MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Marco de referencia de buenas prácticas para el cumplimiento de la normativa SBS-JB-3066 y su medición del impacto

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la/el estudiante:

Juan Carlos GUALSAQUÍ VIVAR

Bajo la dirección de:

Washington Antonio CEVALLOS GAMBOA

Universidad Espíritu Santo
Facultad de Postgrado
Maestría en Auditoría en Tecnologías de la Información
Guayaquil - Ecuador

Noviembre de 2018

Marco de referencia de buenas prácticas para el cumplimiento de la normativa SBS-JB-3066 y su medición del impacto

Framework for Best practices in compliance with SBS-JB-3066 regulation and its measurement of impact

Juan Carlos GUALSAQUÍ VIVAR1
Washington Antonio CEVALLOS GAMBOA 2

Resumen

La tecnología de la información es la herramienta que ofrece a las organizaciones soporte a la demanda de nuevos productos y servicios financieros para sus clientes. Actualmente, la tendencia de una nueva era digital ha generado que los clientes realicen transacciones a través de distintos canales electrónicos incrementando a su vez potenciales riesgos que pudieran afectar a la seguridad de la información. El presente trabajo desarrolla un marco de referencia de buenas prácticas respecto gobierno tecnológico, continuidad del negocio, seguridad en canales electrónicos, administración de riesgo operativo y seguridad de la información que deberían estar implementadas por las instituciones financieras del país regidas por la Superintendencia de Bancos a fin de dar cumplimiento con la normativa SBS-JB-3066 y evitar cualquier tipo de multas. Para el efecto, se revisaron normativas y buenas prácticas locales e internacionales para desarrollar un marco de referencia con las medidas de seguridad mínimas necesarias que deberían estar implementadas en el sistema de control interno de las instituciones con la finalidad de minimizar amenazas y riesgos relacionados con la seguridad, integridad y disponibilidad de su información. Finalmente, se presenta una medición de estas buenas prácticas aplicadas a una institución financiera determinando requerimientos mínimos y recomendaciones que deberá tomar dicha institución antes de la visita en situ por parte del ente de control.

Palabras clave: Cumplimiento, Canales Electrónicos, Medidas de Seguridad, Seguridad de la Información

Abstract

Information technology is the tool that offers organizations support for the demand for new products and financial services for their clients. Currently, the trend of a new digital age has generated that customers make transactions through different electronic channels, increasing in turn potential risks that could affect the security of information. The present article develops a framework of good practices regarding technological governance, business continuity, security in electronic channels, operational risk management and information security that should be implemented by the country's financial institutions governed by the Superintendence of Banks. For the purpose, local and international regulations and good practices were reviewed to develop a framework with the minimum necessary security measures that should be implemented in the internal control system of the institutions in order to minimize threats and risks related to the security, integrity and availability of your information. Finally, a measurement of these good practices applied to a financial institution is presented, determining minimum requirements and findings that said institution must take before the on-site visit by the control entity.

Key words Compliance, Electronic Channels, Security Measures, Information Security.

1 Estudiante de la Maestría en Auditoría en Tecnologías de la Información, Universidad Espíritu Santo – Ecuador. E-mail jgualsaqui@uees.edu.ec
2 Director de la Facultad de Tecnologías de la Información Universidad Espíritu Santo- Ecuador. acevallos@uees.edu.ec

INTRODUCCIÓN

La tecnología de la información es la herramienta que ofrece a las compañías crecimiento y soporte a la demanda de nuevos productos y servicios financieros; aspectos que se traducen en mayor rapidez, crecimiento del servicio al cliente, incremento de las comunicaciones y mayores capacidades del personal de la compañía para que tome decisiones y actué frente al cambio, más aún en las compañías que administran gama de productos y servicios financieros como financiamientos, inversiones, seguros, tarjetas de crédito a través de medios de pago electrónicos que faciliten las transacciones con los clientes, como su principal estrategia corporativa (Deloitte Touche, 2011). Además, Fanjul Suárez y Valdunciel Bustos (2008) mencionan que los principales servicios financieros han sido impactados sustancialmente por la aplicación de nuevas tecnologías de la información como un componente fundamental para conseguir la consecución de los objetivos corporativos.

También, los cambios que se suscitan como la transformación digital surge por la necesidad de las empresas de adaptarse al cambio en las demandas de sus clientes. El desarrollo de Internet y la telefonía móvil ha trasformado la forma en que los usuarios se relacionan con las empresas; los clientes exigen más servicios en menos tiempo. Para poder responder a estas exigencias, las empresas necesitan transformarse y transformar sus sistemas. La transformación digital viene del lado del consumidor y de la tecnología que necesita la empresa para dar este servicio y soporte a los procesos de negocio (Navarro, 2017).

