UNIVERSIDAD DON BOSCO

VICERRECTORIA DE ESTUDIOS Y POSTGRADO

TRABAJO DE GRADUACION
METODOLOGÍA PARA IMPLANTAR SEGURIDAD DE LA INFORMACIÓN EN UNA EMPRESA FINANCIERA EN EL SALVADOR

PARA OPTAR AL GRADO DE:
MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:
ING. MANUEL DE JESÚS VELASCO - MAE, CISA

PRESENTADO POR:
CARLOS ALFREDO NAJARRO ALFARO
ERMIDES URRUTIA LÓPEZ
LINDA JEANNETTE IBARRA DE MARTÍNEZ

ABRIL DE 2015
Antiguo Cuscatlán, La Libertad, EL SALVADOR, CENTROAMERICA.

Agradecimientos

A Dios todopoderoso por permitirme este nuevo triunfo.

A mi familia por el apoyo incondicional brindado.

A mis maestros por compartir conocimientos en forma espontánea y profesional

A nuestro asesor por la forma tan profesional de plantear sus acertadas observaciones.

CARLOS ALFREDO NAJARRO ALFARO

Agradecimientos

Quiero agradecer a dios por haberme permitido continuar mis estudios y darme los recursos y fuerza para culminar este nuevo proyecto de mi vida.

A mi esposa e hijos, por tolerarme y tenerme la paciencia necesaria por no contar con el tiempo necesario para compartir con ellos.

A todos los maestros y compañeros de la maestría de quienes aprendí mucho

A mis compañeros de tesis, Carlos Najarro y Linda de Martinez por su esfuerzo en realizar este trabajo.

A nuestro asesor Ing. Manuel Velasco, por compartir sus conocimientos y experiencias con el grupo

Ermides Urrutia López

Agradecimientos

Quiero agradecer primeramente a Dios, por darme la oportunidad de seguir estudiando, por ser fiel y protector en todo este tiempo.

A mi esposo por ese optimismo que siempre me impulso a seguir adelante y por los días y horas que hizo el papel de madre y padre.

A mis padres y hermana, por su gran ejemplo de superación y valioso apoyo en todo momento desde el inicio de mis estudios de maestría.

A mis compañeros de tesis Don Carlos y Ermides, por compartir conmigo sus experiencias y conocimientos.

A nuestro asesor Ing. Manuel Velasco por sus ideas y recomendaciones, en fin a todas aquellas personas que nos apoyaron para hacer posible la conclusión de esta tesis.

Linda Ibarra de Martínez.

INDICE

INTRODUCCION

En la actualidad la realidad impone a empresas públicas y privadas optar e impulsar iniciativas que implanten o refuercen la Seguridad de la Información y la Seguridad Informática, que en adelante referiremos como “Seguridad de la Información”, como una forma de forjar una posición de mayor y mejor calidad empresarial ante propios, clientes, público en general y entidades rectoras, en los casos que estas existen.

En El Salvador las instituciones Financieras no cuentan con una orientación, por parte de los entes rectores para la implantación de Seguridad de la Información. No obstante, una Organización puede optar por implantar Seguridad de la Información y además complementarla con otro marco de referencia adicional que signifique una ventaja para hacer la Organización más segura, confiable y atractiva a su mercado natural de negocios y de la sociedad en general.

En el presente documento, se analizaran las metodologías más conocidas de Seguridad de la Información que incorporen los conceptos de gobierno corporativo y gobierno de la Tecnología de la Información, aunados a los de Seguridad de la Información tales como COBIT, ISO 27001, eITIL.

Dicho análisis comparativo, estará enfocado a las necesidades de Seguridad de la Información que sean relevantes en instituciones Financieras en El Salvador, independientemente de su tamaño, pero teniendo en consideración que existe dependencia de Instituciones transnacionales a las que sus respectivas casas matrices, en algunos de los casos, y que desde el extranjero les imponen implantar una determina metodología o marco de referencia.

Con ello pretendemos llevar claridad a las altas autoridades de las instituciones financieras en El Salvador con relación al marco de referencia que mejor se puede implantar en sus respectivas organizaciones, dado que no todas las organizaciones,

aun siendo financieras, explotan todos los servicios existentes actualmente, a los clientes, al menos en la realidad actual.

Dichas iniciativas, además de las implicaciones que representan en cuanto a la destinación de diferentes recursos para lograrlo, tales como, pero no limitadas a; personal capacitado en diferentes niveles de la Organización, tiempo, dinero, espacio físico y mobiliario, involucramiento como patrocinadores y responsables de ejecutivos de la alta dirección, divulgación y concientización al personal, y posterior seguimiento, para en los casos que aplique, lograr la certificación respectiva y luego mantenerla ante los entes certificadores, las Organizaciones se encuentran ante un número significativo de “Marcos de Referencia”, “Buenas Prácticas”, “Estándares Internacionales”, etc. que representan en sí mismos una dificultad adicional para seleccionar la correspondiente a menos que exista razón suficiente para optar por una específica.

CAPÍTULO 1: EL ESTADO ACTUAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL SALVADOR Y LAS REGULACIONES LEGALES Y/O INTERVENCIÓN DE ENTES RECTORES RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN

1.1 Las Entidades Financieras en El Salvador registradas por la Superintendencia del Sistema Financiero

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.

La Asamblea Legislativa aprobó, mediante Decreto Legislativo No.592 de fecha 14 de enero 2011, la nueva Ley de Supervisión y Regulación del Sistema Financiero, marco legal que regirá a la Superintendencia del Sistema Financiero como ente supervisor único, que integra las atribuciones de las Superintendencias del Sistema Financiero, Pensiones y Valores.

En este trabajo vamos a centrarnos en las entidades Financieras, específicamente los 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 con las que hacen uso de estos servicios, aún, cuando por la naturaleza de la transacción en sí, no se tipifican como clientes de los bancos, 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 nacional, como se evidencia el siguiente cuadro.

Ingresos Mensuales - Remesas Familiares			
	FLUJOS (Millones de Dólares)		Crecimiento Anual (%)
	2013	2014	2014
Ene	$280.30	$288.10	2.80
Feb	$300.40	$317.80	5.80
Mar	$336.60	$383.20	13.90
Abr	$354.50	$361.90	2.10
May	$357.30	$393.30	10.10
Jun	$320.60	$360.80	12.50
Jul	$331.30	$359.60	8.50
Ago	$322.70	$350.50	8.60
Total:	**$2,603.80**	**$2,815.20**	**8.10**

Figura 1 Estadísticas Banco Central de Reserva de El salvador[1]

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", dado que son entidades existentes o en formación, pero con pleno contacto y 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 los diferentes servicios que prestan, aun cuando no todas prestan la totalidad de dichos servicios.

[1] http://www.bcr.gob.sv/esp/

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 dado que 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, a manera de ejemplo. 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 aparecimiento de los Corresponsales Financieros, que se completan 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 grandes, extensos y complejos recursos tecnológicos para poder brindar el servicio las veinticuatro horas del día, siete días a la semana en forma material o virtual por medio de los llamados canales electrónicos, para lo que se necesita una infraestructura tecnológica que permita almacenar, transmitir / 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, aun cuando se tienen 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. Presentamos a continuación una gráfica que esboza dicha infraestructura.

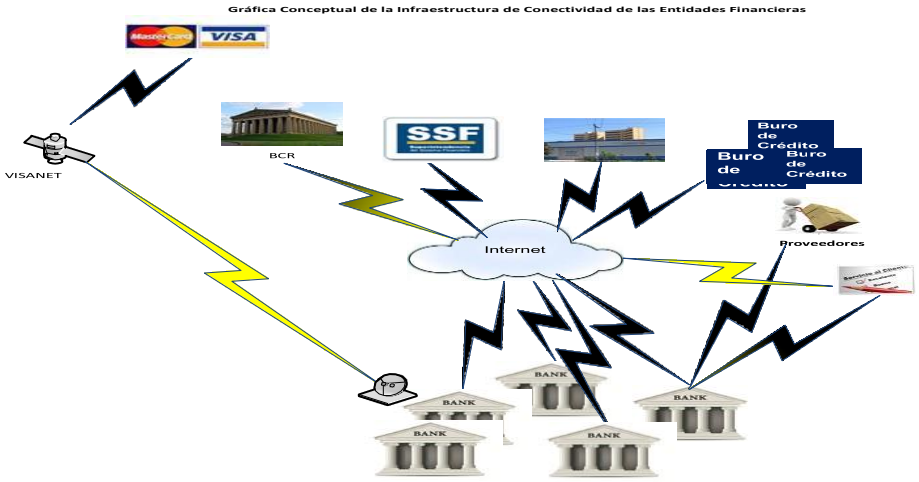


Figura 2 Gráfica Conceptual de la Infraestructura de Conectividad de las Entidades Financieras

Igualmente se puede inferir que ello implica manejar bases de datos que contengan enormes cantidades de datos sensitivos 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, de aceptación internacional, tal como la seguridad del PIN, el enmascaramiento de los números de las tarjetas y el transporte seguro de los datos, que algunas entidades ofrecen como un producto y en otros casos se limita a un servicio.

Por lo antes expuesto la normativa PCI-DSS, no es apta para ser tenida como una metodología de seguridad aplicable a la Seguridad de la Información en forma integral y para 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 nosotros hemos incorporado los servicios que prestan las diferentes entidades.

No.	Insitución / Servicios que presta Intistituciones Autorizadas SSF captar Fondos	Agencias	Atm	Corresp. Financ.	Capat Fondos	Colocac Fondos	Bca x Internet	Bca x Telef	Bca Mov Mall Cente	Tarj Credit Comercio Exterior	Finanzas Asoc.
	Bancos Privados	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
1	Banco Agrícola , S. A.	Sí	Sí	Sí		Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
2	Banco de América Central	Sí	Sí	Sí		Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
3	Banco Davivienda	Sí	Sí	Sí		Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
4	Banco Scotiabank	Sí	Sí	Sí		Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
5	Banco Citibank El Salvador	Sí	Sí	Sí		Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	
6	Banco Promerica	Sí	Sí	NO		Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	
7	Banco Procredit	Sí	Sí	Sí		Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	
8	Banco Azteca	Sí	Sí	NO		Sí	Sí	Sí	NO	NO	NO	NO	NO	Sí	Sí
9	Banco Industrial de El Salvador														
	Bancos Cooperativos														
10	Multi Inversiones Banco Coop, de Trabajadores Soc. Coop. De R.L. de C. V.	Sí	NO	NO		Sí	Sí	NO	NO	NO	NO	Sí	NO	NO	NO
11	Banco de Los Trabajadores Salvadoreños S. C. de R. L. de C. V. (BTS)	Sí	NO	NO		Sí	Sí	NO	NO	NO	NO	NO	NO	NO	NO
12	Banco izalqueño de los Trabajadores S. C. de R. L de C.V.	Sí	Sí	NO		Sí	Sí	NO	NO	NO	NO	Sí	NO	NO	NO
13	Primer Banco de los Trabajadores S. C. de R. L. de C.V.	Sí	NO	NO		Sí	Sí	NO	NO	NO	NO	NO	NO	NO	NO
14	Asoc. Coop. De Ahorro y crédito Vicentina de R. L. ACCOVI de R.L.	Sí	NO	NO		Sí	Sí	NO	NO	NO	NO	NO	Sí	NO	Sí
	Sociedades de Ahorro y Crédito														
15	Sociedad de Ahorro y crédito Credicomer S. A.	Sí	NO	NO		Sí	Sí	NO	NO	NO	NO	NO	NO	NO	NO
16	Sociedad de Ahorro y crédito Apoyo Integral S. A.	Sí	NO	NO											
17	Sociedad de Ahooro y Crédito constelación S. A.	Sí	NO	NO											
	Casas corredorras de Bolsa Solo Intermedian Valores														
18	Sysvalores S. A. de C. V.														Sí
19	Prival Securities El salvador														Sí
20	Lafise Valores El Salvador														Sí
21	Roble Aciones y Valores														Sí
22	G & T continental S. A. de C. V.														Sí
23	Asesores de Inversiones S. A. de C. V.														Sí
	Casas corredorras de Bolsa Intermedian Valoresy Adnimistran Cartera														
24	Inversiones Bursátiles Credomatic S. A. de C. V.						Sí								Sí
25	Servicios Generales Bursátiles S. A. de C.V.						Sí								Sí
26	Acciones Y Valores S. A. de C.V,/**1**														Sí
27	Valores Davivienda S. a. de C.V. /**1**														Sí
28	Valores Banagrícola S. A. de C. V./**1**														Sí
29	Valores Custacatlán El Salvador/**1**														Sí
	NOTA 1 = Actualmente no Administran Cartera														
	No Referidos por la SSF														
30	Banco Azul														
31	Banco Hipotecario														
32	Banco Fomento Agropecuario														
33	Banco de Desarrollo de El Salvador (BANDESAL)														
34	Banco Central de Reserva de El Salvador														
	Aseguradoras Certificadas														
35	Aseguradora Mundial, S. A. Seguros de Personas														
36	Progeso Azul, Compañía de Seguros S. A.														
37	Progeso S. A. Seguros de Personas														
38	Seguros La Hipotecaria, VIDA, S. A. Seguros de Personas														
39	Seguros La Hipotecaria														

Figura 3 Detalle de las Entidades Financieras de El Salvador. Fuente www.ssf.gob.sv[2]

En el cuadro previo se destaca que en adición a los típicos servicios bancarios de captación y colocación de fondos, los bancos hoy día presentan una gama de

[2] http://www.bcr.gob.sv/esp/

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, Aplicación para ser usadas desde 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 al eficiente trabajo de supervisión y regulación que anteriormente realizaban las Superintendencias del Sistema Financiero, Pensiones y Valores.

Es en virtud de esa competencia, que 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, transcritos a continuación:

"**NBP4-50**
CAPÍTULO II
FACTORES Y EVENTOS DE RIESGO OPERACIONAL
Factores de riesgo
Art. 3.- Las entidades deben gestionar los diferentes factores generadores de riesgo operacional, siendo éstos los siguientes:

a) Procesos: Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las entidades deben contar con procesos documentados, definidos y actualizados permanentemente, que pueden ser agrupados en procesos estratégicos y operativos.
Las entidades deben gestionar apropiadamente los riesgos asociados a dichos procesos, con énfasis en las fallas o debilidades que presenten, dado que éstas pueden tener como consecuencia el desarrollo deficiente de las operaciones.

b) Personas: Las entidades deben establecer políticas, procesos y procedimientos que procuren una adecuada planificación y administración del capital humano, que incluyan el proceso de contratación, permanencia y desvinculación del personal.

Asimismo, deben establecer mecanismos preventivos que permitan identificar y gestionar fallas, insuficiencias, negligencia, sabotaje, robo, inadecuada capacitación, apropiación indebida de información, entre otros, asociadas al personal, vinculado directa o indirectamente a la entidad; de tal modo que se minimice la posibilidad de pérdidas económicas.

La vinculación directa es aquélla que está basada en un contrato interno de trabajo, de acuerdo a la legislación laboral respectiva. La vinculación indirecta está referida a aquellas personas que tienen una relación jurídica con la entidad para la prestación de determinados servicios, diferente de aquélla que se origina de un contrato interno de trabajo.

c) Tecnología de información: Las entidades deben gestionar los riesgos asociados a la tecnología de información, entre otros, los relacionados a fallas en la seguridad y

continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, así como la calidad de la información y una adecuada inversión en tecnología.

CAPÍTULO IV

DISPOSICIONES GENERALES

Plan de continuidad del negocio y de seguridad de la información

Art. 16.- Las entidades deben implementar un sistema de gestión de continuidad del negocio en caso de interrupciones que incluya planes de contingencia, análisis de impacto en el negocio, plan de recuperación de desastres y planes de gestión del incidente, que aseguren la operatividad normal del negocio ante la ocurrencia de eventos adversos.

Los planes de continuidad del negocio deben considerar como mínimo lo siguiente:

a) La identificación de eventos que ponen en riesgo la continuidad del negocio, las actividades a realizar para superarlos, las alternativas de operación y el retorno a las actividades normales;

b) La definición de los roles y responsables de implementarlos;

c) La realización de las pruebas necesarias para confirmar su eficacia y eficiencia, al menos una vez al año; y

d) La divulgación del plan a todos los miembros de la entidad.

Asimismo, las entidades deben contar con un sistema de gestión de seguridad de la información que les garantice su disponibilidad, integridad y confidencialidad."

