticas como ITIL v.3, más la norma COBIT 5, que además de buenas prácticas incorpora los conceptos de Gobierno Corporativo y Administración de TI, Valor de TI y facilita además “drivers” ad-hoc, para que la Auditoría de Sistemas o Tecnología puedan realizar los exámenes correspondientes de seguimiento y evaluación a la Seguridad de la Información, versus que el estándar ISO/IEC 27002, no obstante sus 14 dominios, que por estar diseñados en términos generales para organizaciones que se dediquen a cualquier ramo de industria o giro de negocio, son un tanto generales, en este ejercicio hemos encontrado que para ninguno de los Servicios de las Entidades Financieras se aplican la totalidad de esos catorce dominios.

Por otra parte, la combinación de normas y estándares es una realidad axiomática (no necesita demostración), lo cual está ya evidenciado en la “**Figura 5:** Cuadro con detalle de norma y/o estándar de seguridad adoptado” (**capítulo 1**), en el que se consigna la situación actual de la Seguridad de la Información implantada actualmente en algunas de las entidades financieras, filiales de transnacionales, en la que se puede apreciar que por razones de cumplimiento las entidades financieras que emiten Tarjetas de Crédito y/o Débito de aceptación internacional han implantado la norma “PCI-DSS Payment Card Industry Data Security Standard”, la cual incluso manda en lo referente al cifrado de datos (también consignado en COBIT e ITIL v.3), usar un algoritmo de cifrado, como 3DES, para evitar gestionar reclamos a nivel internacional por transacciones a cargo de sus tarjetahabientes en El Salvador, asumir las pérdidas monetarias resultantes y

además pagar una multa anual al concesionario de la Franquicia de La Tarjeta de Crédito / Débito.

#### **4 - METODOLOGÍA PARA SELECCIONAR LA NORMAS Y/O ESTÁNDAR QUE CONVenga PARA IMPLANTAR SEGURIDAD DE LA INFORMACIÓN EN ENTIDADES FINANCIERAS EN EL SALVADOR.**

##### **4.1 Evaluación de las Normas y/o Estándares de Seguridad de la Información que mejor cubran los procesos del negocio en base al método en cascada.**

Teniendo habida cuenta que, por razones de conveniencia, otros países como Ecuador, Perú, México, España, etc., han adecuado a sus propias necesidades, normas a partir de las versiones emitidas por sus creadores, adaptándolas así a las necesidades, costumbres y/o léxico local para gozar de una mejor y mayor adaptación a sus características, lo cual es factible y las normas y, estándares mismos lo permiten e incluso sugieren, en nuestro trabajo hemos considerado tres marcos de referencia constituidos por COBIT 5, ISO/IEC 27002 e ITIL v.3, para ser considerados en la implantación de la Seguridad de la Información en las entidades Financieras, bancos, en El Salvador, y teniendo presente la naturaleza o giro de negocio de las entidades financieras, quienes prestan servicios de intermediación en el mercado del dinero entre depositantes y usuarios de créditos, además de los dominios, controles y prácticas de control que cubren cada uno de esos marcos, presentamos, un extracto de dichos marcos de referencias, los cuales en forma resumida, son los siguientes; Anexo 32.

Como puede observarse ITIL v.3 considera o enuncia en forma explícita, como parte integral, el aspecto relacionado con la mejora continua del servicio al igual que la ISO/IEC 27002 y COBIT, basándose en el llamado círculo de Deming o círculo de Calidad.

##### **4.2 Obtención de Resultados**

Para tener un punto de apoyo en cuanto a cuál es la norma y/o estándar más idóneo para implantar seguridad de la Información, y después de haber reconocido la necesidad y conveniencia de adoptarla y con base en la investigación de la situación y la existencia de normas prudenciales, dictadas por el ente regulador, aunado a la ausencia de una legislación adecuada en forma integral.

Todos estos, aspectos fueron planteados en el capítulo 1, luego en el capítulo 2 resumimos dichas normas para posteriormente en el capítulo 3, hacer un mapeo de los Dominios y controles en cada caso contra los 16 servicios (generales), identificados que prestan las entidades financieras.

Luego procedemos a realizar un mapeo de los procesos comprendidos en dichos servicios, contra COBIT 5, ISO/IEC 27002 e ITIL v.3, de lo cual presentamos a manera de ejemplo del cómo debe hacerse, tomando como base cuatro servicios esenciales y de mayor uso por parte de los clientes y del público en general, y en cada uno de ellos, cuatro de sus procesos, contra cada una de las normas y estándares ya referidos.