Sin embargo, la Organización de Estados Americanos en el reporte de seguridad cibernética e infraestructura crítica de las Américas del año 2018 menciona un incremento importante del 69% en el nivel de ataques contra la infraestructura tecnológica de las compañías en Latino América y el Caribe, incluyendo a Ecuador como un país no preparado para solventar un incidente cibernético, debido a la implementación de medidas improvisadas de seguridad. (Organización de Estados Americanos, 2018). Así mismo, Radware (2017) en su reporte *Global Application & Network Security Report 2016-2017* manifiesta que las organizaciones financieras son el principal objetivo de los atacantes cibernéticos, resultando con más de un 40% expuestas a distintos cyber ataques como el de malware (58%), denegación de servicios (51%), ataques a aplicaciones web (57%), entre otros.

Así pues, los resultados de la Encuesta Global de Seguridad de la Información 2016 realizado por *PriceWaterhouseCoopers* determinan que los incidentes de seguridad de la información han aumentado un 38%, mientras que los costos financieros de los incidentes se han incrementado un 58% y aumento de pérdidas financieras a causa de incidentes de seguridad en un 44% (PriceWaterhouseCoopers, 2016).

Como se puede evidenciar en los antecedentes expuestos anteriormente, las compañías financieras son las que sufren el mayor número de ataques cibernéticos en su infraestructura tecnológica debido a la falta de mecanismos de seguridad robustos que permitan evitar posibles riesgos desde el uso no adecuado de información sensible hasta interrupciones en la operatividad que podrían afectar la confidencialidad, integridad y disponibilidad de la información (Radware, 2017).

Para mitigar los riesgos antes expuestos, a nivel local, la Superintendencia de Bancos emitió una serie de disposiciones específicas para la implementación de medidas de seguridad en los canales electrónicos para el cumplimiento de las instituciones financieras controladas por este organismo de control mediante resolución SB-JB-3066 incorporada al Libro I.- Normas Generales para la Aplicación de la Ley General de Instituciones del Sistema Financiero, Título X.- De la gestión y administración de riesgos, Capítulo V.- De la gestión de riesgo operativo (SuperIntendencia de Bancos y Seguros, 2014).

Estas medidas de seguridad establecen y proponen mejoras en la gestión del gobierno de tecnología de la información, comunicaciones, riesgo operativo, continuidad del negocio y de la seguridad de la información, todo esto contribuye a tener un correcto sistema de control interno en la organización y por otra parte permite reducir y mitigar fraudes relacionados al interactuar a través de este tipo de canales electrónicos (The IIA Research Foundation, 2011).

La Superintendencia de Bancos estableció fechas límite de implementación y cumplimiento para los aspectos descritos en la normativa, para algunos aspectos deberían estar implementadas hasta el mes de septiembre de 2017. Es así como, este organismo de control en cualquier momento podría realizar auditorías y revisión in situ en las instituciones financieras controladas por la misma, a fin de verificar el cumplimiento íntegro de las disposiciones específicas contenidas en la normativa antes referenciada (SuperIntendencia de Bancos y Seguros, 2014)

El presente trabajo tiene como objetivo principal desarrollar un marco de referencia con las medidas de seguridad mínimas necesarias que deberían estar implementadas en el sistema de control interno de las instituciones financieras del país para dar cumplimiento normativo del ente de control. Adicionalmente, este marco servirá de guía para que la alta gerencia de las organizaciones apoye la implementación de tecnología y buenas prácticas adecuadas a fin de

proteger la información de sus clientes, su procesamiento, almacenamiento y disponibilidad a través de su infraestructura tecnológica como apoyo a los procesos de negocio, operaciones y estratégicos de la organización.

MARCO TEÓRICO

Gobierno Corporativo

Según Isaca (2015) el gobierno corporativo se define como el sistema por el cual se dirigen y controlas las corporaciones de negocios. Específicamente, es un conjunto de responsabilidades y prácticas usadas por la gerencia de una organización para proveer dirección estratégica para garantizar el cumplimiento de las metas deseadas.

Gobierno de Tecnología

De acuerdo a Cobit (2012) el gobierno de tecnología garantiza que las tecnologías de información y las relacionadas soportan y habilitan la estrategia de la empresa y la consecución de las metas corporativas. También incluye el gobierno funcional de TI, por ejemplo, garantizando que las capacidades de TI son provistas de forma eficiente y efectiva

Gobierno de Seguridad de la Información

Según ISO/IEC (2013) el gobierno de la información es responsabilidad de la alta dirección y deber ser parte integral y transparente del gobierno corporativo que provee dirección estratégica para las actividades de seguridad. Garantiza que el riesgo para la seguridad sea gestionado de manera apropiada y que los recursos de información se usen con responsabilidad.