Para ilustración del universo de las NPB, adjuntamos el siguiente cuadro:

Normas Prudenciales de Bancos

1	**Normas Técnicas para Realizar Operaciones y Prestar Servicios por medio de Corresponsales Financieros (NASF-01)**
2	Normas Técnicas para la Gestión del Riesgo de Liquidez (NRP-05)
3	Reglamento para constituir y operar nuevos bancos financieras en El Salvador (NPB1-04)
4	Instructivo para conversión de financieras en banco (NPB1-05)
5	Normas para autorizar a los bancos y controladoras de finalidad exclusiva a realizar inversiones accionarias en sociedades salvadoreñas (NPB1-10)
6	Normas para autorizar a los bancos y controladoras de finalidad exclusiva a realizar inversiones accionarias en subsidiarias y oficinas en países extranjeros (NPB1-11)
7	Normas para autorizar el establecimiento de oficinas de información de bancos extranjeros (NPB1-12)
8	Normas para el establecimiento de sucursales de bancos extranjeros (NPB1-13)
9	Normas para la apertura, funcionamiento y cierre de agencias (NPB1-14)
10	Reglamento de la unidad de auditoría interna de bancos, financieras y sociedades de seguros (NPB2-04)
11	Normas para las auditorías externas de bancos y sociedades de seguros (NPB2-05)
12	Normas para la inscripción de los auditores externos en el registro de la Superintendencia del Sistema Financiero (NPB2-07)
13	Normas de aplicación del requerimiento de fondo patrimonial a las entidades que regula la Ley de Bancos y Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito (NPB3-04)
14	Normas de aplicación del requerimiento de fondo patrimonial a los conglomerados financieros (NPB3-05)

15	Normas para el cálculo y utilización de la reserva de liquidez sobre los depósitos y otras obligaciones (NPB3-06)
16	Normas sobre la relación entre las operaciones activas y pasivas en moneda extranjera de los bancos (NPB3-07)
17	Normas para determinar las relaciones de plazo entre las operaciones activas y pasivas de los bancos (NPB3-08)
18	Normas sobre el otorgamiento de créditos a personas relacionadas con los bancos (NPB3-09)
19	Normas técnicas para las inversiones de las reservas de liquidez en el extranjero (NPB3-10)
20	Normas para el requerimiento de activos líquidos de los bancos (NPB3-11)
21	Normas para el procedimiento de recolección de información para el registro público de accionistas (NPB4-12)
22	Normas sobre enajenación y adquisición de bienes por bancos (NPB4-13)
23	Normas para la remisión de información contable financiera de bancos (NPB4-16)
24	Normas sobre el procedimiento para la recolección de datos del Sistema Central de Riesgos (NPB4-17) **Anexos (NPB4-17)**
25	Normas para la contratación de las tasas de interés, comisiones y recargos entre los bancos y sus clientes (NPB4-20)
26	Normas para la transparencia de información en las operaciones y servicios bancarios (NPB-4-21)
27	Normas para informar los depósitos garantizados (NPB4-22)
28	Normas sobre la transferencia de acciones de bancos, controladoras de finalidad exclusiva y sociedades de ahorro y crédito (NPB4-23)
29	Normas sobre emisión, depósito, colocación y suscripción de acciones de tesorería (NPB4-24)
30	Normas para la publicación de la calificación de riesgo de los bancos (NPB4-25)
31	Normas para la aplicación de la Ley de Integración Monetaria (NPB4-27)
32	Normas que se aplicarán a los procesos de liquidación voluntaria de una entidad bancaria (NPB4-28)
33	Normas para autorizar operaciones con entidades vinculadas (NPB4-29)
34	Normas para la tenencia de activos extraordinarios en los bancos (NPB4-30)
35	Normas para contratos de arrendamientos de bienes inmuebles entre bancos y partes relacionadas (NPB4-31)
36	Normas sobre información de depósitos y de sus titulares (NPB4-32)
37	Normas para determinar las sociedades que pueden formar parte de los conglomerados financieros (NPB4-33)
38	Normas para la modificación de pactos sociales de los bancos (NPB4-34)
39	Normas de aplicación de los límites en la asunción de riesgos de los bancos (NPB4-36)
40	Normas para regular los efectos registrales sobre bienes hipotecados a favor de los bancos (NPB4-37)

41	Normas para la elaboración del informe financiero trimestral (NPB4-38)
42	Normas para la utilización del sistema de consulta de deudores vía internet de la Central de Riesgos (NPB4-40)
43	Normas sobre el procedimiento de recolección y emisión de información electrónica de operaciones regulares y sospechosas (NPB4-41)
	Anexos (NPB4-41)
44	Normas para la inscripción de peritos valuadores y sus obligaciones profesionales en el sistema financiero (NPB4-42)
45	Normas para determinar las entidades financieras extranjeras de primera línea (NPB4-43)
46	Normas para la generación de información de los depósitos monetarios y sus titulares (NPB4-44)
47	**Normas para la seguridad física de los cajeros automáticos (NPB4-45)**
48	Normas para la transparencia de la información de los servicios financieros (NPB4-46)
49	**Normas para la gestión integral de riesgos de las entidades financieras (NPB4-47)**
50	**Normas de gobierno corporativo para las entidades financieras (NPB4-48)**
51	Normas para la gestión del riesgo crediticio y de concentración de crédito (NPB4-49)
52	**Normas para la gestión del riesgo operacional de las entidades financieras (NPB4-50)**
53	Normas para la prestación del servicio de banca corresponsal (NPB4-51)

Figura 4 Consolidado de las NPB dictadas por la SSF. [3]

La mayoría de las diferentes normas internacionalmente aceptadas para implantar Seguridad de la Información (COBIT; ITIL, ISO 27002, etc.), dedican un apartado a las consideraciones del riesgo para lo cual se requiere un equipo de personas especializadas en gestión de riesgos y seguridad, entre los cuales se reconocen como también críticos los riesgos tecnológicos y de imagen, que puedan identificar los diferentes riesgos inherentes a la seguridad de la Información, lo que permitirá, con base en un mapa de riesgos, desarrollar los controles correspondientes a fin de administrarlos de manera eficiente.

[3] http://www.ssf.gob.sv/index.php/normativa/normas/513-normas-prudenc-bancos

1.4 Recursos de Tecnología de la Información enunciados en diferentes leyes de El Salvador

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

Da la impresión que el Legislador se preocupó principalmente por el aspecto tributario y eventualmente por algunas consideraciones delictivas, obviando el Tecnológico en sí. También pesa el poco conocimiento generalizado en nuestros abogados de los aspectos técnicos propios de este ámbito, dificultando que se presente a la Asamblea Legislativa, una propuesta de ley que regule de manera integral y sistemática dichos usos y por ende la seguridad de la Información.

Presentamos contenidos enunciados en leyes de El Salvador relativos a recursos de Tecnologías de la Información en los que el legislador aborda dicha temática de forma que abarca desde conceptualizaciones generales hasta algunas transacciones electrónicas y la forma como deben ejecutarse, y 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 definiciones ni en un enfoque integral de seguridad.

Encontramos incluso el caso extremo de como en El Salvador 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.[4]

[4] Ley Especial contra Actos de Terrorismo
Art. 12 Delito Informático y art. 46 Régimen de las Pruebas

Evidenciando 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 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 las entidades financieras, 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 en la entidad financiera con impacto negativo directo en su imagen y en algunos casos afectar las utilidades del ejercicio.

Las Entidades Financieras en casos de sucederse un fraude que es evidenciado ya sea por sus controles internos o denunciado por el usuario, 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, y mucho menos se tipifican asocian dichos eventos como fallas en la seguridad de la información.

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, algunos recursos tecnológicos y/o transacciones, se han mencionado ya 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 en las que se denota un crecimiento explosivo sin una adecuada regulación legal, se visualiza una 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”.[5]

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, así:

“**SECCIÓN SEXTA**
MEDIOS DE REPRODUCCIÓN DEL SONIDO, VOZ O DE LA IMAGEN
Y ALMACENAMIENTO DE INFORMACIÓN
Medios de reproducción de imágenes o palabras
Art. 396.- Los medios de reproducción del sonido, la voz, los datos o la imagen podrán ser propuestos como medios de prueba.

1.4.2 Medios de almacenamiento de información

Art. 397.- Los recursos de almacenamiento de datos o de información podrán ser propuestos como medio de prueba.

Para este fin, se aportarán **las cintas, discos u otros medios** en los que esté contenido el material probatorio; cuando la otra parte lo pidiera, se llevarán a la

[5] Ley de Simplificación Aduanera
art.8-b Bases de Datos de acceso privado

sede judicial los soportes en que se encuentren almacenados los datos o la información.
Si el traslado no fuere posible, el juez acudirá al lugar en el que la información se encuentre, previa cita de partes.

Proposición

Art. 398.- La proposición como prueba de los medios de reproducción del sonido o de la imagen, así como los **soportes magnéticos o informáticos donde se almacena información,** deberá hacerse según lo prescrito en este código. El proponente indicará el lugar donde el material se encuentra para que el juez lo requiera o se persone en dicho lugar.

Necesidad de reproducción en audiencia

Art. 399.- La parte que pretendiere utilizar este medio de prueba deberá remitir al tribunal y a la parte contraria copia de los materiales cuya utilización solicita, salvo que ello resultare excesivamente gravoso o no se encontrare a su disposición. En este caso, el juez ordenará su exhibición y aportación al proceso.

Los medios de reproducción del sonido o de la imagen y el almacenamiento de información deberán ser expuestos en audiencia, si fuere necesario.

Para este efecto, la parte deberá poner a disposición el soporte técnico donde conste y el medio que permita evidenciar su contenido. Si no fuere posible el traslado del instrumento donde la información se encuentre almacenada, el juez y las partes se trasladarán al lugar respectivo.

Necesidad de auxilio pericial

Art. 400.- Si para poner en práctica la grabación o duplicación se requiriese, además, de conocimiento especializado, el juez podrá designar un perito para ese solo efecto. **Se aplicará lo mismo en caso de información almacenada".**[6]
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, 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 sobrepasando la 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 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?

INFORNET, una empresa Guatemalteca, maneja 4 millones de datos de salvadoreños; información personal que vende por Internet, al que mejor pague por ella.

-¿Cómo obtuvieron esa información personal?

Esto concuerda extrañamente, con un caso público en El Salvador, en el 2003, cuando la ex presidenta del RNPN denunció que después de la 6 de la tarde hubo una intromisión al sistema informático del Duicentro. Nunca se investigó quiénes fueron ni qué sacaron.

---

[6] **CÓDIGO PROCESAL CIVIL Y MERCANTIL**
ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR
18 de Septiembre de 2008

La gente en la calle va andar vendiendo de todo al que mejor le pague y los delincuentes se seguirán escondiendo tras la supuesta impunidad que genera estar detrás de un ordenador.
La Asociación Salvadoreña para la Protección de Datos e Internet (INDATA El Salvador) propondrá este tipo de situaciones al gobierno, a instituciones públicas para que se cree una vigilancia permanente de la red.

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 implanta 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 de Teledespacho 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.

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 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 en la comunicación, la Firma Electrónica tiene la virtud de ser un mecanismo de transparencia proporcionando el máximo grado de confidencialidad y seguridad en internet.[7]

[7] Secretaría para Asuntos Legislativos y Jurídicos de la Presidencia (2012). "DOCUMENTO EXPLICATIVO DEL ANTEPROYECTO DE LEY DE FIRMA ELECTRÓNICA EL SALVADOR"

El uso de las firmas digitales y la factura electrónica será un gran impulso al Comercio electrónico en general, potenciando la demanda, facilidad de compra y mayores elementos de control para ambas partes, esto también abarca al sector gobierno el cual desde 1999 está impulsando iniciativas, aisladas, para implantar el concepto de Gobierno Electrónico, lógicamente se requerirá modificaciones en otras leyes como LACAP.

No obstante en 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 incursionado ya en la atención a los ciudadanos por medio de redes informáticas interconectadas electrónicamente entre sus diferentes sedes, que representan aspectos relacionados con el nacimiento del Gobierno electrónico, alusión a la Ley de Acceso a la Información Pública (LAIP), los Plazos de LAIP y Marco Normativo Internacional del derecho de acceso a la información.

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 a la población estudiantil en el conocimiento y uso de dichos recursos, plantea una utilización masiva de dichas tecnologías 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 en 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.[8]

La difusión masiva de las TIC ha dado origen a lo que se conoce actualmente como las "sociedades de la información" que no son más que sociedades en las que la creación, distribución, y manipulación de la información, forman parte importante de las actividades económicas y culturales de una región determinada, lo que incluye a El Salvador. Esto tiene aplicación cierta y directa en el campo de las empresas gubernamentales y el sector privado.

"Según estadísticas de las Naciones Unidas, el número de teléfonos móviles en el país creció 1,063% respecto al año 2000.

Las suscripciones de telefonía móvil en El Salvador alcanzaron los 8,649,000 al cierre de 2012, según estadísticas de la Unión Internacional de Telecomunicaciones (UIT), la agencia de las Naciones Unidas especializada en las tecnologías de la información y comunicación.

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

Así, El Salvador se ha convertido en un país donde hay más celulares en uso que habitantes, pues según datos oficiales la población alcanzó 6,288,899 personas en 2012. De hecho, las estadísticas de la UIT indican que, en el país, por cada 100 habitantes hay 138,07 teléfonos móviles."

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 una 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 nuestros 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 delincuenciales relacionados o no con el uso de las tecnologías de la Información y no se enfoca en la Seguridad de la información en sí.[9]

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,

[9] Ley Especial contra Actos de Terrorismo
Art. 12 Delito Informático y art. 46 Régimen de las Pruebas

siempre dependientes del Ministerio de Educación y comprendiendo en su estructura organizacional al CONACYT.[10]

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, así:

"CAPÍTULO III PLAN NACIONAL DE CIENCIA Y TECNOLOGÍA

Objeto del Plan

Art. 6. El Plan será el instrumento superior de planificación del desarrollo científico y tecnológico para orientar la gestión del Estado salvadoreño en el sistema educativo y de manera transversal con las otras entidades del Gobierno, empresa privada y organismos no gubernamentales, en concordancia con las Políticas Gubernamentales. Se deberá estimar en el Plan, los recursos necesarios para la implementación de las acciones del mismo."

De igual forma se reorientó el CONACYT (el nuevo CONACYT), para que sus funciones y responsabilidades estén focalizadas a la prestación del servicio de Internet en los centros escolares públicos.

Dentro de la nuevas atribuciones del **Nuevo CONACYT**, está la de organizar, dirigir, y coordinar las actividades e interrelaciones interinstitucionales del **Observatorio Nacional de Ciencia y Tecnología**, que tiene como labor la de : recolección, tratamiento, análisis, y divulgación de la información estadística y estudios provenientes de cada una de las unidades e instituciones dedicadas a la innovación, ciencia y tecnología, según el ***Art. 15 Capitulo V de la Ley de Desarrollo Científico y Tecnológico.***

---

[10] 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

“LEY DE DESARROLLO CIENTÍFICO Y TECNOLÓGICO
CAPÍTULO V
OBSERVATORIO NACIONAL DE CIENCIA Y TECNOLOGÍA

Establecimiento del Observatorio
Art. 15. Se establecerá el Observatorio, como una unidad especializada del MINED que se encargará de la recolección, tratamiento, análisis y divulgación de información estadística y estudios provenientes de cada una de las unidades e instituciones dedicadas a la innovación, ciencia y tecnología”.

En el sitio del Vice Ministerio de Ciencia y Tecnología, encontramos una pestaña nominada “Documentos Científicos” que corresponden a iniciativas como “CENICSH - (Centro Nacional de Investigaciones en Ciencias Sociales y Humanidades), Documentos UNESCO, CICES (Centro Nacional de Investigación Científicas de El Salvador) y otros.

De ello se infiere que en dicha institución, de cara a la Tecnología, no necesariamente de la Información, su enfoque se limita al ámbito de los centros escolares públicos y no a nivel país, no obstante que la ley de creación del Viceministerio de Ciencia y Tecnología consigna “**garantizando la vinculación del desarrollo tecnológico, la educación y la productividad del país.**” [11]

Al revisar cada una de las diferentes publicaciones sobre el listado de decretos y leyes hechas por el Diario Oficial desde el 2012 a Marzo del 2014, se puede comprobar que una Ley del delito informático no cuenta con el impulso de ningún sector fuerte del país, si no que más bien es impulsado por individuos en su carácter personal, que realmente comprende la necesidad de leyes de este tipo y por ende es difícil que el peso que ejerce un pequeño grupo de personas se

[11] **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

compare con el que ejerce un grupo popular que pujan por otro tipo de leyes. Lo antes expuesto es importante desde la perspectiva de la Seguridad de la Información, dado que para tipificar delitos, es necesario que previamente se haya inferido en la definición de la Seguridad de la Información, punto de partida para establecer un orden formal al respecto y por ende estar en la posibilidad de identificar acciones, eventos o situaciones que perturban ese orden que per se, atentan contra la seguridad de la Información.

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 dado 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 grave para todos sus usuarios, accionistas, asociados de negocios, público en general e incluso impactará negativamente en la imagen de las demás entidades financieras, pudiendo llegar a provocar una completa crisis económica a nivel país.

1.6 Seguridad de la Información implantada en Entidades Financieras en El Salvador

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, sobre todo las que sus respectivas casas matrices operan en la bolsa de valores de New York

que tienen por mandato de ley cumplir la Ley Sarbanes Oaxley, Ley SARBOX o Ley SOX (Es una ley de transparencia y control, emitida por el Gobierno de los Estados Unidos de América, el 30 de julio del 2002, como resultado de una serie de escándalos corporativos que afectaron a ciertas empresas estadounidenses a finales del 2001, producto de quiebras, fraudes y otros manejos administrativos no apropiados), , que en sus secciones 302 (Sección 302: Responsabilidad Corporativa por los reportes Financieros), 404 (Sección 404: Valoración, realizada por la administración, respecto de los controles internos) y 902(Sección 902. Intentos y Conspiraciones Para Cometer Infracciones de Fraude Penal), consigna el establecimiento de controles que aseguren la transparencia, integridad y confiabilidad de los datos contenidos en los Estados Financieros los cuales a su vez son respaldados mediante formularios ad-hoc, diseñados específicamente para ese propósito.