El método sugerido se basa en el método utilizado por el “balanced scorecard” sugerido por COBIT 5 para determinar los objetivos de gobierno prioritarios para una organización, en ese sentido sometemos los diferentes objetivos de los procesos de negocio a un análisis de prioridades mapeándolos con los objetivos y controles de las normas y/o estándares que estamos evaluando, en el cual asignaremos dos valores (P) primario y (S) secundario.

Posteriormente se evalúa el soporte que le brindan al proceso de negocio, tomando en cuenta que en este caso sólo se ha tomado una muestra de dichos procesos para demostrar el método y se han asignado los valores según nuestro criterio y sin reunirnos con las unidades de negocio reales para hacer un análisis más real, así presentamos los siguientes cuadros. Anexos 31, 32, 33, 34 y 35.

##### **4.3 Análisis de Resultados**

En el mapeo de los procesos de servicios ejemplificados en el numeral anterior hemos asignado una “P” a los que tienen característica de Primarios, y una “S” a los que las tienen de Secundarios, con valores numéricos de 2 y 1 ó pesos, respectivamente, para determinar la norma y/o estándar que mejor cubran las necesidades de Seguridad de la Información de las entidades financieras, bancos, y teniendo presente su naturaleza de ser organizaciones con vocación de servicio. Para lo cual realizamos una tabulación obteniendo los siguientes resultados: (Anexo 5, correspondiente al capítulo 1).

No obstante el resultado primario, que puede inferir a una conclusión no válida, debe mantenerse presente que la designación de “P” a determinados controles, se refiere a que dichos controles son los relevantes y de ahí su mayor valor o peso por la incidencia en la seguridad de la información, para ilustrarlo mejor presentamos el siguiente tabulado:

Norma ó Estándar	Controles	Procesos	Puntaje Absoluto	Participación Controles	Participación Relativa
<b>COBIT</b>	37	16	592		
“P”				448	71.80%
“S”				<u>176</u>	<u>28.20%</u>
<b>Total</b>				<b>624</b>	<b>100.00%</b>
<b>ISO/IEC 27002</b>	35	16	560		
“P”				384	<b>75.00%</b>
“S”				<u>128</u>	25.00%
<b>Total</b>				<b>512</b>	<b>100.00%</b>
<b>ITIL</b>	28	16	448		
“P”				496	64.58%
“S”				<u>272</u>	35.42%
<b>Totales</b>				<b>768</b>	<b>100.00%</b>

En atención este tabulado, si bien es cierto, numérico, su enfoque es de carácter cualitativo y por su medio logramos inferir la mayor, aunque no sustancial, representatividad de la ISO/IEC 27002 con una participación de **75%** de controles primarios o relevantes, un segundo lugar para COBIT 5 con **71.80%** y, luego ITIL v.3 con un **64.58%**, de acuerdo a este análisis ISO-27002 es el elegible sin descuidar que desde el punto de vista del servicio, ITIL v.3, sigue siendo válido a efecto de consolidar la naturaleza de servicio de las entidades financieras, bancos.

#### 4.4 Aplicación de catalizadores a los resultados para descartar norma Y/o estándar con menor puntaje.

Los catalizadores son elementos que sirven para acelerar o retardar una reacción química y en este caso servirán para determinar la conveniencia para una entidad financiera de adoptar el mejor marco de referencia o conjunto de mejores prácticas que más le convenga para su proceso de implantación de Seguridad de la Información, que por sí mismo es muy importante para la entidad que lo ejecuta y se debe asegurar el éxito del mismo en tiempo, resultados y dentro del presupuesto, a manera de orientación por lo tanto aunque el resultado del análisis anterior arroje un indicador a favor de implantar la combinación de ISO/IEC 27002, ITIL v3 y COBIT 5, aún hay algunos factores que pueden cambiar dicha decisión.

Estos factores tienen que ver con los siguientes elementos que consideraremos como catalizadores y que le darán algunos elementos de peso o una ponderación adicional a alguno de los 3 marcos de trabajo que estamos evaluando.

##### Catalizadores:

- 1- Tiempo de implantación estimado
- 2- Costos de la implantación
- 3- Recursos internos capacitados con los que se cuenta
- 4- Costos por asesoría externa
- 5- Costos de mantenimiento
- 6- Estado actual de la gestión de seguridad de TI.