Continuidad del Negocio

Según Nickolett y Schmidt (2008) en el nivel más básico, continuidad de negocio puede ser definido como un proceso interactivo que es diseñado para identificar los procesos de misión crítica del negocio y desarrollar políticas, planes y procedimientos para asegurar la continuidad de estos procesos en el caso de un evento imprevisto. Por otro lado, continuidad del negocio puede ser descrito como un conjunto de actividades técnicas y administrativas dirigido a seguir pasos para recuperar y restaurar procesos críticos de negocios después de un evento de desastre (Cremonini & Samarati, 2008).

Gestión de Riesgos

Isaca (2015) menciona que la gestión de riesgos es el proceso de identificar las vulnerabilidades y las amenazas para los recursos de información utilizados por una organización para lograr los objetivos de negocio.

La gestión de riesgos abarca identificar, analizar, evaluar, tratar, monitorear el impacto del riesgo sobre los procesos de TI.

Análisis de Impacto en el Negocio

Según Cybuski (2016) el Análisis de impacto en el negocio busca identificar y calificar las funciones y procesos empresariales sensibles al tiempo. Al medir estos procesos, las organizaciones están capacitadas para entender el momento en el que un impacto empieza a generar consecuencias negativas. Una vez entendidos estos impactos, la organización puede desarrollar el marco para aceptar, remediar o desarrollar estrategias de planificación para apoyar la recuperación organizacional. El siguiente paso en la fase de descubrimiento es la evaluación del riesgo.

Canales Electrónicos

Según SuperIntendencia de Bancos y Seguros (2014) los canales electrónicos son todas las maneras mediante las cuales los usuarios pueden realizar transacciones con las compañías del sistema financiero, a través de dispositivos electrónicos o tecnológicos, principalmente: los cajeros automáticos, dispositivos de puntos de venta, internet (comercio electrónico), banca electrónica.

Cajeros Automáticos

Según Isaca (2015) un cajero automático es un terminal diseñado para clientes de compañías financieras sin la necesidad de requerir la atención de personas. Estas terminales permiten ejecutar transacciones bancarias, depósitos financieros y retiros de efectivo con el uso de tarjetas de crédito; puesto que, transfiere información y dinero a través de canales de comunicación, este canal debe proveer niveles altos de seguridad lógica con una adecuada gestión de claves de encriptación. Además, GrgBanking (2011) menciona que existen una variedad de ataques a estos terminales, entre los que se encuentran el robo a la información de la tarjeta de crédito y ataque a la red y software instalado en el mismo, con la finalidad de controlar el retiro de los billetes del cajero automático.

Dispositivos de Puntos de Venta

De acuerdo a Isaca (2015) los dispositivos de punto de venta permiten capturar información en el lugar donde ocurren las transacciones de pago. Las transacciones más comunes que operan estos dispositivos son las tarjetas de crédito y débito asociadas a una cuenta financiera. Al estar en línea con una computadora central de una compañía financiera, lo más importante es determinar que cualquier información del cliente deberá ser encriptada utilizando técnicas de encriptación fuertes.

Comercio Electrónico

De acuerdo a Calvo (2009) el comercio electrónico se trata de la compra y venta de productos en línea, por medio del Internet. Básicamente, el sitio web publicita productos y servicios, el cliente llena un formulario con el producto que va a comprar y entrega información para la transacción de pago. Este proceso de compra depende de la existencia de niveles de confianza entre las dos partes, es decir, entre el comprador y el vendedor. Por tal motivo, se deberá demostrar las identidades respectivas antes de ejecutar a transacción para prevenir ataques de intermediarios (man in the middle). Luego, debe asegurarse que las partes de la transacción no puedan negar que la transacción se realizó, esto se lo conoce como autenticación y no repudio. Adicionalmente, según Isaca (2015) deberá implementarse una arquitectura de seguridad de encriptación, certificados digitales y gestión de claves.

Banca Electrónica

Como lo menciona la SuperIntendencia de Bancos y Seguros (2014) la banca electrónica son servicios otorgados a través sitio web de una compañía financiera, desde cualquier dispositivo tecnológico desde la que acceda. Así mismo, a través de la banca electrónica se realiza transferencias electrónicas de dinero presentado riesgos asociados al de reputación y seguridad de la información con amenazas al robo de datos confidenciales y restringidos.