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 Superintendencia del Sistema Financiero, para apoyar este aspecto presentamos a continuación, cuadro que contiene indicaciones de 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.

Seguridad de la Información		Norma adoptada										
No.	Bancos Privados	COBIT	ITIL	ISO 27001	Otro	Personal Propio	Por Casa Matriz	Personal Propia + Casa Matriz	Por Terceros	Periodicidad Revisiones	Antigüedad Implantado	PCI-DSS
1	Banco Agrícola , S. A.	4.0 *				X				1 año	+ 5 as	Sí
2	Banco de América Central			X		X				1 año	2 as	Sí
3	Banco Davivienda	4.0						X		3 meses	2 as	Sí
4	Banco Scotiabank	4.0	X				X			1 año	2 as	Sí
5	Banco Citibank El Salvador	4.1		X				X		3 meses	3- 5 as	Sí
6	Banco Promerica				X	X				1 año	+ 5 as	Sí
7	Banco Procredit	N/D	N/D	N/D		N/D	N/D	N/D	N/D	N/D	N/D	N/D
8	Banco Azteca	N/D	N/D	N/D		N/D	N/D	N/D	N/D	N/D	N/D	N/D
9	Banco Industrial de El Salvador	N/D	N/D	N/D		N/D	N/D	N/D	N/D	N/D	N/D	N/D
	Bancos Cooperativos											
10	Multi Inversiones Banco Coop, de Trabajadores Soc. Coop. De R.L. de C. V.	N/D	N/D	N/D		N/D	N/D	N/D	N/D	N/D	N/D	N/D
11	Banco de Los Trabajadores Salvadoreños S. C. de R. L. de C. V. (BTS)	N/D	N/D	N/D		N/D	N/D	N/D	N/D	N/D	N/D	N/D
12	Banco Izalqueño de los Trabajadores S. C. de R. L de C.V.	N/D	N/D	N/D		N/D	N/D	N/D	N/D	N/D	N/D	N/D
13	Primer Banco de los Trabajadores S. C. de R. L. de C.V.	N/D	N/D	N/D		N/D	N/D	N/D	N/D	N/D	N/D	N/D
14	Asoc. Coop. De Ahorro y crédito Vicentina de R. L. ACCOVI de R.L.	N/D	N/D	N/D		N/D	N/D	N/D	N/D	N/D	N/D	N/D

Figura 5 Cuadro con detalle de norma y/o estándar de seguridad adoptado.

Como puede inferirse fácilmente, existe conciencia de la importancia en las entidades financieras filiales de una transnacional, con lo que por otra parte han 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 al 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.

1.7 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, esta 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 implementen 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.

Igualmente la gestión de riesgos de la seguridad de la información, puede ser aplicada a toda la organización, a una porción discreta de la misma organización (departamento, ubicación, servicio, etc.) existentes ó planeados ó un aspecto particular de control.

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

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

Nos centraremos en algunas técnicas muy específicas de los proyectos de análisis y gestión de riesgos, técnicas que no se utilizan en otros contextos de trabajo.

Se han considerado de especial interés las siguientes:

1. Uso de tablas para la obtención sencilla de resultados
2. Técnicas algorítmicas para la obtención de resultados elaborados
3. Árboles de ataque para complementar los razonamientos de qué amenazas se ciernen sobre un sistema de información.

1.7.1.1 Análisis mediante tablas

Dícese, análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En el análisis de riesgos hay que trabajar con múltiples elementos que hay que combinar en un sistema para ordenarlo por importancia sin que los detalles, muchos, perjudiquen la visión de conjunto.

La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí 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:

a) **MB:** Muy Bajo
b) **B:** Bajo
c) **M:** Medio
d) **A:** Alto
e) **MA:** Muy Alto

La estimación del impacto Se puede calcular el impacto 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.

1.7.1.2 Análisis algorítmico.

Dícese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En ciencias químicas, dícese análisis cualitativo del que tiene por objeto descubrir y aislar los elementos o ingredientes de un cuerpo compuesto. A diferencia del análisis cuantitativo que es el que se emplea para determinar la cantidad de cada elemento o ingrediente.

Primero, un modelo cualitativo que busca una valoración relativa del riesgo que corren los activos (¿qué es lo más, frente a qué es lo menos?). Segundo, un modelo cuantitativo que ambiciona responder a la pregunta de cuánto más y cuánto menos.

Un modelo cualitativo

En un análisis de riesgos cualitativo se busca saber qué es lo que hay, sin cuantificarlo con precisión más allá de relativizar los elementos del modelo.

Valores. En un análisis de riesgos es necesario poder valorar, al menos relativamente, los elementos involucrados. En particular, los activos, el impacto de las amenazas y el riesgo que se corre. Para todo ello se usará una escala de niveles simbólicos:

V = { 0, ..., v0, v1, ..., vi, ... }

El valor 0 representa que no vale absolutamente nada.

Esta serie de niveles satisface las siguientes propiedades:

• elemento mínimo:

• orden total:∀ i, 0 < vi ∀ i, vi < vi+1

• existe un elemento singular, *“v0”,* que se denomina “despreciable”.

Informalmente, se dice que un activo tiene “i puntos” para indicar que su valoración es *“vi“*.

El valor de los activos. Cada activo, en cada dimensión, recibe un valor de la escala *V*. Los activos reciben una valoración en cada una de las dimensiones de seguridad.

Las dependencias entre activos. Sólo hay que preocuparse de si un activo A depende, significativamente, o no de otro activo B. Es decir, la dependencia entre activos es un valor booleano: sí o no.

$$A \rightarrow B$$

La dependencia puede ser transitiva:

$$(A \rightarrow B) \wedge (B \rightarrow C)$$

A depende de B; B depende de C.

En este modelo, denominado cualitativo, se han posicionado los activos en una escala de valor relativo, definiendo arbitrariamente un valor *"v0"* como frontera entre los valores que preocupan y los que son despreciables. Sobre esta escala de valor se ha medido tanto el valor del activo, propio o acumulado, como el impacto de una amenaza cuando ocurra y el riesgo al que está expuesto.

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.[12]

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, más 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 y los esfuerzos de un área son desconocidos o entorpecidos por otras. Una de las áreas claramente afectada por este fenómeno

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

es el área de TI, que muchas veces tiene objetivos claros pero estos no están necesariamente alineados con los objetivos del negocio. Otro problema que frecuentemente se adiciona al anterior se materializa por la pobre alineación estratégica entre ambos, ya que los ritmos de desarrollo del área de TI y los ritmos del negocio son diferentes (Ross & Weil, 2002).

El gran problema del gobierno de TI es alinear los objetivos estratégicos de TI con los de la organización. Pareciera este solo un problema de planeación estratégica pero no es necesariamente solo este aspecto el que debe tenerse en cuenta; las áreas de TI están sometidas a diferentes presiones pues deben apoyar la marcha del negocio, soportar además presiones regulatorias, técnicas y comerciales. La respuesta rápida a estas presiones puede llevar fácilmente a perder el alineamiento con la organización y dedicarse a resolver problemas puntuales (Weill, Subramani & Broadbent, 2002).

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.

Entre otros esfuerzos se puede mencionar los que realizan entidades especializadas como: ISACA (*Information Systems Audit and Control Association*), ITGI (*IT Governance Institute*) ITSMF (*IT Service Management Forum*) IT GOVUK (*IT Governance UK*) y ECGI (*European Corporate Governance Institute*) y organizaciones desarrolladoras de estándares como: ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*) y BSI (*The British Standards Institution*). Los aportes de las entidades reguladoras, que vienen emitiendo reportes de absoluto interés y vigencia son: el Informe Coso –

Internal Control - Integrated Framework– (Committee on Sponsoring Organizations of the Treadway Commission [COSO], 1992); el Informe Cadbury –*Report of the Committee on the Financial Aspects of Corporate Governance*– (Cadbury, 1992); el Código Olivencia de Buen Gobierno –*El Gobierno de las Sociedades Cotizadas*– (Olivencia, 1998); el Informe Turnbull –*Report of the Committee on the Financial Aspects of Corporate Governance*– (The Financial Reporting Council [FRC], 2005); el Informe Winter –*Report of the High Level Group of Company Experts on a Modern Regulatory Framework for Company Law in Europe*– (Winter, 2002); el Informe Aldama –*Informe de la Comisión Especial para el fomento de la transparencia y seguridad en los mercados y en las sociedades cotizadas*– (Aldama y Miñon, 2003); y *El Company Law and Corporate Governance* (European Commission, 2011). *Principios de la OCDE para el Gobierno de las sociedades* (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 1999); y *Enhancing Corporate Governance in Banking Organizations del Bank for International Settlements* (Basel Committee on banking supervision, 2005 &2006) cuyos reportes han tenido origen, entre otros, por los escándalos de Enron (Bryce, 2002; McLean & Elkind, 2005) y Worldcom (Jeter, 2003) donde en últimas se han producido fraudes en la información que presentan las corporaciones, a los accionistas y al mundo, aprovechando la falta de control en las tecnologías de información.

Algunas normas y estándares que apoyan el gobierno de TI

Los 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 presentados 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, PMBok (Project Management Institute, 2010) CMMI.[13]

La seguridad de la Información, históricamente ha sido objeto de preocupación de todas las entidades que administran información, unas en mayor grado que otras y es así como en el ámbito de los ejércitos se implantaron modelos de seguridad de la información y se mantuvieron en reserva por la importancia que la misma les confería.

Como resultado surgen, en sus orígenes, "modelos de Seguridad de la Información" entre los cuales se pueden encontrar; Bell La Padula, BIBA y Clark Wilson, el primero focalizado primordialmente en la Confidencialidad, el segundo en la Integridad y el tercero hace un balance entre ambos, aspectos por considerar y de suma importancia y utilidad en cuanto a la Seguridad de la Información.

"**Bell La-Padula**

En seguridad informática, el modelo de seguridad **Bell La-padula** , llamado así por sus creadores Billy Elliott Bell y Len La-Padula, consiste en dividir el permiso de acceso de los usuarios a la información en función de etiquetas de seguridad. Por ejemplo, en sistemas militares norteamericanos, categorizándola en 4 niveles: no clasificado, confidencial, secreto y ultrasecreto.

Este modelo se centra en la confidencialidad y no en la integridad. Se distinguen 2 tipos de entidades, sujetos y objetos. Se define estados seguros y se prueba que cualquier transición se hace de un estado seguro a otro. Un estado se define como

[13] 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.

estado seguro, si el único modo de acceso permitido de un sujeto a un objeto está en concordancia con la política de seguridad."

Posteriormente tenemos publicaciones como la del Ministerio de Defensa de los Estados Unidos de América, el libro, "Criterios de Evaluación de un Sistema de Computo Seguro", conocido como el "Libro Naranja"[14]

Posteriormente y ya con designación para implantar seguridad de la información, aparece la metodología "BS-7799 - British Standard Institute" que en su proceso de evolución natural, sentó las bases para la posterior ISO- 17799 y luego, convertirse en lo que hoy se conoce como ISO/IEC 27001.

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. COBIT sirve de orientación a las instituciones que lo adoptan para cerrar las brechas entre los requerimientos del negocio, aspectos técnicos y necesidades de control. Se trata de un modelo de control para cubrir las necesidades de gobierno de la Tecnología de la Información y asegurar, para garantizar la integridad de los sistemas de información.[15]

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

[14] http://csrc.nist.gov/publications/history/dod85.pdf

[15] http://www.isaca.org/Knowledge-Center/cobit/Pages/FAQ.aspx#1

servicios son definidos en ITIL, como un medio de aportar valor al cliente sin que éste deba asumir los riesgos y costos que implican.[16]

La fase de Estrategia del Servicio es central al concepto de Ciclo de vida del servicio y tiene como principal objetivo convertir la Gestión del Servicio en un activo estratégico. Esta fase de Estrategia del Servicio, es el eje que permite que las fases de Diseño, Transición y Operación del servicio se ajusten a las políticas y visión estratégica del negocio.

Con lo antes expuesto estamos evidenciado que en El Salvador, a pesar del gran auge de la bancarización, país en el que operan grandes y reconocidos bancos a nivel Centro americano e internacional, y que la actividad bancaria tiene fuerte apoyo en la Tecnología de la Información, no se cuenta con una metodología cierta a nivel gremial que oriente o mejor aún que requiera la implantación de seguridad de la información, como forma de asegurar la Confidencialidad, Integridad y Disponibilidad de la Información, para satisfacción de los clientes, proveedores, asociados de negocios, entes rectores y público en general.

[16] http://itilv3.osiatis.es/estrategia_servicios_TI/introduccion_objetivos_creacion_valor.php

CAPÍTULO 2: MARCO TEORICO DE LA ISO 27001, ITIL Y COBIT

2.1 Alcance

Tomando en cuenta que el objetivo principal del presente documento está delimitado a orientar 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 cada uno de los 3 marcos de trabajo que hemos seleccionado, por lo que no abordaremos a fondo la metodología de implantación que cada uno de ellos recomienda, sino que más bien presentamos sus características como sus objetivos de control, procesos, dominios de tal forma que permita obtener una mayor asociación de cada uno de ellos con los procesos de negocio de una institución financiera y determinar si solo es necesario implantar 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 alcance. 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 específicas 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.

Un SGSI, como sistema de gestión que es, de una disciplina específica como lo es la seguridad de la información, debe relacionarse con otros sistemas de gestión, por ejemplo de Gestión de Calidad entre otros. Es así que también deben

considerarse en el contexto, estos otros sistemas y los respectivos estándares metodológicos en los que se apoyan.

Es importante destacar que aunque las últimas versiones publicadas de los diferentes estándares o marcos de referencia que abordaremos en el presente documento, están acercándose cada vez más a brindar un enfoque holístico de gobierno de TI, aun se considera que un solo marco de referencia no alcanza a cubrir todo lo necesario como para lograr una implantación completa de gobierno de seguridad de TI, es por ello que se hace necesario cubrir los vacíos que un estándar puede dejar en el SGSI, con la combinación de varios de ellos.

2.2.1 Serie ISO/IEC 27.000

2.2.1.1 Marco Histórico

ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la International Electrotechnical Commission.

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).
Con la publicación de la ISO 27001:2013, se implantan varios cambios con respecto a la versión 2005. Entre ellos destacan:

- Desaparece la sección "enfoque a procesos" dando mayor flexibilidad para la elección de metodologías de trabajo para el análisis de riesgos y mejoras.
- Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO.
- Pasa de 102 requisitos a 130.
- Considerables cambios en los controles establecidos en el Anexo A, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114.
- Inclusión de un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre empresa y proveedor en la nube.
- Se parte del análisis de riesgos para determinar los controles necesarios y compararlos con el Anexo “A”, en lugar de identificar primero los activos, las amenazas y sus vulnerabilidades.

A continuación se presenta un listado de los 14 dominios, los 35 objetivos de control y los 114 controles que incluye la norma ISO 27002:2013 en el Anexo “A” de la norma, los cuales se presentan con la nomenclatura y numeración tal y como aparece en dicho anexo.

2.2.1.2 Contenido de la norma ISO/IEC 27002

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.

5.1.1 Conjunto de políticas para la seguridad de la información.

5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

6.1 Organización interna.

6.1.1 Asignación de responsabilidades para la seguridad de la información.

6.1.2 Segregación de tareas.

6.1.3 Contacto con las autoridades.

6.1.4 Contacto con grupos de interés especial.

6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos Móviles y Telecomunicaciones.

6.2.1 Política de uso de dispositivos para movilidad.

6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.

7.1.1 Investigación de antecedentes.

7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.

7.2.1 Responsabilidades de gestión.

7.2.2 Concienciación, educación y capacitación en seguridad de la información

7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.

7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.

8.1.1 Inventario de activos.

8.1.2 Propiedad de los activos.

8.1.3 Uso aceptable de los activos.

8.1.4 Devolución de activos.

8.2 Clasificación de la información.

8.2.1 Directrices de clasificación.

8.2.2 Etiquetado y manipulado de la información.

8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.

8.3.1 Gestión de soportes extraíbles.

8.3.2 Eliminación de soportes.

8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.

9.1.1 Política de control de accesos.

9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.

9.2.1 Gestión de altas/bajas en el registro de usuarios.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales.

9.2.4 Gestión de información confidencial de autenticación de usuarios.

9.2.5 Revisión de los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.

9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información.

9.4.2 Procedimientos seguros de inicio de sesión.

9.4.3 Gestión de contraseñas de usuario.

9.4.4 Uso de herramientas de administración de sistemas.

9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.

10.1.1 Política de uso de los controles criptográficos.

10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.

11.1.1 Perímetro de seguridad física.

11.1.2 Controles físicos de entrada.

11.1.3 Seguridad de oficinas, despachos y recursos.

11.1.4 Protección contra las amenazas externas y ambientales.

11.1.5 El trabajo en áreas seguras.

11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.

11.2.1 Emplazamiento y protección de equipos.

11.2.2 Instalaciones de suministro.

11.2.3 Seguridad del cableado.

11.2.4 Mantenimiento de los equipos.

11.2.5 Salida de activos fuera de las dependencias de la empresa.

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.

11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.

11.2.8 Equipo informático de usuario desatendido.

11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.