#### 4.5 Actividades adicionales recomendadas

En adición a los resultados obtenidos para cimentar la implantación de la Seguridad de la Información nos permitimos sugerir la realización de actividades complementarias que, en el día a día, marcan la diferencia y acentúan la preocupación de una organización por mantener vigente e institucionalizada la Seguridad, esbozadas a continuación:

##### 4.5.1 Análisis de Riesgo de la Seguridad de la Información

Un factor crítico de éxito en la implantación de un Sistema de Gestión de la Seguridad de la Información - SGSI, una vez definido la norma o estándar a adoptar para implantarlo, consiste en estimar el impacto de los riesgos potenciales en caso llegasen a materializarse, es decir, hacer en forma conjunta con los dueños de los procesos dicha ponderación para con esa base poder fijar de mejor forma los objetivos de la implantación de la Seguridad de la Información.

##### 4.5.2 Campaña de divulgación y concientización del personal a nivel organizacional para la implantación de la Seguridad de la Información

Es de sobra conocido que el éxito de la implantación de Seguridad desde los puntos de vista de Responsabilidad y Cumplimiento no pueden ser ciertos con sólo el involucramiento de TI, aun cuando se cuente con el necesario y decidido apoyo de la alta administración de la Organización, es imprescindible la participación activa de todo el personal lo cual requiere que éste tenga conciencia sobre la importancia vital de la Seguridad de la Información y su percepción desde la óptica de los clientes, proveedores, entes rectores y público en general para proyectar una imagen de Seguridad de la Información Institucionalizada.

Por lo antes expuesto es muy importante que se involucre, en el nivel de detalle correspondiente, a todo el personal mediante charlas de concientización, a partir de la contratación e inducción inicial del mismo y reiterativas en forma periódica para mantener un estado de cumplimiento que se perfile como un elemento integral del desempeño de las funciones y responsabilidades de cada individuo en su puesto de trabajo.

Lo anterior puede reforzarse, haciendo mención de su importancia en el código de ética de la institución y enunciando en el mismo, que en caso de producirse incidentes de seguridad estos serán atendidos con prontitud y diligencia hasta determinar sus causas y persona(s) involucrada(S) a quien se le aplicarán las medidas correctivas correspondientes.

##### 4.5.3 Impulso al Proceso de implantación de la Seguridad de la información alineada a los objetivos del negocio y los objetivos de TI

El proceso de implantación de Seguridad de la Información no puede satisfacerse en un corto período de tiempo, dependiendo de la extensión y complejidad de los servicios que presta una entidad específica, y del tamaño o complejidad de la misma,

pero en términos generales requerirá esfuerzo de un grupo de trabajo con la dirección de un especialista y el apoyo de la alta dirección que deberá impulsarla ante todo el personal para lograr su éxito y aprobar las inversiones necesarias en atención a la importancia de las mismas según las circunstancias que se presenten, en todo caso, debe mantenerse, desde la perspectiva de TI, un alineamiento con los objetivos del negocio para apoyar adecuadamente aquellos servicios que la entidad financiera ha definido como prioritarios y, que se identifiquen y traten adecuadamente los riesgos inherentes en cada caso para evitar pérdidas monetarias y de imagen.

#### **4.5.4 Evaluación de la Seguridad de la Información implantada y reporte a la alta dirección**

Seguridad de la Información no es considerada un producto per sé, sino un proceso en marcha y que requiere una periódica revisión del grado de avance en su implantación conocida en este ambiente como “grado de madurez”, lo que denota que tanto se ha cubierto y cuál es el estado actual a un momento dado.

Dicha situación reviste una importancia institucional y por lo tanto debe, periódicamente, hacerse un reporte de su alcance y de los eventos de seguridad identificados en el período a que corresponde el informe, consignando en el mismo las acciones correctivas tomadas para superarlo y las acciones preventivas a futuro.

Una práctica reconocida para ello, es que periódicamente se ejecuten pruebas de penetración e identificación de vulnerabilidades, por terceras partes especializadas en el tema, con el objetivo de proceder de inmediato a la remediación de las mismas, siempre que sea posible y de ser necesario acciones de mayor envergadura desde el punto de vista de Inversión en TI, proceder a considerarlas para su inclusión en el presupuesto con el objetivo de obtener su aprobación que permita atenderlas y erradicarlas.