12.1.1 Documentación de procedimientos de operación.

12.1.2 Gestión de cambios.

12.1.3 Gestión de capacidades.

12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.

12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.

12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.

12.4.1 Registro y gestión de eventos de actividad.

12.4.2 Protección de los registros de información.

12.4.3 Registros de actividad del administrador y operador del sistema.

12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.

12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Gestión de las vulnerabilidades técnicas.

12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.

12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.

13.1.1 Controles de red.

13.1.2 Mecanismos de seguridad asociados a servicios en red.

13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.

13.2.1 Políticas y procedimientos de intercambio de información.

13.2.2 Acuerdos de intercambio.

13.2.3 Mensajería electrónica.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.

14.1.1 Análisis y especificación de los requisitos de seguridad.

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.

14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.

14.2.1 Política de desarrollo seguro de software.

14.2.2 Procedimientos de control de cambios en los sistemas.

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

14.2.4 Restricciones a los cambios en los paquetes de software.

14.2.5 Uso de principios de ingeniería en protección de sistemas.

14.2.6 Seguridad en entornos de desarrollo.

14.2.7 Externalización del desarrollo de software.

14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.

14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.

14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.

15.1.1 Política de seguridad de la información para suministradores.

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.

15.2.1 Supervisión y revisión de los servicios prestados por terceros.

15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.

16.1.1 Responsabilidades y procedimientos.

16.1.2 Notificación de los eventos de seguridad de la información.

16.1.3 Notificación de puntos débiles de la seguridad.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.

16.1.5 Respuesta a los incidentes de seguridad.

16.1.6 Aprendizaje de los incidentes de seguridad de la información.

16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE

LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.

17.1.1 Planificación de la continuidad de la seguridad de la información.

17.1.2 Implantación de la continuidad de la seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.

18.1.1 Identificación de la legislación aplicable.

18.1.2 Derechos de propiedad intelectual (DPI).

18.1.3 Protección de los registros de la organización.

18.1.4 Protección de datos y privacidad de la información personal.

18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.

18.2.1 Revisión independiente de la seguridad de la información.

18.2.2 Cumplimiento de las políticas y normas de seguridad.

18.2.3 Comprobación del cumplimiento.

2.2.1.3 Mapeo de controles de la norma ISO27001:2013 y la ISO27001:2005

		A5 Política de Seguridad	A6 Organización	A7 Administración de Activos	A8 Recursos humanos	A9 Seguridad física	A10 Comunicaciones	A11 Control de Acceso	A12 Adquisición	A13 Incidentes	A14 Continuidad del negocio	A15 cumplimiento
A5.1	Directrices de la Dirección en seguridad de la información	X										
A6.1	Organización interna		X		X		X					
A6.2	Dispositivos móviles y telecomunicaciones							X				
A7.1	Investigación Antes de la contratación				X							
A7.2	Investigación después de la contratación				X							
A7.3	Terminación y cambio de empleo				X							
A8.1	Responsabilidad por los activos			X	X							
A8.2	Clasificación de la información			X			X					
A8.3	Manejo de los soportes de almacenamiento						X					
A9.1	Requisitos de negocio para el control de accesos							X				
A9.2	Gestión de acceso de usuario				X			X				
A9.3	Responsabilidades del usuario.							X				
A9.4	Control de acceso a sistemas y aplicaciones							X	X			
A10.1	Controles criptográficos.								X			
A11.1	Áreas seguras.					X						
A11.2	Seguridad de los equipos					X		X				
A12.1	Responsabilidades y procedimiento de operación						X					
A12.2	Protección contra código malicioso						X					
A12.3	Copias de seguridad						X					
A12.4	Registro de actividad y supervisión						X					
A12.5	Control del software en explotación								X			
A12.6	Gestión de la vulnerabilidad técnica								X			
A12.7	Seguimiento auditorías de los sistemas de información											X
A13.1	Gestión de la seguridad en las redes						X	X				
A13.2	Intercambio de información con partes externas		X				X					
A14.1	Requisitos de seguridad de los sistemas de información						X		X			
A14.2	Seguridad en los procesos de desarrollo y soporte						X		X			
A14.3	Datos de prueba								X			

A15.1	Seguridad de la información con proveedores	X										
A15.2	Gestión de la prestación del servicio proveedores						X					
A16.1	Gestión de incidentes de seguridad de la información									X		
A17.1	Continuidad de la seguridad de la información										X	
A17.2	Redundancias											
A18.1	Cumplimiento de los requisitos legales y contractuales											X
A18.2	Revisiones de la seguridad de la información	X									X	

Figura 6 Mapeo controles ISO 27002, Cobit e ITIL

2.2.1.4 *Flujo de trabajo para su implementación*

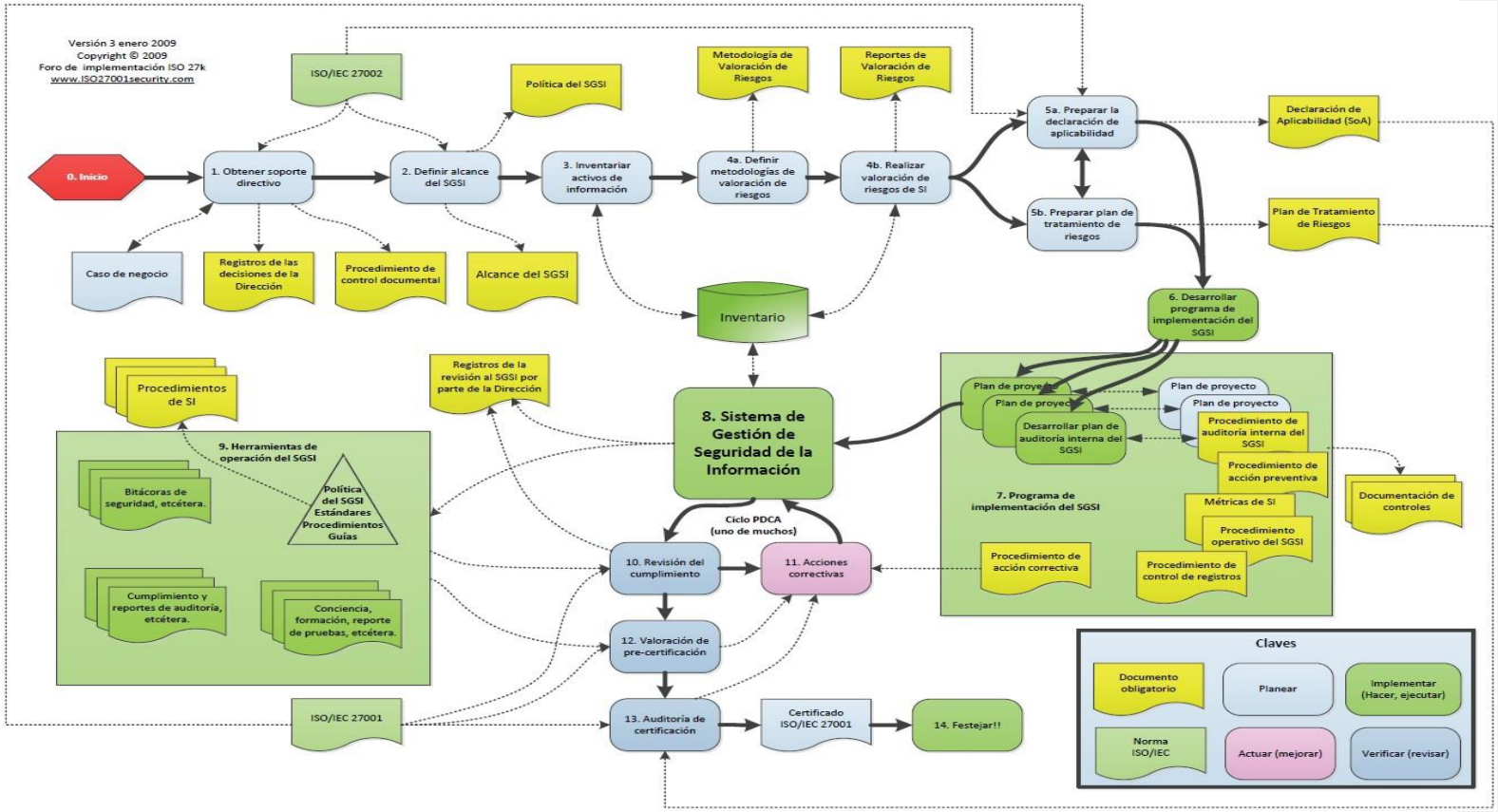


Figura 7 Flujo de Trabajo para su implementación

2.2.2 COBIT 5

2.2.2.1 Marco Histórico.

Figura 8 Representación gráfica de la evolución de COBIT (Mejora Continua)

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 descargar 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 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 (IT), orientado en el negocio y en procesos, y basado en controles. Para ello considera tres dimensiones:

a) los dominios, procesos y actividades de IT;
b) los requerimientos de la información del negocio; y
c) los recursos de IT.

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)*.

En particular, en el dominio A*PO*, se centra la atención en la alineación de IT con los objetivos y estrategia del negocio, y en la gestión de riesgos. Así como en M*EA*, se especifica un proceso de "*Aseguramiento de Continuidad del Servicio / Operaciones*".

A los efectos de satisfacer los objetivos de negocio se definen criterios en términos de requerimientos de la información, ellos son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento (marco legal y reglamentario, normas, contratos, etc.), y confiabilidad. A continuación se presenta un detalle completo de los procesos que se incluyen en COBIT 5.

2.2.2.2 Procesos.

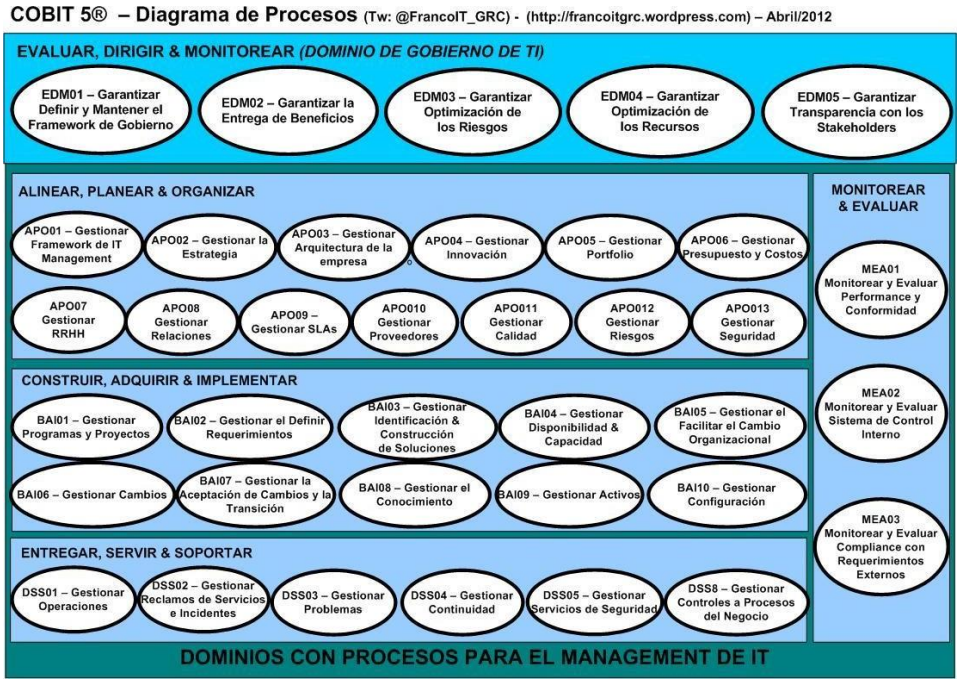


Figura 9 Dominios, Controles y prácticas de control COBIT 5

Tal como se define en el *Marco Referencial* de COBIT, cada uno de los siguientes 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. COBIT incluye:

a) Objetivos de control — Declaraciones genéricas tanto de alto nivel como detallado de un nivel mínimo de buen control
b) Prácticas de control — Motivaciones prácticas y asesoramiento sobre "cómo implantar" los objetivos de control

c) Directrices de auditoría — Asesoramiento para cada área de control sobre cómo obtener un entendimiento, evaluar cada control, evaluar el cumplimiento y sustanciar el riesgo de que los controles no se cumplan
d) Directrices gerenciales — Asesoramiento sobre cómo evaluar y mejorar el desempeño del proceso de TI, utilizando modelos de madurez, métricas y factores críticos de éxito.

Proporcionan un marco de referencia administrativo orientado hacia una continua y proactiva autoevaluación del control, enfocada específicamente en:

– Medición del desempeño —¿Qué tan adecuadamente está apoyando la función de TI los requisitos del negocio? Las directrices gerenciales se pueden utilizar para apoyar talleres de autoevaluación, y también se pueden utilizar para apoyar a la gerencia en la implantación de procedimientos de monitoreo y mejora continuos, como parte de un esquema de gobernabilidad de TI.

– Perfil del control de TI — ¿Cuáles procesos de TI son importantes? ¿Cuáles son los factores críticos de éxito para el control?
– Concientización — ¿Cuáles son los riesgos de no lograr los objetivos?
– Benchmarking — ¿Qué hacen los demás? ¿Cómo pueden medirse y compararse los resultados? Las directrices gerenciales proporcionan ejemplos de métricas que permiten la evaluación del desempeño de TI en términos del negocio. Los indicadores claves de resultados identifican y miden los resultados de los procesos de TI, y los indicadores claves de desempeño evalúan lo bien que están funcionando los procesos, al medir los facilitadores del proceso. Los modelos y los atributos de madurez proporcionan evaluaciones de capacidad así como benchmarking, ayudando a que la gerencia pueda medir la capacidad de control y pueda identificar vacíos de control y determinar estrategias para su mejora.

2.2.2.3 Mapeando los procesos de COBIT 4.1 con los procesos de COBIT 5.

COBIT 4.1	COBIT 5.1

Proceso	Descripción	Primaria	Secundaria
PO	**Planear Organizar**	**Alinear, Planear Organizar**	
PO1	Definir un plan estratégico de TI	APO02	EDM02/APO05
PO2	Definir la arquitectura de la información	APO03	APO01
PO3	Definir la dirección tecnológica	APO02/APO04	EDM01/APO11/DSS06
PO4	Definir los procesos organización y relación de TI	APO01	APO07/APO11/DSS06
PO5	Administrar la inversión en TI	APO06	APO05
PO6	Comunicar las metas y la dirección de la gerencia	APO01	EDM03
PO7	Administrar los recursos humamos de TI	APO12	EDM03/APO01
PO8	Administrar la calidad	APO11	
PO9	Evaluar y administrar los riesgos	APO12	EDM03/APO01
PO10	Administrar los proyectos	BAI01	
A1	**Adquirir e Implementar**	**Construir, Adquirir Implementar**	
AI1	Identificar las soluciones automatizadas	BAI02	
AI2	Adquirir y mantener software aplicativo	BAI03	
AI3	Adquirir y mantener la infraestructura TI	BAI03	DSS02
AI4	Facilitar la operación y el uso	BAi08	BAI05
AI5	Procurar recursos de TI	APO10	BAI03
AI6	Administrar los cambios	BAi06	
AI7	Instalar y acreditar las soluciones y cambios	BAI07	BAI05
DS	**Entrega de Servicio**	**Entregar Servicio y Soportar**	
DS1	Definir y administrar los niveles de servicio	APO09	
DS2	Administrar los servicios de terceros	APO10	

DS3	Administrar el desempeño y la capacidad	BAI04	
DS4	Asegurar el servicio continuo	DSS04	
DS5	Garantizar la seguridad de los sistemas	DSS05	APO13
DS6	Identificar y asignar costos	APO06	
DS7	Educar y entrenar a los usuarios	APO07	
DS8	Administ. la mesa de servicio y los incidentes	DSS02	
DS9	Administrar la configuración	BAI10	DSS02
DS10	Administrar los problemas	DSS03	
DS11	Administrar los datos	DSS04	DSS01/DSS05/DSS06
DS12	Administrar el ambiente físico	DSS01/DSS05	
DS13	Administrar las operaciones	DSS01	DSS05/BAI09
ME	**Monitorear y Evaluar**	**Monitorear y Evaluar**	
ME1	Monitorear y evaluar el desempeño de TI	MEA01	
ME2	Monitorear y evaluar el control interno	MEA02	
ME3	Garantizar el cumplimiento regulatorio	MEA03	
ME4	Proporcionar gobierno de TI	EDM01/EDM02/EDM03/EDM04/MEA02	

Figura 10 Mapeo comparativo COBIT 4.1 versus COBIT 5

2.2.2.4 Ruta de Implantación COBIT 5

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

a) Evaluar las normas de auditoría y prácticas actuales de seguridad de la información

b) Es importante aceptar los principios del modelo COBIT 5, pero más importante aún es que la organización los evalué y acepte para que los pueda impulsar de forma holística.
c) 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.
d) 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.
e) 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 de COBIT deberá ser planeado desde sus inicios cumpliendo con la metodología recomendada, iniciando por el proceso APO (Alinear., Planificar 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 de todos los dominios y procesos cuales son los que más se adaptan a las necesidades del negocio.

Figura 11 Navegación COBIT

2.2.2.5 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 ahora en la versión 5 ya son parte de las metodologías 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 una 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.