Vale mencionar que en cada uno de estos ejercicios se podrán identificar vulnerabilidades nuevas e incluso reiterativas por diversas razones siendo una de ella los cambios de versión en los sistemas operativos, motores de bases de datos y/o aplicativos en producción.

#### **4.5.5 Seguimiento a la Seguridad de la información implantada por parte de la Auditoría Externa, Interna y Autoevaluación por parte de TI**

El acompañamiento a la Seguridad de la Información que debe dar la Auditoría, es una actividad considerada constante y con el propósito de cubrir en cada nuevo examen, nuevos aspectos por conjuntamente con el proceso de autoevaluación que realice TI, poder apoyar la consolidación de la misma, manteniendo un esfuerzo sostenido para lograr cada vez un grado de madurez de mayor significado.

Lógicamente, en base a la 1ra. Ley de la Seguridad de la Información “**No hay Sistema Absolutamente Seguro**”, se reconoce que la Seguridad de la Información tiene características de un proceso continuo al que en ningún momento se le puede dar por concluido, de ahí la importancia

de una supervigilancia continuada por parte de las Auditorías; Interna, Externa y la Autoevaluación que debe realizar TI (tal como se consigna en el dominio de COBIT 5 “MEA – Supervisar, Evaluar y Valorar)

#### **4.5.6 Mejora continua de la Seguridad de la Información en la Organización.**

La Mejora de los servicios debe centrarse en el aumento de la eficiencia, maximizando la eficacia y optimizar el costo de los servicios y los procesos de TI subyacentes. El objetivo de hacer esto es asegurar que las oportunidades de mejoras se identifican a través de todo el ciclo de vida de servicio.

La mejora de la gestión del servicio es iniciar y mantener un programa de cambio organizacional. El éxito de la Gestión de la Seguridad de la Información (ITSM), requiere comprender la forma en que se realiza el trabajo y poner en marcha un programa de cambio dentro de la organización de TI. Este tipo de cambio es, por su propia naturaleza, propenso a dificultades. Se trata de personas y su forma de trabajar. A la gente en general no les gustan los cambios; los beneficios se deben explicar a todo el mundo para ganar su apoyo y asegurar que se modifican las prácticas de trabajo tradicionales.

El principio de la propiedad es fundamental para cualquier estrategia de mejora. “Chief Security Officer – CSI” es una buena práctica y una de las claves para la implantación exitosa, es asegurar que un gerente específico, un gerente de CSI, sea responsable de asegurar que se adoptan las mejores prácticas y se sostienen a lo largo de la organización. El gerente CSI se convierte en el propietario de CSI y el principal defensor. El Gerente CSI es responsable del éxito de Mejora Continua de la Seguridad de la Información en la organización. Esta responsabilidad se extiende más allá de la propiedad, para garantizar que las prácticas de CSI están vigentes en la organización, sino también, y asegurarse que hay recursos adecuados (incluyendo personas y la tecnología). También se deben incluir actividades en la CSI, como el seguimiento, análisis, evaluación y tendencias de informes, así como las actividades de mejora de servicios basados en proyectos - actividades que son fundamentales, ya que sin rendición de cuentas claras e inequívocas no habrá ninguna mejora.

La adopción de Acuerdos de Nivel de Servicio (Service Level Agreement – SLA) es un principio clave de la CSI. Mientras que en el pasado muchas organizaciones de TI consultados sobre los SLA, los consideraban como meramente un puñado de acuerdos aislados alrededor de la disponibilidad del sistema o mesa de ayuda, esto ya no se concibe así, los SLA ya no son opcionales. Los negocios de hoy exigen que sean impulsados por un modelo de servicio. Esta orientación de servicio de TI hacia el negocio se convierte en la base para la asociación de confianza que debe forjarse en la organización para lograr los objetivos institucionales. Hoy en día, los SLA fungen como catalizadores esenciales de todos los procesos de negocio críticos, y deben esforzarse por ser incluidos en todos los canales de comunicación y en todo el camino hasta la sala de juntas de decisiones.

## 5 - CONCLUSIONES Y RECOMENDACIONES

Consideramos importante hacer unas reflexiones sobre la adopción e implantación de Seguridad de la Información en una organización y con mayor énfasis en una entidad financiera, banco, lo que significará una mayor aceptación de los clientes y público en general, una sustancial mejora en la administración de los Riesgos e incremento de su imagen institucional ante terceros, estos considerandos no están explícitamente enunciados en las normas y/o estándares pero son producto de la experiencia en el campo y dictadas por el sentido común.

### 5.1 Conclusiones

El éxito en la construcción de un programa duradero de seguridad de la información sólo puede lograrse a través de influir en la cultura organizacional. No es diferente de cuando una empresa contrata a un nuevo director general para darle vuelta a una empresa que no es rentable. Se requiere un fuerte liderazgo y la capacidad de vender la importancia de la seguridad de la información en la organización.

El principal indicador de la preparación para el cambio cultural, probablemente estará en el apoyo que se otorgue al programa de seguridad de la información por parte de otros líderes ejecutivos. Muchos “Chief Information Security Officer – CISO” han rechazado oportunidades potenciales de carrera después de entrevistarse con los ejecutivos y ver signos de falta de flexibilidad corporativa. Algunas organizaciones están adoptando la seguridad de la información sólo a regañadientes como respuesta al aumento de las infracciones y al cumplimiento normativo. El CISO no tendrá la autoridad para efectuar cualquier cambio, si hay la limitación en el reclutamiento de personal, bajos recursos o informes erróneos, falta de flexibilidad corporativa y de los altos directivos, lo que dificultará su gestión.

Una técnica alternativa para cambiar la cultura organizacional es actuar con un enfoque de abajo hacia arriba en la organización. Este método consiste en la construcción de relaciones sólidas con el personal de TI con el fin de generar una oleada de apoyo para el programa de seguridad de la información.

El factor más importante para cualquier CISO que intenta crear un programa de seguridad de la información es la capacidad de cambiar la cultura de la organización. Los principales indicadores de la disposición de una organización para el cambio cultural serán la existencia o falta de apoyo ejecutivo. Un CISO que es un líder fuerte no será capaz de lograr tanto sin este tipo de apoyo. El enfoque de abajo hacia arriba es un método alternativo de generar soporte para un programa de seguridad de la información, pero puede ser más difícil de lograr.

Para la implantación de la Seguridad de la información, una vez dominadas las normas y estándares ya referidos, deben tenerse presentes y hacer uso de los controles relevantes

aplicables a los diferentes servicios que presta la entidad financiera para estar acordes a la realidad de la entidad misma.

### 5.2 Recomendaciones

En las organizaciones seguras, la seguridad de la información es soportada por la alta dirección. El apoyo incluye poner recursos y presupuestos disponibles para la seguridad de la información, así como declaraciones claras de la alta dirección de que la seguridad de la información es una prioridad para la organización. Ya que los altos directivos establecen prioridades y marcan la pauta para una organización, es difícil ser una organización segura sin su apoyo claro y consistente. Como resultado de la reciente oleada de violaciones de seguridad de alto perfil, la mayoría de los altos directivos ahora entienden la importancia de la seguridad de la información y apoyarán los esfuerzos enfocados hacia este tema.

Las organizaciones seguras identifican y documentan con regularidad cómo los datos sensibles del cliente y/o propietarios fluyen hacia, a través de y fuera de la organización. Esto permite a una organización enfocar su tiempo, esfuerzo y dinero en la protección de sus datos confidenciales. Por el contrario, es difícil para una organización proteger aquello de lo que no sabe nada, y las organizaciones luchan para proteger sus datos.

Las organizaciones seguras crean y mantienen un inventario formal, documentado de todos los sistemas que procesan, transmiten o almacenan datos sensibles incluyendo el sistema operativo, si es físico o virtualizado, y qué aplicaciones principales han sido instaladas. Sin dicho inventario, una organización no puede entender completamente qué sistemas debe proteger. Tener un inventario de este tipo permite a una organización determinar rápidamente si una vulnerabilidad de seguridad en particular es relevante para los sistemas de la organización.

Las organizaciones seguras separan los sistemas sensibles de los sistemas no sensibles a través de servidores de salto, reglas configuradas en el firewall, ACL, routers o switch VLANs. Esto minimiza las posibilidades de ataque para los sistemas sensibles de una organización y permite que el acceso a los sistemas sea muy controlado y registrado.

Las organizaciones seguras tienen un fuerte proceso de control de cambios que se hace cumplir rigurosamente. Los cambios, incluyendo los cambios de emergencia, deben ser totalmente documentados y luego formalmente revisados y aprobados. Los cambios no aprobados pueden llevar vulnerabilidades de seguridad de las que nadie se percata, hasta que estas son explotadas o identificadas en el análisis de vulnerabilidades siguiente. Las organizaciones seguras tienen un fuerte proceso de gestión de la configuración.