Matriz de Asignación de Responsabilidades

	Rol	Descripción	
R	Responsible	Responsable	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R; si existe más de uno, entonces el trabajo deberá ser subdividido a un nivel más bajo, usando para ello las matrices RACI. Es quien debe ejecutar las tareas.
A	Accountable	Aprobador	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	Consulted	Consultado	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	Informed	Informado	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Figura 12 Matriz RACI sde asignación responsabilidades

La siguiente figura muestra un ejemplo de lo que sería la utilización de esta herramienta para el proceso EDM01 (Evaluar, Dirigir, 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.

EDM01 Grafica RACI									
Practicas Clave de Gobierno	CEO	CFO	COO	Dueños de procesos de negocio	Comité ejecutivo estratégico	proyectos	riesgo	Oficial de Continuidad de negocio	Riesgo Operativo
EDM01.01 Evaluar el sistema de gobierno	A	R	C				C	C	C
EDM01.02 Dirigir el sistema de gobierno	A	R	C	C	I	I	C	I	I
EDM01.03 Monitorear el sistema de Gobierno	A	R	C	C	I	R	I	I	I

Figura 13 Matriz RACI prácticas clave de Gobierno

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, estos objetivos por lo general son una lista de objetivos comúnmente utilizados y definidos para sí mismo, Aunque esta lista no es exhaustiva, la mayoría de metas específicas de la empresa se pueden mapear 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
-

Dimensión del BSC	Objetivos empresariales	Relación de Gobierno con objetivos		
		Realización de Beneficios	Optimización de Riesgo	Optimización de Recursos
Financieros	1.Valor para las partes interesadas de las inversiones	P		S
	2.Portafolio de productos y servicios competitivos	P	P	S
	3.Administración del riesgo al negocio		P	S
	4.Cumplimiento con leyes y regulaciones externas		P	
	5.Transparencia financiera	P	S	S
Clientes	6.Cultura de servicio al cliente	P		S
	7.Continuidad y disponibilidad del servicio		P	
	8. Respuesta ágil a los cambios del negocio.	P		S
	9.Desiciones estratégicas basadas en información	P	P	P
	10.Optimizacion de costos en entrega de servicios	P		P
Internos	11.Optimización funcionabilidad de los procesos de negocio	P		P
	12. Optimización de costos en procesos de negocio.	P		P
	13. Programa de administración de cambios de negocio.	P	P	S
	14.Productividad Operacional y Corporativa	P		P
	15.Cumplimiento de políticas internas	P		
Aprendizaje y Crecimiento	16.Personal capacitado y motivado	S	P	P
	17.Cultura de innovación en productos y servicios	P		

Figura 14 Mapeo Objetivos Empresariales versus Objetivos de Gobierno

Mapeo de Procesos

Por ultimo COBIT 5 propone iniciar el análisis del entorno de los objetivos de gobierno relacionándolos con TI, esto, por medio de un mapeo de los procesos corporativos de COBIT 5 con los objetivos de TI para lo cual se marca con (**P**) Primario o (**S**) secundario donde aplique.

Mapeando los objetivos corporativos de COBIT 5 con los objetivos de TI

			Objetivo Corporativo																		
			Valor para las partes interesadas de las inversiones de negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personal entrenado y motivado	Cultura de innovación del producto y del negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Objetivo Relativo a TI			**Financiera**					**Cliente**					**Interna**					**Aprendizaje y Crecimiento**	
Financiera	1	Alineamiento de TI y la estrategia de negocio	P		S		P										S	S	
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S														
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S				S	S		S					S	S	
	4	Riesgos de negocio relacionados con las TI gestionados				S			S					S		S	S		
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P				S		S		S	S			S			S	
	6	Transparencia de los costes, beneficios y riesgos de las TI	S		S					S	S								
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P		S	S		P	S		S			S	S			S	S
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S		S				S	S
Interna	9	Agilidad de las TI	S		S			S							S	S		S	P
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones																	

	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	T P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de las políticas internas por parte de las TI			S	S											P		
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S							S	P

Figura 15 Mapeo Objetivos Corporativos versus Objetivos de TI

Posteriormente se debe realizar el mapeo 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.

Mapeo entre Objetivos relacionados con TI en COBIT 5 con procesos																						
			Objetivo relacionados a TI																			
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnologicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y Aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de Negocio
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Procesos de COBIT 5			Financiera						Cliente		Interna							Aprendizaje y Crecimiento			
Evaluar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	P	S	P			S	P				S	S	S			S	S	S	S

	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S					S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S

Figura 16 Mapeo Objetivos relacionados con TI versus Procesos

2.2.3 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. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

2.2.3.1 Marco Histórico

Aunque se desarrolló durante los años 1980, ITIL no fue ampliamente adoptada hasta mediados de los años 1990. Esta mayor adopción y conocimiento ha llevado a varios estándares, incluyendo ISO/IEC 20000, que es una norma internacional cubriendo los elementos de gestión de servicios de TI de ITIL. ITIL se considera a menudo junto con otros marcos de trabajo de mejores prácticas como la “Information Services Procurement Library-ISPL”, (‘Biblioteca de adquisición de servicios de información’), la “Application Services Library-ASL”, (‘Biblioteca de servicios de aplicativos’), el método de desarrollo de sistemas dinámicos (“DSDM-Dynamic Systems Development Method”), el Modelo de Capacidad y Madurez (CMM/CMMI) y a menudo se relaciona con la gobernanza de tecnologías de la

información mediante COBIT (Control Objectives for Information and Related Technology).

El concepto de gestión de servicios de TI, aunque relacionado con ITIL, no es idéntico: ITIL contiene una sección específicamente titulada «Gestión de Servicios de TI» (la combinación de los volúmenes de Servicio de Soporte y Prestación de Servicios, que son un ejemplo específico de un marco ITSM). Sin embargo es importante señalar que existen otros marcos parecidos. La Gestión de Servicio ITIL está actualmente integrada en el estándar ISO 20000 (anterior BS 15000).

ITIL se construye en torno a una vista basada en proceso-modelo de control y gestión de las operaciones a menudo atribuida a W. Edwards Deming. Las recomendaciones de ITIL fueron desarrolladas en los años 1980 por la "Central Computer and Telecommunications Agency-CCTA" del gobierno británico como respuesta a la creciente dependencia de las tecnologías de la información y al reconocimiento de que sin prácticas estándares, los contratos de las agencias estatales y del sector privado creaban independientemente sus propias prácticas de gestión de TI y duplicaban esfuerzos dentro de sus proyectos TIC, lo que resultaba en errores comunes y mayores costos.

ITIL fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la Gestión de TI. Los nombres ITIL e IT Infrastructure Library ('Biblioteca de infraestructura de TI') son marcas registradas de la Office of Government Commerce ('Oficina de comercio gubernamental', OGC), que es una división del Ministerio de Hacienda del Reino Unido.

En abril de 2001 la CCTA fue integrada en la OGC, desapareciendo como organización separada.1
En diciembre de 2005, la OGC emitió un aviso de una actualización a ITIL v2 conocida comúnmente como ITIL v3, que estuvo planificada para ser publicada a finales de 2006; habiendo sido realizada en junio de 2007. Se esperaba que la publicación de ITIL versión 3 incluyera cinco libros principales, concretamente: Diseño de Servicios de TI, Introducción de los Servicios de TI, Operación de los

Servicios de TI, Mejora de los Servicios de TI y Estrategias de los Servicios de TI, consolidando buena parte de las prácticas actuales de la versión 2 en torno al Ciclo de Vida de los Servicios.
Ref. http://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library
.

2.2.3.2 Certificación

Los particulares pueden conseguir varias certificaciones oficiales ITIL. Los estándares de calificación ITIL son gestionados por la ITIL Certification Management Board (ICMB) que agrupa a la OGC, a ITSMF International y a los dos Institutos Examinadores existentes: EXIN (con sede en los Países Bajos) e ISEB (con sede en el Reino Unido).

Existen tres niveles de certificación ITIL para profesionales:

1. *Foundation Certificate* (Certificado Básico): acredita un conocimiento básico de ITIL en gestión de servicios de tecnologías de la información y la comprensión de la terminología propia de ITIL. Está destinado a aquellas personas que deseen conocer las buenas prácticas especificadas en ITIL.
2. *Practitioner's Certificate* (Certificado de Responsable): destinado a quienes tienen responsabilidad en el diseño de procesos de administración de departamentos de tecnologías de la información y en la planificación de las actividades asociadas a los procesos.
3. *Manager's Certificate* (Certificado de Director): garantiza que quien lo posee dispone de profundos conocimientos en todas las materias relacionadas con la administración de departamentos de tecnologías de la información, y lo habilita para dirigir la implantación de soluciones basadas en ITIL.

No es posible certificar una organización o sistema de gestión como «conforme a ITIL», pero una organización que haya implementado las guías de ITIL sobre Gestión de los Servicios de TI puede lograr certificarse bajo la ISO/IEC 20000.

La versión 3 de ITIL, que apareció en junio de 2007, cambió ligeramente el esquema de Certificaciones, existiendo certificaciones puentes, se definen 3 niveles:

1. *Basic Level* (Equivalente a ITIL Foundation en v2)
2. *Management and Capability Level* (Equivalente a los niveles Practitioner y Manager en ITIL v2)
3. *Advanced Level* (nuevo en v3)

Pero en la versión ITIL v3 publicada en el 2011 las certificaciones se ejemplifican en el siguiente diagrama.

SS = Estrategia del Servicio	SO = Operación del Servicio
SD = Diseño del Servicio	CSI = Mejora Continua del Servicio
ST = Transición del Servicio	

Figura 17 Gráfica fundamentos de ITIL

- Operational Support and Analysis (**OSA**). Gestión de Eventos, Incidentes, Requerimientos, Problemas, Acceso, Service Desk, Gestión Técnica, de Operaciones de TI y de Aplicaciones.

- Planning, Protection and Optimization (**PPO**). Gestión de Capacidad, Disponibilidad, Continuidad, Seguridad, Demanda y Riesgo.

- Release, Control and Validation (**RCV**). Gestión de Cambios, Liberaciones e Implantación, Pruebas, Activos del Servicio y Configuración, Conocimiento, Requerimientos y Validación del Servicio.

- Service Offerings and Agreements (**SOA**). Gestión de Portafolio, Niveles de Servicio, Catalogo, Demanda, Proveedores y Financiera.

2.2.3.3 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, completándose con el quinto proceso aplicable a cada uno de ellos.

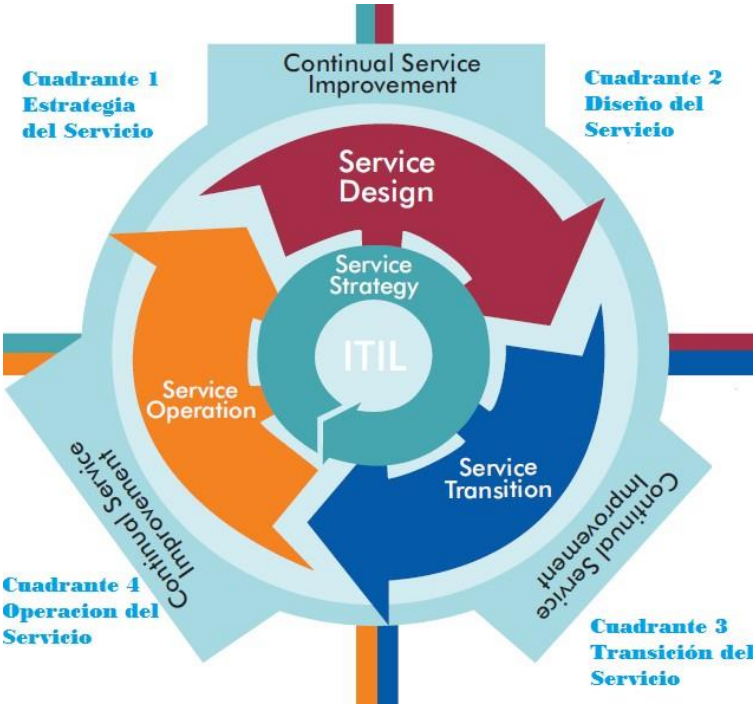


Figura 18 Cuadrantes de ITIL

Ya completando cada uno de los cuadrantes, con sus respectivos procesos tendríamos el siguiente diagrama de procesos del cuadrante uno.

Diagrama de procesos del cuadrante dos.

Figura 19 Cuadrantes versus Procesos ITIL

Diagrama de procesos del cuadrante 3

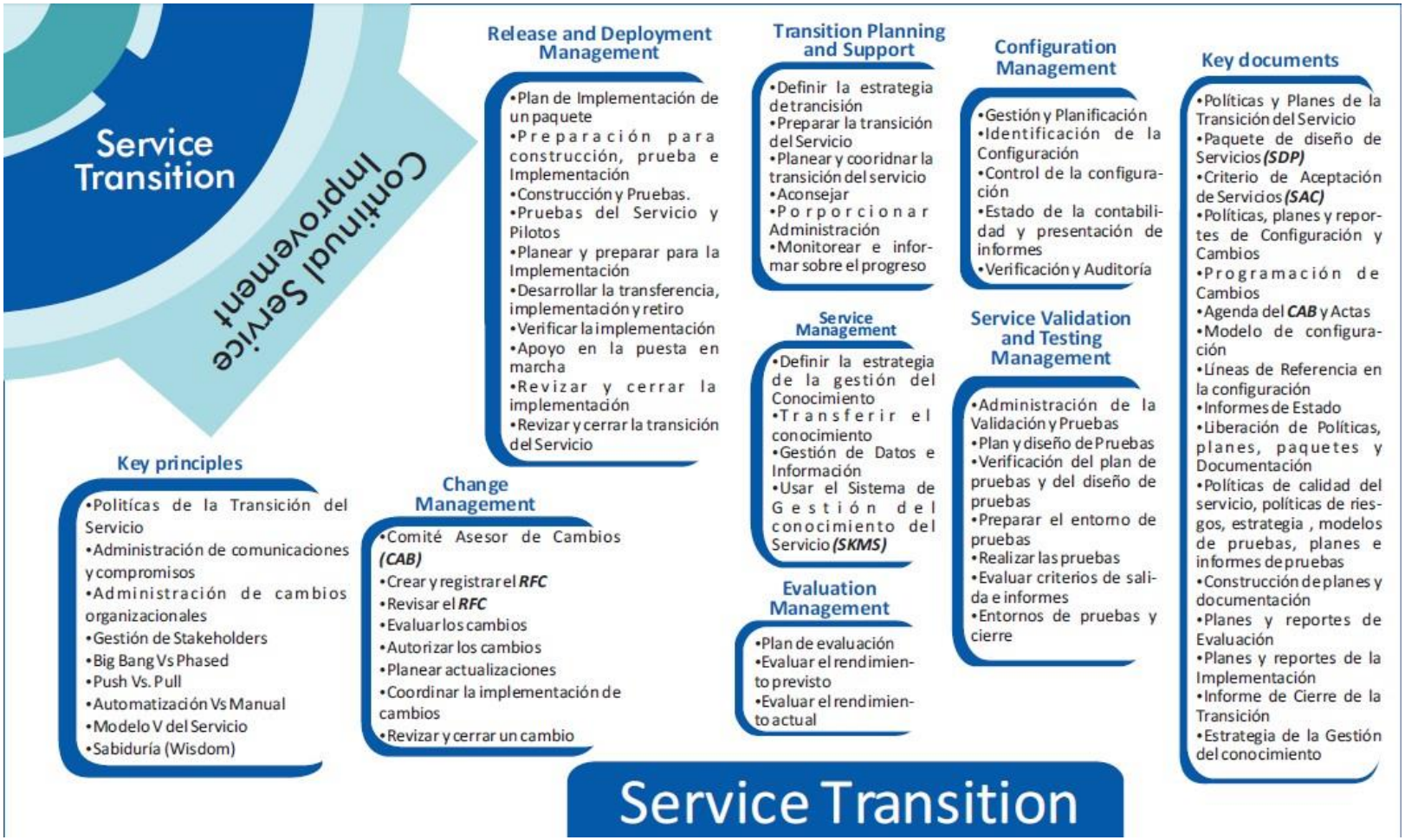
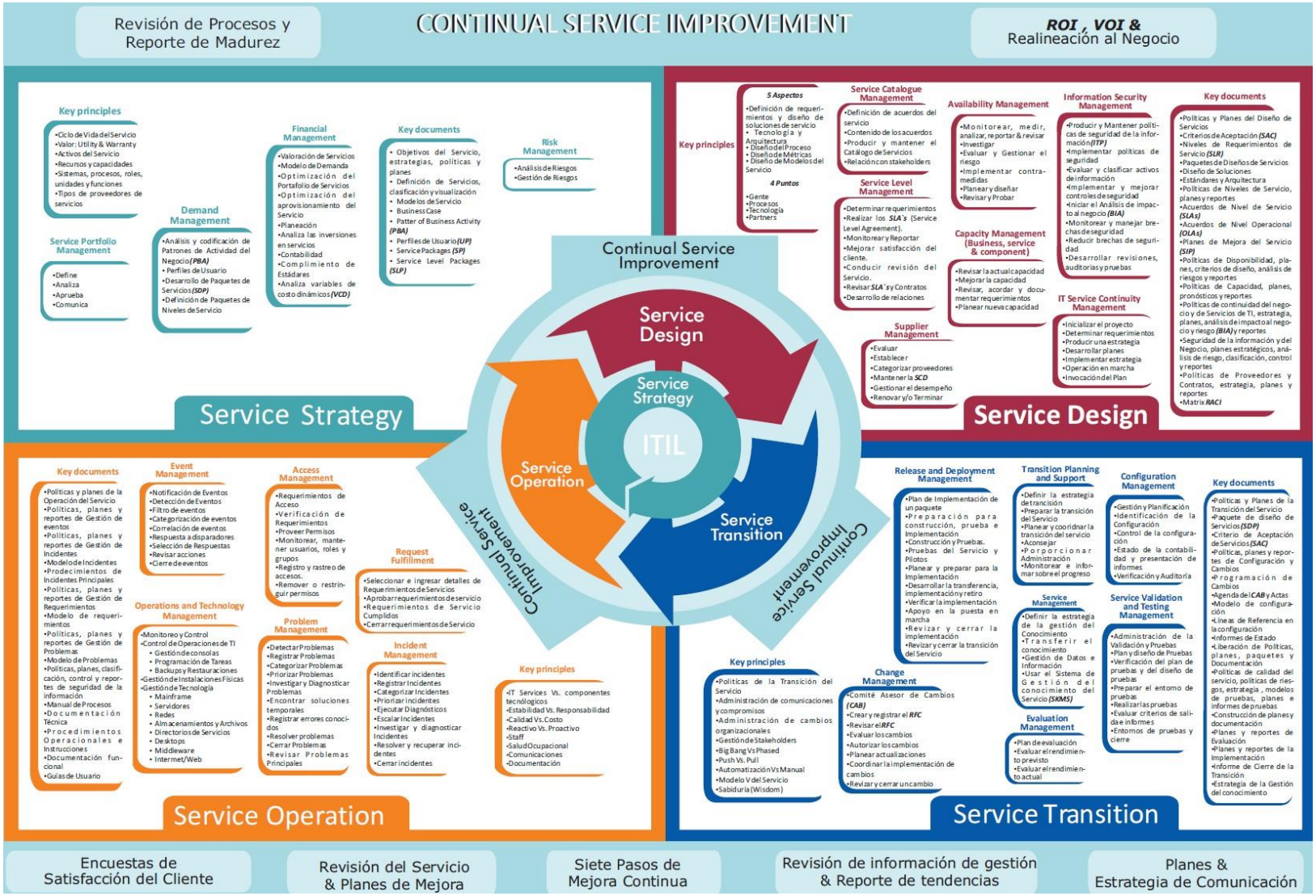


Diagrama de procesos del cuadrante cuatro.


Revisión de Procesos y Reporte de Madurez
CONTINUAL SERVICE IMPROVEMENT
ROI , VOI & Realineación al Negocio
Key principles
•Ciclo de Vida del Servicio
•Valor: Utility & Warranty
•Activos del Servicio
•Recursos y capacidades
•Sistemas, procesos, roles, unidades y funciones
•Tipos de proveedores de servicios
Financial Management
•Valoración de Servicios
•Modelo de Demanda
•Optimización del Portafolio de Servicios
•Optimización del aprovisionamiento del Servicio
•Planeación
•Analiza las inversiones en servicios
•Contabilidad
•Cumplimiento de Estándares
•Analiza variables de costo dinámicos (VCD)
Key documents
• Objetivos del Servicio, estrategias, políticas y planes
• Definición de Servicios, clasificación y visualización
• Modelos de Servicio
• Business Case
• Patter of Business Activity (PBA)
• Perfiles de Usuario (UP)
• Service Packages (SP)
• Service Level Packages (SLP)
Risk Management
•Análisis de Riesgos
•Gestión de Riesgos
Demand Management
•Análisis y codificación de Patrones de Actividad del Negocio (PBA)
• Perfiles de Usuario
•Desarrollo de Paquetes de Servicios (SDP)
•Definición de Paquetes de Niveles de Servicio
Service Portfolio Management
•Define
•Analiza
•Aprueba
•Comunica
Service Strategy
Continual Service Improvement
Service Design
Service Strategy
ITIL
Service Operation
Service Transition
Continual Service Improvement
Continual Service Improvement
Key principles
5 Aspectos
•Definición de requerimientos y diseño de soluciones de servicio
• Tecnología y Arquitectura
• Diseño del Proceso
• Diseño de Métricas
• Diseño de Modelos del Servicio
4 Puntos
•Gente
•Procesos
•Tecnología
•Partners
Service Catalogue Management
•Definición de acuerdos del servicio
•Contenido de los acuerdos
•Producir y mantener el Catálogo de Servicios
•Relación con stakeholders
Service Level Management
•Determinar requerimientos
•Realizar los SLA's (Service Level Agreement).
•Monitorear y Reportar
•Mejorar satisfacción del cliente.
•Conducir revisión del Servicio.
•Revisar SLA´s y Contratos
•Desarrollo de relaciones
Supplier Management
•Evaluar
•Establecer
•Categorizar proveedores
•Mantener la SCD
•Gestionar el desempeño
•Renovar y/o Terminar
Availability Management
•Monitorear, medir, analizar, reportar & revisar
•Investigar
•Evaluar y Gestionar el riesgo
•Implementar contra-medidas
•Planear y diseñar
•Revisar y Probar
Capacity Management (Business, service & component)
•Revisar la actual capacidad
•Mejorar la capacidad
•Revisar, acordar y documentar requerimientos
•Planear nueva capacidad
Information Security Management
•Producir y Mantener políticas de seguridad de la información (ITP)
•Implementar políticas de seguridad
•Evaluar y clasificar activos de información
•Implementar y mejorar controles de seguridad
•Iniciar el Análisis de impacto al negocio (BIA)
•Monitorear y manejar brechas de seguridad
•Reducir brechas de seguridad
•Desarrollar revisiones, auditorías y pruebas
IT Service Continuity Management
•Inicializar el proyecto
•Determinar requerimientos
•Producir una estrategia
•Desarrollar planes
•Implementar estrategia
•Operación en marcha
•Invocación del Plan
Key documents
•Políticas y Planes del Diseño de Servicios
•Criterios de Aceptación (SAC)
•Niveles de Requerimientos de Servicio (SLR)
•Paquetes de Diseños de Servicios
•Diseño de Soluciones
•Estándares y Arquitectura
•Políticas de Niveles de Servicio, planes y reportes
•Acuerdos de Nivel de Servicio (SLAs)
•Acuerdos de Nivel Operacional (OLAs)
•Planes de Mejora del Servicio (SIP)
•Políticas de Disponibilidad, planes, criterios de diseño, análisis de riesgos y reportes
•Políticas de Capacidad, planes, pronósticos y reportes
•Políticas de continuidad del negocio y de Servicios de TI, estrategia, planes, análisis de impacto al negocio y riesgo (BIA) y reportes
•Seguridad de la información y del Negocio, planes estratégicos, análisis de riesgo, clasificación, control y reportes
•Políticas de Proveedores y Contratos, estrategia, planes y reportes
•Matrix RACI
Key documents
•Políticas y planes de la Operación del Servicio
•Políticas, planes y reportes de Gestión de eventos
•Políticas, planes y reportes de Gestión de Incidentes
•Modelo de Incidentes
•Procedimientos de Incidentes Principales
•Políticas, planes y reportes de Gestión de Requerimientos
•Modelo de requerimientos
•Políticas, planes y reportes de Gestión de Problemas
•Modelo de Problemas
•Políticas, planes, clasificación, control y reportes de seguridad de la información
•Manual de Procesos
•Documentación Técnica
•Procedimientos Operacionales e Instrucciones
•Documentación funcional
•Guías de Usuario
Event Management
•Notificación de Eventos
•Detección de Eventos
•Filtro de eventos
•Categorización de eventos
•Correlación de eventos
•Respuesta a disparadores
•Selección de Respuestas
•Revisar acciones
•Cierre de eventos
Operations and Technology Management
•Monitoreo y Control
•Control de Operaciones de TI
• Gestión de consolas
• Programación de Tareas
• Backups y Restauraciones
•Gestión de Instalaciones Físicas
•Gestión de Tecnología
• Mainframe
• Servidores
• Redes
• Almacenamientos y Archivos
• Directorios de Servicios
• Desktops
• Middleware
• Internet/Web
Access Management
•Requerimientos de Acceso
•Verificación de Requerimientos
•Proveer Permisos
•Monitorear, mantener usuarios, roles y grupos
•Registro y rastreo de accesos.
•Remover o restringuir permisos
Problem Management
•Detectar Problemas
•Registrar Problemas
•Categorizar Problemas
•Priorizar Problemas
•Investigar y Diagnosticar Problemas
•Encontrar soluciones temporales
•Registrar errores conocidos
•Resolver problemas
•Cerrar Problemas
•Revisar Problemas Principales
Request Fulfillment
•Seleccionar e ingresar detalles de Requerimientos de Servicios
•Aprobar requerimientos de servicio
•Requerimientos de Servicio Cumplidos
•Cerrar requerimientos de Servicio
Incident Management
•Identificar incidentes
•Registrar Incidentes
•Categorizar Incidentes
•Priorizar incidentes
•Ejecutar Diagnósticos
•Escalar Incidentes
•Investigar y diagnosticar Incidentes
•Resolver y recuperar incidentes
•Cerrar incidentes
Key principles
•IT Services Vs. componentes tecnológicos
•Estabilidad Vs. Responsabilidad
•Calidad Vs. Costo
•Reactivo Vs. Proactivo
•Staff
•Salud Ocupacional
•Comunicaciones
•Documentación
Release and Deployment Management
•Plan de Implementación de un paquete
•Preparación para construcción, prueba e Implementación
•Construcción y Pruebas.
•Pruebas del Servicio y Pilotos
•Planear y preparar para la Implementación
•Desarrollar la transferencia, implementación y retiro
•Verificar la implementación
•Apoyo en la puesta en marcha
•Revizar y cerrar la implementación
•Revizar y cerrar la transición del Servicio
Transition Planning and Support
•Definir la estrategia de transición
•Preparar la transición del Servicio
•Planear y coordinar la transición del servicio
•Aconsejar
•Proporcionar Administración
•Monitorear e informar sobre el progreso
Service Management
•Definir la estrategia de la gestión del Conocimiento
•Transferir el conocimiento
•Gestión de Datos e Información
•Usar el Sistema de Gestión del conocimiento del Servicio (SKMS)
Evaluation Management
•Plan de evaluación
•Evaluar el rendimiento previsto
•Evaluar el rendimiento actual
Configuration Management
•Gestión y Planificación
•Identificación de la Configuración
•Control de la configuración
•Estado de la contabilidad y presentación de informes
•Verificación y Auditoría
Service Validation and Testing Management
•Administración de la Validación y Pruebas
•Plan y diseño de Pruebas
•Verificación del plan de pruebas y del diseño de pruebas
•Preparar el entorno de pruebas
•Realizar las pruebas
•Evaluar criterios de salida e informes
•Entornos de pruebas y cierre
Key documents
•Políticas y Planes de la Transición del Servicio
•Paquete de diseño de Servicios (SDP)
•Criterio de Aceptación de Servicios (SAC)
•Políticas, planes y reportes de Configuración y Cambios
•Programación de Cambios
•Agenda del CAB y Actas
•Modelo de configuración
•Líneas de Referencia en la configuración
•Informes de Estado
•Liberación de Políticas, planes, paquetes y Documentación
•Políticas de calidad del servicio, políticas de riesgos, estrategia , modelos de pruebas, planes e informes de pruebas
•Construcción de planes y documentación
•Planes y reportes de Evaluación
•Planes y reportes de la Implementación
•Informe de Cierre de la Transición
•Estrategia de la Gestión del conocimiento
Key principles
•Políticas de la Transición del Servicio
•Administración de comunicaciones y compromisos
•Administración de cambios organizacionales
•Gestión de Stakeholders
•Big Bang Vs Phased
•Push Vs. Pull
•Automatización Vs Manual
•Modelo V del Servicio
•Sabiduría (Wisdom)
Change Management
•Comité Asesor de Cambios (CAB)
•Crear y registrar el RFC
•Revisar el RFC
•Evaluar los cambios
•Autorizar los cambios
•Planear actualizaciones
•Coordinar la implementación de cambios
•Revizar y cerrar un cambio
Service Strategy
Service Design
Service Operation
Service Transition
Encuestas de Satisfacción del Cliente
Revisión del Servicio & Planes de Mejora
Siete Pasos de Mejora Continua
Revisión de información de gestión & Reporte de tendencias
Planes & Estrategia de Comunicación

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

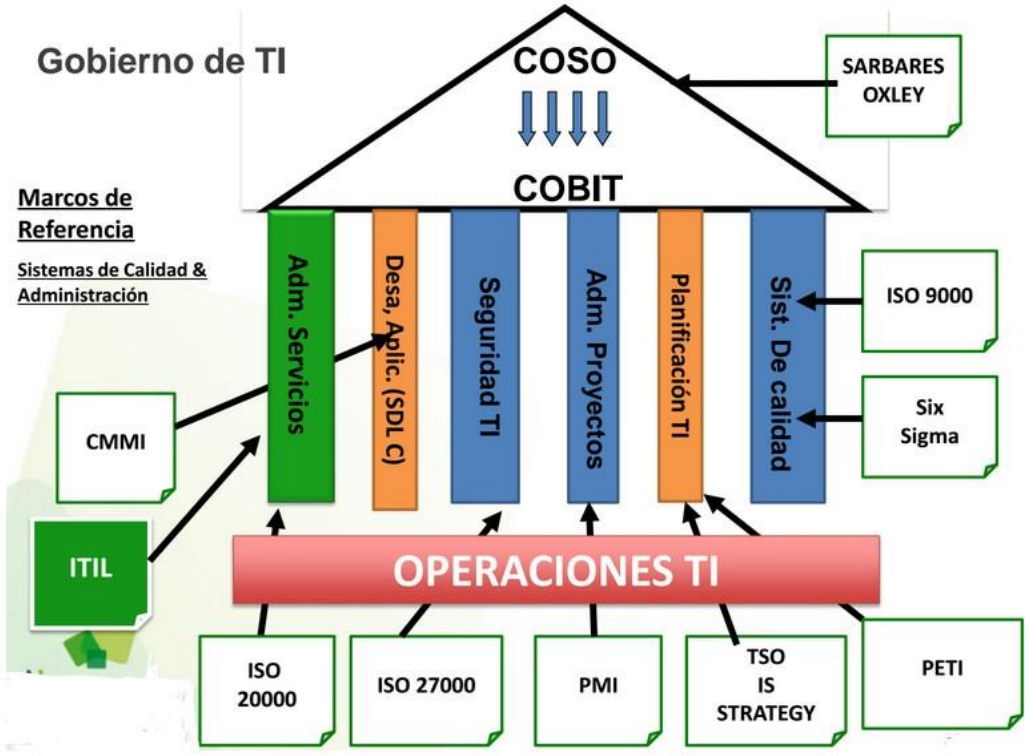


Figura 20 Gobierno de TI

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

- Un proceso es un conjunto estructurado de actividades designadas a lograr un objetivo específico.
- Los procesos toman entradas, procesan, 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.

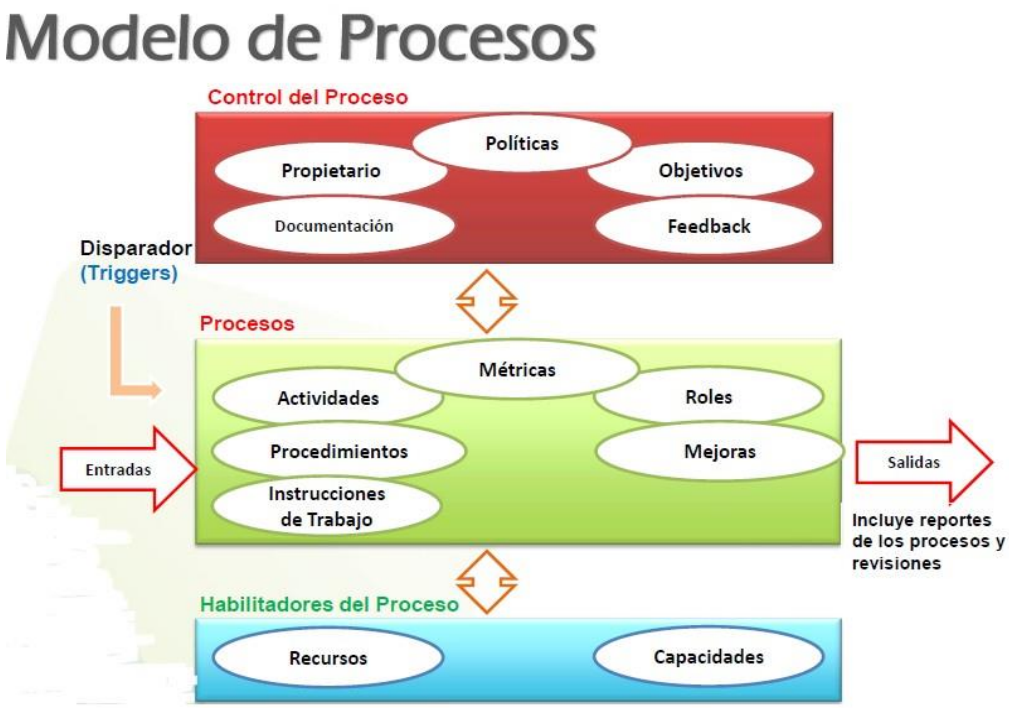


Figura 21 Modelo de Procesos

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.