Las organizaciones seguras almacenan tan poca información sensible como sea posible en sus sistemas. La información

Código de campo cambiado

confidencial que debe mantenerse por razones de negocios o legales se almacena en el menor número de sistemas posible por una política de retención de datos formal y documentada y se elimina de forma segura cuando ya no es necesaria. Toda la información sensible almacenada se revisa y se justifica con regularidad.

Las organizaciones seguras cifran fuertemente los datos sensibles almacenados y transmitidos y tienen sólidos procedimientos y procesos de gestión de claves de cifrado. Correctamente implantados y gestionados, los datos fuertemente cifrados son esencialmente "indescifrables" y no se pueden utilizar por un atacante.

Las organizaciones seguras recogen y revisan sistemáticamente los registros de sus sistemas sensibles. Los scripts o procesos automatizados se utilizan para buscar registros recopilados para eventos predefinidos, como cuando se agregan nuevas cuentas. Cuando se detectan este tipo de eventos, se envía una alerta al empleado (s) apropiado que luego investiga el caso.

Las organizaciones seguras prueban regularmente sus sistemas sensibles en busca de vulnerabilidades a través de análisis de vulnerabilidad o pruebas de penetración. Hecho de manera correcta y con regularidad, por un especialista, tales pruebas proporcionan una confirmación del "mundo real" y que los controles de seguridad de una organización están funcionando. Si una organización no está poniendo a prueba sus defensas, los hackers probablemente hagan la prueba y, ellos no van a reportar los resultados.

El hecho que persigue a todos los profesionales de seguridad de la información es que nunca habrá suficientes recursos para mitigar cualquier riesgo potencial de seguridad. Es trabajo del CISO tomar estas decisiones críticas acerca de dónde asignar los limitados recursos de la organización para mitigar al máximo los riesgos. Esta es la teoría, pero la aplicación práctica puede ser aún más difícil, ya que el equilibrio entre el riesgo de la organización y los recursos disponibles continúa cambiando. Es muy importante crear un cuerpo de gobierno de la seguridad de TI que ayude a priorizar los riesgos y crear apoyo para cuando se requieran más recursos para proteger a la organización.<sup>16</sup>

<sup>16</sup> ITIL Version 3 Service Improvement

## Referencias

### Banco Central de Reserva de El Salvador.

<http://www.bcr.gob.sv/esp/>

### Normas Prudenciales de Bancos:

#### Superintendencia del Sistema Financiero,

<http://www.ssf.gob.sv/>

<http://www.ssf.gob.sv/index.php/normativa/normas/513-normas-prudenc-bancos>

### Decreto No. 12, "Decreto de Creación del Viceministerio de Ciencia y Tecnología, Consejo de Ministros

<http://www.cienciaytecnologia.edu.sv/index.php/programas.html>

Redefinición de las funciones del "nuevo" CONACYT, unidad Organizacional del Viceministerio de Tecnología, dependencia del Ministerio de Educación.

[http://www.conacyt.gob.sv/index.php?option=com\\_k2&view=item&id=64:publicación-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77](http://www.conacyt.gob.sv/index.php?option=com_k2&view=item&id=64:publicación-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77)

Publicación en El Diario Oficial de El Salvador

<http://www.imprentanacional.gob.sv/index.php/novedades/avisos/25-avisos-ciudadano>

### Ley de Simplificación Aduanera

Art. 1-A Transición electrónica art. 6 Teledespacho art. 7 Uso de medios informáticos y de la vía electrónica art. 8 Entidades certificadoras Pareja de llaves, una pública y otra privada "Criptografía" art.8-a Funciones de las entidades Certificadoras art.8-b Bases de Datos de acceso privado art.8-c Deberes de las Entidades Certificadoras, literales a y b, literal d-Expedir Certificados literales e y k art.8-d Deberes de los suscriptores art. 9 Datos y registro constituyen plena prueba (haciendo uso de la llave) DADO EN EL SALON AZUL DEL PALACIO LEGISLATIVO; San Salvador a los trece días del mes de enero de mil novecientos noventa y nueve

### Código Procesal Civil y Mercantil,

ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR  
18 de Septiembre de 2008

### Ley Especial contra Actos de Terrorismo

Art. 12 Delito Informático y art. 46 Régimen de las Pruebas

### Ley de Fomento y Protección a la Propiedad Intelectual

### Código de Comercio

Art. 451 Conservación de registros (5 años después de la liquidación de todos sus negocios mercantiles art. 455 Medios de conservación de los registros (microfilm – Discos ópticos)

### Código Tributario

Sección cuarta Prueba Contable La contabilidad art.209 (no limita tiempo)

Código de campo cambiado

Secretaría para Asuntos Legislativos y Jurídicos de la Presidencia (2012).  
“DOCUMENTO EXPLICATIVO DEL ANTEPROYECTO DE LEY DE FIRMA ELECTRÓNICA EL SALVADOR”

Legislación del comercio electrónico, “ARTICULO PUBLICADO POR LA UFG DE EL SALVADOR SOBRE LEGISLACION DEL COMERCIO ELECTRONICO EN AMERICA LATINA”

Diario Oficial Tomo No. 398 San Salvador, martes 19 de Febrero de 2013. Órgano Legislativo Decreto No. 234 – Ley de Desarrollo Científico y Tecnológico.  
[http://unctad.org/es/docs/dtlstict2011d4\\_sp.pdf](http://unctad.org/es/docs/dtlstict2011d4_sp.pdf)

Decreto No. 12, “Decreto de Creación del Viceministerio de Ciencia y Tecnología, Consejo de Ministros ,  
<http://www.cienciaytecnologia.edu.sv/index.php/programas.html>

Redefinición de las funciones del “nuevo” CONACYT, unidad organizacional del Viceministerio de Tecnología, dependencia del Ministerio de Educación.  
[http://www.conacyt.gob.sv/index.php?option=com\\_k2&view=item&id=64:publicación-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77](http://www.conacyt.gob.sv/index.php?option=com_k2&view=item&id=64:publicación-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77)  
[http://www.conacyt.gob.sv/index.php?option=com\\_k2&view=22upe&id=64:publicación-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77](http://www.conacyt.gob.sv/index.php?option=com_k2&view=22upe&id=64:publicación-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77)

Anexos:

Universidad Centroamericana “José Simeón Cañas”, Gobierno electrónico y Acceso a la Información Tesis preparada para la Facultad de Postgrados para optar al grado de Maestro en Comunicación. Oscar Alberto Girón Umaña. Junio 2013.

Las TIC en la educación: caso de El Salvador  
<http://webquery.ujmd.edu.sv/siab/bvirtual/Fulltext/ADLI0000548/Capitulo%203.pdf>

National Institute of Standards and Technology  
<http://csrc.nist.gov/publications/history/dod85.pdf>

Information Systems Audit and Control Association  
<http://www.isaca.org/Knowledge-Center/cobit/Pages/FAQ.aspx#1>

Information Technology Infrastructure Library  
[http://itilv3.osiatis.es/estrategia\\_servicios\\_TI/introduccion\\_objetivos\\_creacion\\_valor.php](http://itilv3.osiatis.es/estrategia_servicios_TI/introduccion_objetivos_creacion_valor.php)

Basel Committee on banking 22supervisión. (2006). *Enhancing corporate governance in banking organizations*. Basilea: Bank for International Settlements.  
Bosch, A. (2008). *COSO – ISO 38500* [video]. Conferencia presentada en el tercer curso de verano itSMF – Universidad: El gobierno de TI. Recuperado de: [http://www.youtube.com/watch?v=37z\\_vCvb31cw&feature=relmfu](http://www.youtube.com/watch?v=37z_vCvb31cw&feature=relmfu)

Chrissis, M. B., Konrad, M., & Shrum S. (2011). *CMMI for development@: Guidelines for process integration and product improvement* (3ª ed.). Upper Saddle River, NJ: Addison-Wesley Professional.

Committee on Sponsoring Organizations of the Treadway Commission [COSO]. (1992). *Internal Control – Integrated Framework*. Durham, NC: American Institute of CPAs.

OCDE. (2004). *OCDE Principios de Gobierno Corporativo*. Madrid: Sarbanes-Oxley. (Julio de 2002). Sarbanes- Oxley Act of 2002 Pub. L. No. 107- 204, 116 Stat. 745. Washington D.C: The U.S Government Printing Office.

U.S. Inter-Affairs International Division  
<http://interamerican-usa.com/articulos/Leyes/Ley-Sar-Oxley.htm>

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información  
Libro III – Guía de Técnicas / ISO/IEC 27005:2008

Código de campo cambiado

---