2.2.3.4 Función

Una función está formada por un grupo de personas con un fin común, quienes utilizan herramientas específicas para llevar a cabo una o más actividades o procesos. Un ejemplo de función es “la mesa de servicio”, que cumple la función de recibir, documentar y darle seguimiento a los incidentes ocurridos, mientras que infraestructura cumplirá el rol de atender y corregir dichos incidentes como una segunda línea de escalamiento.

2.2.3.5 Roles.

Es un conjunto de conductas vinculadas a acciones que son realizadas por una persona, equipo o grupo en un concepto específico.

Roles:

- Analistas de Service Desk (Mesa de Servicio)
- Segunda línea de Soporte
- Administradores de Bases de Datos
- Analistas de Bases de Datos
- Desarrolladores, entre otros
-

Algunos roles importantes para ITIL serían:

- **Gerente de Servicios**: Evalúa, Implanta y administra productos y servicios nuevos y existentes.
- **Dueño del Servicio**: Responsable de un servicio específico siendo de mucha importancia que se defina independientemente de sus procesos, personas o silos verticales o departamentos por los que el servicio atraviese. Es importante que el dueño del servicio este en capacidad de buscar oportunidades de mejora.

2.2.3.6 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 necesarios u obtener la

asesoría de expertos externos a la organización, aunque lo recomendable es capacitar a alguien interno, que 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, la manera de aplicarlos, y los beneficios que ofrecen.
   A largo plazo no será suficiente depender exclusivamente de los conocimientos de asesores externos. La aceptación de un proyecto ITIL dentro de una organización de TI aumentará drásticamente si sus colaboradores internos están en posición de comunicar de forma competente los beneficios de ITIL, y explicar los pasos necesarios para su implantación.

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 debe 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 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 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.

En esta etapa del proyecto no es absolutamente necesario definir los roles en detalle, por ejemplo, en documentos extensos. Esto se hará implícitamente durante las fases subsiguientes del proyecto. Cuando se definan los procesos en detalle, las actividades individuales aparecerán junto con los roles responsables de su ejecución. La mayoría de los sistemas de Gestión de Procesos generan los documentos, en los que se resumen las responsabilidades de cada rol en los procesos.

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. A menudo, el análisis de procesos existentes conlleva documentar laboriosamente estos procesos con mucho detalle.

Según nuestra experiencia, el resultado final, generalmente, no compensa el esfuerzo ya que al analizar los procesos existentes se orienta demasiado hacia el pasado. Una fijación en las prácticas laborales existentes, con frecuencia anticuadas, tiende a obstruir la visión cuando se quiere rediseñar procesos más simples y efectivos.

En vez de ello, 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 de 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.**

   Aquí se debe definir las entradas y las salidas con relación a los demás procesos determinando que salidas debe producir cada uno para que los subsiguientes puedan funcionar. 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. En muchos casos, se producen interrupciones en el flujo de información o en los medios, lo que no permite intercambiar la información deseada.

   La definición de las interfaces de procesos es un paso separado en el proyecto, antes de manejar los entresijos de los proceso en detalle. Obviamente, antes de poder definir las actividades detalladas, debe estar

claro qué entradas válidas puede esperar un proceso de los anteriores, y qué rendimiento debe producir.

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 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 unos beneficios a largo plazo, ya que presenta los datos necesarios para un proceso de mejoramiento continuo.

   ¿Cómo decidir si un proceso "fluye bien" o no? Con este propósito se deben determinar unos criterios objetivos (métricas de calidad, también conocidas como Indicadores Claves de Rendimiento o KPI, en inglés).

   Cuando estén claros los niveles de calidad que debe lograr un proceso, se pueden diseñar con confianza sus detalles, teniendo en cuenta esas metas. Es importante en esta fase determinar los propietarios de los procesos y definir las métricas y procedimientos de medición ó 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 de cada proceso es responsable por esta tarea. Como resultado, se llega a un consenso, el cual se documenta en un diagrama de flujo ó flujograma, detallado del proceso.

Se puede añadir información adicional (como documentos relacionados) que describan los procedimientos y salidas en detalle, para facilitar la ejecución del proceso. Por ejemplo, pueden haber unas páginas extra que describan qué tipo de información se recopilará durante el registro inicial de un incidente.

9. 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.

Se pueden añadir más requisitos (ejemplo: "Crear un Incidente nuevo debe ser posible desde el libro de direcciones de Outlook").

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.

Finalmente, se deben identificar todos los requisitos no funcionales para que resulte, como un todo, la siguiente estructura para el documento de requisitos:

- Requisitos funcionales
  - Referencia a modelos detallados de procesos
  - Requisitos adicionales relacionados con la funcionalidad
  - Definiciones de las salidas de procesos (estructura de datos)
  - Requisitos de informes
- Requisitos no funcionales

    - Requisitos relacionados con capacidades y cantidades
    - Ejecución y rendimiento
    - Escalabilidad / expansión
    - Disponibilidad
- Requisitos desde un punto de vista operacional
- Requisitos desde un punto de vista de Seguridad de TI
- Interfaces con otros sistemas
- Manejo
    - Modelos de procesos
    - Datos que se importarán de sistemas previos

10. Implementación de procesos ITIL y adiestramiento.

Es importante que durante las etapas tempranas del proyecto se involucre a la mayor cantidad de empleados posible, de lo contrario podría haber una falta de aceptación masiva, es por eso que no solo los participantes deben recibir la inducción adecuada.

Ante todo, los participantes se deben familiarizar con los nuevos procesos. Esta 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.

Puede haber un adiestramiento adicional en diferentes niveles:

- Un trasfondo de conocimientos de ITIL es decisivo para el éxito de los nuevos procesos, y debe ser provisto a todas las partes involucradas; el adiestramiento básico de ITIL se puede llevar a cabo al comienzo del proyecto para personal clave, para que pueda comunicar los principios de ITIL a los otros participantes del proyecto.

- Miembros específicos del personal de TI necesitarán un adiestramiento más intensivo, dependiendo de sus roles ITIL
- Tras la implantación de un sistema nuevo o cambiado, pueden ser necesarios adiestramientos sobre su operación
- Como suplemento, se pueden considerar adiestramientos que contribuyan a mejorar la imagen pública de la Organización de TI ("¿Cómo actúo con clientes críticos?")
- Al final, se informa a los clientes si, por ejemplo, se estableció una Mesa de Servicio “Service Desk” nuevo y como resultado, cambió el procedimiento para las solicitudes de servicio.

2.2.3.7 Herramientas utilizadas.

2.2.3.7.1 CMMI-SVC – Capability Mature Model Integration for services

Un conjunto completo de buenas prácticas aplicable para cualquier organización que ofrezca algún servicio y que su giro de negocio dependa mucho de dicho servicio.

A diferencia de COBIT 5, ITIL V3 se apoya mucho en CMMI-SVC, ya que ambos se complementan, por ejemplo ITIL, no contempla una forma objetiva para medir el nivel de madurez en la calidad de los servicios que la organización posee al momento de iniciar el proyecto, dicho de otra forma CMMI-DEV proporciona el qué debe hacerse e ITIL, el cómo.

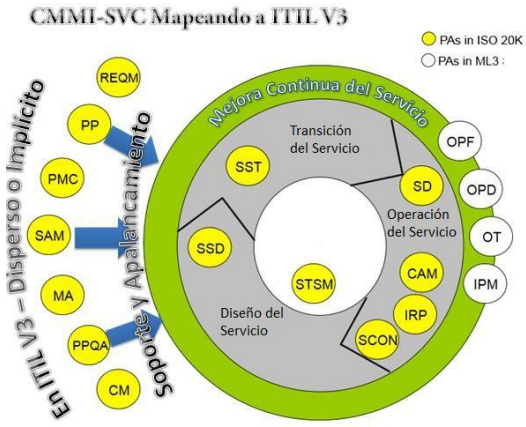


Figura 22 Mejora Continua del servicio

REQM = Administración de Requerimientos

PP-PMC = Administración de Proyectos-Áreas de Proceso

SAM = Administración de acuerdos con proveedores

MA = Medición y Análisis

CM = Administración de Cambios

PPQA = Aseguramiento de Calidad Procesos y Productos.

IPM = Administración de Proyectos Integrales

OT = Entrenamiento Organizacional

OPD = Definición de procesos Organizacionales.

OPF = Enfoque de procesos Organizacionales

2.2.3.7.2 RACI

Al igual que COBIT, ITIL se apoya mucho en RACI, para la designación de roles y responsabilidades, por lo que a continuación se presenta una matriz RACI alineada con algunos procesos de ITIL V3 para lograr comprender mejor este proceso.

En el ejemplo siguiente se puede apreciar cómo se asignan diferentes roles y responsabilidades de acuerdo a los procesos y relacionando cada uno con el ciclo de vida del servicio, en una organización grande estos roles pueden ser

permanentes y ser considerados dentro del organigrama de la organización, mas sin embargo en una organización pequeña varios de estos roles pueden recaer en una sola persona y no necesariamente ocuparía un estatus en el organigrama.

El cuadro siguiente es solo un ejemplo para ilustrar como se llevaría a cabo el desarrollo de la matriz RACI, como una importante herramienta en el proceso de implementar ITIL V3.

Figura 23 Matriz RACI, implementar ITIL

2.2.3.8 Primer Paso.

Es importante como punto de partida si se quiere implantar ITIL V3, tener un entendimiento completo del catálogo de servicios de la organización y una priorización de los mismos a modo de determinar prioridades a la hora de diseñar bien el proyecto, para esta fase es necesario comprender bien la misión y la visión, determinar con qué recursos se cuenta, presupuesto y factores críticos de éxito, no olvide que como parte de los primeros pasos es necesario también conocer el estado actual o el nivel de madurez de cada uno de los servicios a considerar.

CAPÍTULO 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/ICE 27002. La primera defina 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 genera, 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 u 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 integridad. 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 basada 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:

$\mathbf{SC}_{\text{Information type or Information system type}}$ ={(**confidentiality**, impact), (**integrity**, impact), (**availlability**, impact)}

Con estas consideraciones previas, haremos una 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 mas 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.

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 siguiente:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Atención en Agencias (Horario de Agencias)	**APO - Alinear, Planificar y Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.01 APO13.02 APO13.03	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.** 6.1 Organización interna. 6.1.1 Asignación de responsabilidades para la segur. de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.2 Dispositivos para movilidad y teletrabajo. 6.2.1 Política de uso de dispositivos para movilidad.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**11. SEGURIDAD FÍSICA Y AMBIENTAL.** 11.1 Áreas seguras. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios

		11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	
	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1 Responsabilidades y procedimientos de operacion. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad. 12.3.1 Copias de seguridad de la información. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.5 Control del software en explotación. 12.5.1 Instalación del software en sistemas en producción. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoria de los sistemas de información.	**SO - Operación del Servicio** Admon de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
		SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2 Intercambio de información con partes externas. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	

Figura 24 Mapeo de Servicios en Agencias versus Dominios / Controles

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 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.

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Servicios en ATM's (horario 24x7x365)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio

	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**11. SEGURIDAD FISICA Y AMBIENTAL.** 11.1 Areas seguras. 11.1.1 Perimetro de seguridad fisica. 11.1.2 Controles fisicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Areas de acceso público, carga y descarga. 11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.03 MEA02.04 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1 Responsabilidades y procedimientos de operación. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad. 12.3.1 Copias de seguridad de la información. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.5 Control del software en explotación. 12.5.1 Instalación del software en sistemas en producción. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoria de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
		SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2 Intercambio de información con partes externas. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)

		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 25 Mapeo de los servicios en ATM's versus los controles de norma/estándar usados.

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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Kioscos de autoservicio (horario 24x7x365)	**APO - Alinear, Planificar y Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio

DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**11. SEGURIDAD FÍSICA Y AMBIENTAL.** 11.1 Áreas seguras. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1 Responsabilidades y procedimientos de operación. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad. 12.3.1 Copias de seguridad de la información. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.5 Control del software en explotación. 12.5.1 Instalación del software en sistemas en producción. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
	SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2 Intercambio de información con partes externas. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)

		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 26 Mapeo de los servicios en los kioscos de autoservicio

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:

Tabla con formato

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Corresponsales Financieros (Depende del horario de servicio del corresponsal)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.** 6.1.3 Contacto con las autoridades. 6.2 Dispositivos para movilidad y teletrabajo. 6.2.1 Política de uso de dispositivos para movilidad.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios

	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**11. SEGURIDAD FÍSICA Y AMBIENTAL.** 11.1 Áreas seguras. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
		12. SEGURIDAD EN LA OPERATIVA. 12.1 Responsabilidades y procedimientos de operación. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad. 12.3.1 Copias de seguridad de la información. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.5 Control del software en explotación. 12.5.1 Instalación del software en sistemas en producción. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		13. SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2 Intercambio de información con partes externas. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	
		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	

	18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.

Figura 27 Mapeo de los servicios que prestan los corresponsales Financieros

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.

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3

Captación de Fondos (horario de Agencias)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.** 6.1 Organización interna. 6.1.1 Asignación de responsabilidades para la segur. de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.2 Dispositivos para movilidad y teletrabajo. 6.2.1 Política de uso de dispositivos para movilidad.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en seguridad de la información	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**11. SEGURIDAD FÍSICA Y AMBIENTAL.** 11.1 Áreas seguras. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1 Responsabilidades y procedimientos de operación. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.5 Control del software en explotación. 12.5.1 Instalación del software en sistemas en producción. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio

		SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2 Intercambio de información con partes externas. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2 Redundancias. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
		18. CUMPLIMIENTO. 18.1 Cumplimiento de los requisitos legales y contractuales. 18.1.1 Identificación de la legislación aplicable. 18.1.3 Protección de los registros de la organización. 18.1.4 Protección de datos y privacidad de la información personal. 18.2.2 Cumplimiento de las políticas y normas de seguridad. 18.2.3 Comprobación del cumplimiento.	

Figura 28 Mapeo de los Servicios de Captación de Fondos

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 de las consideraciones operacionales para la entidad financiera que le obligan a observar ciertas medidas en aras que garantizar la recuperación de dichos fondos los cuales fueron aportados por los depositantes.

Se presenta un análisis de este servicio contra los dominios y controles de las normas y estándares considerados para este propósito.

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Colocación de Fondos (horario de Agencias)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.** 6.1 Organización interna. 6.1.1 Asignación de responsabilidades para la segur. de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la informac.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**11. SEGURIDAD FÍSICA Y AMBIENTAL.** 11.1 Áreas seguras. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios

	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1 Responsabilidades y procedimientos de operación. 12.1.1 Documentación de procedimientos de operación. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.3.1 Copias de seguridad de la información. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.5 Control del software en explotación. 12.5.1 Instalación del software en sistemas en producción. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
		SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2 Intercambio de información con partes externas. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		17.ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.2 Redundancias. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
		18. CUMPLIMIENTO. 18.1 Cumplimiento de los requisitos legales y contractuales. 18.1.1 Identificación de la legislación aplicable. 18.1.3 Protección de los registros de la organización. 18.1.4 Protección de datos y privacidad de la información personal. 18.2.2 Cumplimiento de las políticas y normas de seguridad. 18.2.3 Comprobación del cumplimiento.	

Figura 29 Mapeo de los Servicios de Colocación de Fondos

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 ofrecen 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 un 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.

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Banca por Internet (horario 24x7x365)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.** 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio

		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 30 Mapeo de los Servicios de Banca por Internet

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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Banca por Teléfono (horario 24x7x365)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.** 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio

		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las politicas y normas de seguridad.	

Figura 31 Mapeo de los servicios de Banca por teléfono

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 Banco 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 s 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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Banca Móvil (horario 24x7x365)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios

	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.** 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 32 Mapeo del servicio de BancaMóvil

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 es de 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 el cliente recibe un servicio de calidad en todos sus aspectos. Dado que la Ley de Bancos regula el “secreto

Bancario", 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 ente erector, 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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Call Center (horario 7x24x365)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la informac.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios

	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
		13. SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 33 Mapeo de los Servicios de Call Center

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 las información referidas en este trabajo, para mantener a 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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3

Tarjetas de Crédito (horario 24x7x365)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la información	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio

		13. SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 34 Mapeo del servicio por medio de Tarjetas de Crédito (Nacional /Internacional)

3.3.12 Tarjetas de Débito

El servicio de las tarjetas de crédito, evoluciono con el aparecimiento 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, hacer 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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Tarjetas de Débito (horario 24x7x365)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la informac.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios

	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
		13. SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
		17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 35 Mapeo del servicio Tarjetas de Débito contra las normas / estándares.

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 una 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 hemos 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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3

Comercio Exterior (horario Restringido)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la informac.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio

	13. SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
	18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 36 Mapeo del servicio comercio Exterior

3.3.14 Fianzas, Avales 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, Avales 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 presento.

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, Avales y Garantías Bancarias contra las normas y estándares ya referidos:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Fianzas, Avales y Garantías (horario Restringido)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la informac.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
	DSS - Entregar, dar Servicio y Soporte DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios

	MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**18. CUMPLIMIENTO.** 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio **Mejora Continua del Servicio** (aplica para los cuatro previos)

Figura 37 Mapeo del Servicio Fianzas, Avales y Garantías Bancarias

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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Mercado Bursatil (horario Restringido)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la informac.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI
	BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio

DSS - Entregar, dar Servicio y Soporte DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
	13. SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	**Mejora Continua del Servicio** (aplica para los cuatro previos)
	18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 38 Mapeo del Servicio Mercado Bursátil

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 el 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:

Servicio / Norma ó Estándar Aplicable	COBIT 5	ISO 27002	ITIL V.3
Medios de Pago (horario Restringido y condicionado a Servicio del BCR)	**Alinear, Planificar, Organizar** APO01.06 APO03.02 APO09.03 APO11.02 APO13.02	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.** 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en segur. de la informac.	**SS - Estrategia del Servicio** Generación de estrategia Administración de la demanda Administración del portafolio de servicios Administración Financiera de TI

BAI - Construir, Adquirir e Implantar BAI09.01	**9. CONTROL DE ACCESOS.** 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	**SD - Diseño del Servicio** Admón de proveedores Admón catalogo de servicios **Admón de la Seguridad** Admón de la capacidad Admón de la disponibilidad Admón de los niveles de servicio
DSS - Entregar, dar Servicio y Soporte DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.05 DSS04.06 DSS04.07 DSS04.08 DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06 DSS05.07 DSS06.06	**10. CIFRADO.** 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves.	**ST - Transición del Servicio** Admón del conocimiento Evaluación Validación servicios/pruebas Planeación de la transicción y soporte Admón de liberaciones y distribución Activos / Servicios / Admón configuraciones Admón de Cambios
MEA - Supervisar, Evaluar y Valorar MEA01.01 MEA01.02 MEA01.04 MEA01.05 MEA02.01 MEA02.06 MEA02.08 MEA03.02	**12. SEGURIDAD EN LA OPERATIVA.** 12.1.2 Gestión de cambios. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información.	**SO - Operación del Servicio** Admón de Operaciones Admón de aplicaciones Admón técnica Requerimientos y peticiones Admón de eventos Admón de accesos Admón de problemas Admón de incidentes Mesa de Servicio
	13. SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.2.3 Mensajería electrónica.	**Mejora Continua del Servicio** (aplica para los cuatro previos)

		13.2.4 Acuerdos de confidencialidad y secreto.	
		18. CUMPLIMIENTO. 18.1.5 Regulación de los controles criptográficos. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	

Figura 39 Mapeo del Servicio Medios de Pagos.

3.3.16 Conclusión

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 aunado a la 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, este ejercicio hemos encontrado que para ninguna 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 Debito de aceptación internacional han implantado la norma “PCI-DSS Payment Card Industry Data Securirty Standard”, la cual incluso manda en lo referente al cifrado de datos (también consignado en COBIT e ITIL v.3), usar una algoritmo de cifrado específico, so pena de no poder 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 así emitida por dicha entidad financiera.

CAPÍTULO 4: METODOLOGÍA PARA SELECCIONAR LAS 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:

COBIT 5			
			Prácticas
No.	Dominios	Procesos	de Control
1	EDM - Evaluar, Orientar y supervisar	5	15
2	APO - Alinear, Planificar y Organizar	13	72
3	BAI - Construir, Adquirir e Implantar	10	68
4	DSS - Entregar, dar Servicio y Soporte	6	38
5	MEA - Supervisar, Evaluar y Valorar	3	17
		37	**210**

IS0 27002:2013			
No.	Cláusulas de Control	Objetivos	Controles
1	Política de Seguridad	1	2
2	Organización de la Seguridad de la Información	2	7
3	Seguridad de Recursos Humanos	3	6
4	Gestión de Activos	3	10
5	Control de Accesos	4	14
6	Cifrado	1	2
7	Seguridad Física y Ambiental	2	15
8	Seguridad Operacional	7	14
9	Seguridad en las Telecomunicaciones	2	7
10	Adquisición, Desarrollo y Mantenimiento	3	13
11	Relaciones con Proveedores	2	5
12	Gestión de Incidentes de la Seguridad	1	7
13	Gestión de la Continuidad del Negocio	2	4
14	Cumplimiento	2	8
		35	**114**

Procesos y Funciones ITIL v.3			
Dominios	**Funciones**		
SS - Estrategia del Servicio	Generación de Estrategia		**CSI**
	Admón. de la Demanda		**M**
4	Admón. Portafolio de Servicios		**E**
	Admón. Financiera de TI		**J**
			O
SD - Diseño del Servicio	Admón. de Proveedores		**R**
	Admón. Catálogo de Servicios		**A**
	Admón. de la Seguridad		

7	Admón. de la Continuidad	C
	Admón. de la Capacidad	O
	Admón. de la Disponibilidad	N
	Admón. Niveles de Servicio	T
ST - Transición del Servicio		
	Admón. del Conocimiento	I
	Evaluación	N
	Validación Servicios /Pruebas	U
8	Planeación de la Transición y Soporte	A
	Admón. de Liberaciones y Distribución	
	Activos Servicio / Admón. Configuraciones	D
	Admón. de Cambios	E
SO - Operación del Servicio		
	Admón. de Operaciones	L
	Admón. de Aplicaciones	
	Admón. Técnica	S
	Requerimientos y Peticiones	E
9	Admón. de Eventos	R
	Admón. de Accesos	V
	Admón. de Problemas	I
	Admón. de Incidentes	C
	Mesa de Servicio	I
		O

Figura 40 Dominios, Controles, Servicios

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 circulo de Deming o circulo 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 el siguiente cuadro.

PROCESOS DE NEGOCIOS ENTIDADES FINANCIERAS - BANCOS				
Procesos y sus Servicios Financieros	Servicio en AGENCIAS	Servicio en ATM'S	KIOSCOS de Autoservicio	CORRESPONSALES FINANCIEROS

versus Normas y/o Estándar COBTI 5		Ventanilla	PLATAFORMA	Créditos Personales	Tarjetas	Retiro de Efectivo	Consulta de Saldos	Remesas Familiares	Recarga de Efectivo	Estado de Cuenta	Solicitud Chequera	Consulta Préstamo	Pago de servicios	Pago a Tarjeta	Solicitud Chequera	Transferencia	Pago de Servicios
EDM- Evaluar, Orientar y supervisar	EDM01	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	EDM02																
	EDM03	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
	EDM04																
	EDM05																
APO- Alinear, Planificar y Organizar	APO01	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
	APO02																
	APO03	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
	APO4	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
	APO05																
	APO06																
	APO07																
	APO08																
	APO09	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
	APO10																
	APO11	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
	APO12																
	APO13 APO13.01 APO13.02	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
BAI - Construir, Adquirir e Implantar	BAI01																
	BAI02																
	BAI03																
	BAI04																
	BAI05																
	BAI06	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
	BAI07																
	BAI08																
	BAI09	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
	BAI10	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S
DSS- Entregar, dar Servicio y Soporte	DSS01																
	DSS02																
	DSS03																
	DSS04 DSS04.01 al DSS04.08	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	DSS05 DSS05.01 al DSS05.07	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	DSS06	S		S	S	S	S	S	S	S	S	S	S	S	S	S	S

MEA-Supervisar, Evaluar y Valorar	MEA01 MEA01.01 MEA01.02 MEA01.04 MEA01.05	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	MEA02 MEA02.01 MEA02.03 MEA02.04 ,EA02.06 MEA02.08	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	MEA03 MEA03.02	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P

Figura 41 Mapeo de Procesos de Servicios contra Dominios / Controles COBIT 5

PROCESOS DE NEGOCIOS ENTIDADES FINANCIERAS - BANCOS																
Procesos y sus Servicios Financieros versus Normas y/o Estándar ISO 27002 : 2013	Servicio en AGENCIAS				Servicio en ATM'S				KIOSCOS de Autoservicio				CORRESPONSALES FINANCIEROS			
	Ventanilla	**PIATAFORMA**	**Créditos Personales**	**Tarjetas**	**Retiro de Efectivo**	**Consulta de Saldos**	**Remesas Familiares**	**Recarga de Efectivo**	**Estado de Cuenta**	**Solicitud Chequera**	**Consulta Préstamo**	**Pago de servicios**	**Pago a Tarjeta**	**Solicitud Chequera**	**Transferencia**	**Pago de Servicios**
5. POLÍTICAS DE SEGURIDAD.																
5.1 Directrices de la Dirección en seguridad de la información.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
5,2 Divulgación de la																
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.																

Tabla con formato

Tabla con formato

6.1 Organización interna.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
6.2 Dispositivos para movilidad y teletrabajo.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.																	Tabla con formato
7.1 Antes de la contratación.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
7.2 despúes de la contratación	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
7.3 Cese o cambio de puesto de trabajo.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
8. GESTIÓN DE ACTIVOS.																	Tabla con formato
8.1 Responsabilidad sobre los activos.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
8.2 Clasificación de la información.	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
8.3 Manejo de los soportes de almacenamiento.	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
9. CONTROL DE ACCESOS.																	Tabla con formato
9.1 Requisitos de negocio para el control de accesos.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
9.2 Gestión de acceso de usuario.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
9.3 Responsabilidades del usuario.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
9.4 Control de acceso a sistemas y aplicaciones.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
10. CIFRADO.																	Tabla con formato
10.1 Controles criptográficos.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
11. SEGURIDAD FÍSICA Y AMBIENTAL.																	Tabla con formato
11.1 Áreas seguras.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
11.2 Seguridad de los equipos.	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
12. SEGURIDAD EN LA OPERATIVA.																	Tabla con formato

12.1 Responsabilidades y procedimientos de operación.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
12.2 Protección contra código malicioso	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
12.3 Copias de seguridad	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
12.4 Registro de actividad y supervisión.	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
12.5 Control del software en explotación.																	
12.6 Gestión de la vulnerabilidad técnica.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
12.7 Consideraciones de las auditorías de los sistemas de información.																	
13. SEGURIDAD EN LAS TELECOMUNICACIONES .																	
13.1 Gestión de la seguridad en las redes.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
13.2 Intercambio de información con partes externas.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.																	
14.1 Seguridad en los procesos de desarrollo y soporte	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
14.2 Seguridad en los procesos de desarrollo y soporte.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
14.3 Datos de prueba.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
15. RELACIONES CON SUMINISTRADORES.																	

Tabla con formato

Tabla con formato

Tabla con formato

Tabla con formato

15.1 Seguridad de la información en las relaciones con suministradores.	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
15.2 Gestión de la prestación del servicio por suministradores.	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.																	
16.1 Gestión de incidentes de seguridad de la información y mejoras.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.																	
17.1 Continuidad de la seguridad de la información.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
17.2 Redundancias.	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	
18. CUMPLIMIENTO.																	
18.1 Cumplimiento de los requisitos legales y contractuales.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	
18.2 Revisiones de la seguridad de la información.	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	

Tabla con formato

Tabla con formato

Tabla con formato

Figura 42 Mapeo de Procesos de Servicios contra Dominios / Controles ISO/IEC 27002

PROCESOS DE NEGOCIOS ENTIDADES FINANCIERAS - BANCOS																	
Procesos y sus Servicios Financieros versus Normas y/o Estándar ITIL V.3		Servicio en AGENCIAS				Servicio en ATM'S				KIOSCOS de Autoservicio				CORRESPONSALES FINANCIEROS			
		Ventanilla	PIATAFORMA	Créditos Personales	Tarjetas	Retiro de Efectivo	Consulta de Saldos	Remesas Familiares	Recarga de Efectivo	Estado de Cuenta	Solicitud Chequera	Consulta Préstamo	Pago de servicios	Pago a Tarjeta	Solicitud Chequera	Transferencia	Pago de Servicios
SS-Estrategia del	**Generación de Estrategia**	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Admón de la Demanda	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S

Tabla con formato

Servicio	**Admon Portafolio de Servicios**	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Admon Financiera de TI	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
SD- Diseño del Servicio	**Admon de Proveedorres**	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Admon Catalogo de Servicios	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Admon de la Seguridad Propósitos/Metas y Objetivos Alcance Valor para el Negocio Políticas/Principios/Conceptos Básicos Actividades de Procesos/Métodos y Técnicas Disparadores/Entradas/Salidas e Interfaces Indicadores Clave de Ejecución Admon de la Información Desafíos/Factores críticos de Éxito y Riesgos Admon de los Proveedores	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Admon de la Continuidad	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Admon de la Capacidad	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Admon de la Disponibilidad	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Admon Niveles de Servicio	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
ST - Transición del Servicio	**Admon del Conocimiento**	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Evaluación	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Validación Servicios/Pruebas	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Planeación de la Transición y Soporte	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Admon de Liberaciones y Distribución	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Activos Servicios/Admon de Configuraciones	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Admon de Cambios	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
SO _ Operación del Servicio	**Admon de Operaciones**	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Admon de Aplicaciones	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Admon Técnica	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Requerimientos y peticiones	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S

	Admon de Eventos	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
	Admon de Accesos	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Admon de Problemas	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Adon de Incidentes	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P	P
	Mesa de Servicio	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
CSI - Mejora Continua del Servicio	Todos los Servicios	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
		S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
		S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S

Figura 43 Mapeo de Procesos de Servicios contra Dominios / Controles ITIL v.3

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 primarios:

Evaluación Procesos de Servicios			
Norma/Estándar vrs. Controles de Servicios	**COBIT 5**	**ISO/IEC 27002**	**ITIL V.3**
Primarios (P= 2)	448 x 2	384X 2	496 x 2
Secundarios (S = 1)	176 x 1	128 X 1	272 x 1
Resultado (Puntos absolutos)	**1072**	**896**	**1264**

Figura 44 Tabulación aplicación Controles a Procesos de Servicios

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
COBIT	37	16	592		
"P"				448	71.80%
"S"				176	28.20%
Total				**624**	**100.0%**
ISO/IEC 27002	35	16	560		
"**P**"				384	**75.00%**
"S"				128	25.00%
Total				**512**	**100.00%**
ITIL	28	16	448		
"P"				496	64.58%
"S"				272	35.42%
Totales				**768**	**100.00%**

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 del 75% de controles primarios o relevantes, un segundo lugar para COBIT 5 con 71.80% y, 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 para 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.

CAPÍTULO 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 gestión de os riesgos y en especial el análisis de impacto sobre los procesos y/o servicios, identificando vulnerabilidades de los sistemas y/o recursos de TI, con el objetivo de subsanarlos oportunamente logrando con ello un 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 malos informes sobre las relaciones en estas situaciones.

Una técnica alternativa para cambiar la cultura organizacional es un enfoque de abajo hacia arriba. 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.

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 hacía, 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. Esta actividad es conceptualizada como gestión de riesgos.

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 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.[17]

[17] ITIL Version 3 Service Improvement

Referencias

[1] Banco Central de Reserva de El Salvador,
http://www.bcr.gob.sv/esp/

[2] Normas Prudenciales de Bancos.
Superintendencia del Sistema Financiero, El Salvador.
http://www.ssf.gob.sv/
http://www.ssf.gob.sv/index.php/normativa/normas/513-normas-prudenc-bancos

[3] 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

[4] 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:publicació n-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77

[5] Publicación en El Diario Oficial de El Salvador
http://www.imprentanacional.gob.sv/index.php/novedades/avisos/25-avisos-ciudadano

[6] 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).

[7] CÓDIGO PROCESAL CIVIL Y MERCANTIL
ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR
18 de Septiembre de 2008

[8] Ley Especial contra Actos de Terrorismo
Art. 12 Delito Informático y art. 46 Régimen de las Pruebas

[9] Ley de Fomento y Protección a la Propiedad Intelectual

[10] 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)

[11] Código Tributario Sección cuarta Prueba Contable La contabilidad art.209 (no limita tiempo)

[12] CÓDIGO PROCESAL CIVIL Y MERCANTIL
ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR
18 de Septiembre de 2008

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”

[13] 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

[14] Decreto No. 12, “Decreto de Creación del Viceministerio de Ciencia y Tecnología, Consejo de Ministros
R-ecuperado de http://www.cienciaytecnologia.edu.sv/index.php/programas.html

[15] 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:publicació n-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77
http://www.conacyt.gob.sv/index.php?option=com_k2&view=item&id=64:publicació n-de-indicadores-nacionales-de-ciencia-y-tecnología-2012&Itemid=77

[16] 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.

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

[18] http://csrc.nist.gov/publications/history/dod85.pdf

[19] http://www.isaca.org/Knowledge-Center/cobit/Pages/FAQ.aspx#1

[20] http://itilv3.osiatis.es/estrategia_servicios_TI/introduccion_objetivos_creacion_valor.php

[21] Basel Committee on banking supervision. (2006). *Enhancing corporate governance in banking organizations*. Basilea: Bank for International Settlements.

[22] 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

[23] 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.

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

[25] 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.

[26] http://interamerican-usa.com/articulos/Leyes/Ley-Sar-Oxley.htm

[27] MAGERIT – versión 3.0Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

[28] Libro III - Guía de Técnicas / ISO/IEC 27005:2008

[29] http://www.isaca.com

[30] http://cmmiinstitute.com/wp-content/uploads/2013/11/CMMI-SVC-ESP.pdf

[31] http://www.lamri.com/resources/20KDemystified.pdf
[32]http://wiki.es.it-processmaps.com/index.php/Implementaci%C3%B3n_de_ITILEstructura_de_servicios.html

[33] http://en.it-processmaps.com/products/itil-process-map.html