Criptografía

De acuerdo a Amparo Sabater, Dolores Martínez, Luis Hernández, Fausto Montoya y Jaime Muñoz (2001) manifiestan que la criptografía se encarga de diseñar procedimientos para cifrar, es decir, enmascarar información de carácter restringida y confidencial. Luego, Randall K Nichols y Panos C Lekkas (2003) mencionan que la criptografía es la ciencia que permite mantener de manera secreta la información, a través de medios de autenticación a aquéllos que intervienen en las comunicaciones. Además, López (2010) indica que la criptografía es el uso de técnicas que se refieren a la protección de datos de individuos no autorizados a acceder a los mismos.

Ahora bien, según Marc Farley, Tom Stearns y Jeffrey Hsu (1997) indican que existe dos tipos de sistemas criptográficos: los que utilizan claves únicas o secretas (simétricos), y los que usan pares de claves complementarios (asimétricos), uno secreto y otro de conocimiento público.

Sistemas criptográficos con clave simétrica

De acuerdo a Madjid Nakhjiri y Mahsa Nakhjiri (2005) los sistemas criptográficos con clave simétrica se basan en algoritmos de encriptación simétricos, utilizando una misma clave secreta tanto para encriptar como desencriptar un texto plano. Cabe señalar que en este tipo de sistemas existen los siguientes algoritmos de encriptación fuertes y avanzados, enumerados a continuación: 1) Algoritmo AES, 2) Algoritmo Triple DES y 3) Blowfish (Stallings, 2005).

Aes

Según Christof Para y Jan Pelzl (2009) el algoritmo estándar avanzado de cifrado (AES) sustituyó al ya obsoleto estándar (DES) como algoritmo de encriptación para proteger información confidencial debido a que su clave puede ser vulnerada por la técnica de fuerza bruta, técnica que se limita a probar todas las posibles claves, una detrás de otra. Este algoritmo soporta claves desde 128 bits hasta 256 bits en tamaño.

Triple Des

De acuerdo a Amparo Sabater, Dolores Martínez, Luis Hernández, Fausto Montoya y Jaime Muñoz (2001) este algoritmo de encriptación de datos brinda un método sencillo de aumentar el tamaño de la clave de DES con tres distintas claves cuyo tamaño de longitud de clave es de 168 bits.

Blowfish

Según Schneier (2005) este algoritmo simétrico que utiliza un tamaño de clave desde 32 bits hasta 448 bits, desarrollado por Bruce Schneier se convierte en un algoritmo de encriptación fuerte frente a cualquier tipo de ataque.

Sistemas criptográficos con clave asimétrica

De acuerdo a Konheim (2007) los sistemas criptográficos con clave asimétrica también se les conoce como de clave pública, utilizan dos claves que funcionan juntas como un par, en general la clave de cifrado es conocida por el público, mientras que la de descifrado es conocida únicamente por el usuario. Los algoritmos de encriptación que este tipo de sistemas presenta son: 1) Algoritmo Diffie-Hellman, 2) Algoritmo RSA

Diffie Hellman

Este algoritmo se basa en el concepto de una pareja de claves pública y privada siendo utilizada en distintos protocolos de red y dispositivos de

seguridad telefónica (Randall K Nichols y Panos C Lekkas, 2003).

Además, según lo mencionado por William Cheswick, Steven Bellovin y Aviel Rubin (2003) este algoritmo puede emplear claves públicas y privadas a largo plazo teniendo la desventaja de que se generará la misma clave de mensaje entre los dos usuarios.

Rsa

Milanov (2009) indica que el algoritmo RSA implementa un criptosistema de clave pública tanto como una firma digital. Además, este algoritmo implementa dos importantes ideas: 1) La clave de encriptación es publica mientras que la de desencripción no, únicamente la persona con la correcta clave puede descifrar un mensaje encriptado. 2) Firma digital que utiliza una clave pública y que está destinada a verificar un destinatario, la integridad de los datos y la identidad del remitente. En adición, Kahate (2008) menciona que este algoritmo utiliza dos números primos muy largos formando una clave par, uno como clave privada y el otro como pública.

Pci dss

El estándar de seguridad de datos (Data Security Estándar, DSS) de la Industria de Tarjetas de Pago (PCI, Payment Card Industry) es la normativa que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos, con el propósito de reducir el riesgo de fraude con tarjetas de crédito (Council, 2016).

Cobit 5.0

Cobit 5.0 brinda un marco de trabajo integro que ayuda a las organizaciones a lograr sus objetivos basados en la gestión de Gobierno y de las TI corporativas, creando valores óptimos desde TI generando beneficios y optimizando el riesgo y uso de recursos (Cobit, 2012).

Iso 27002:2013

Estándar Internacional que proporciona un modelo para implementar, operar, monitorear, revisar un sistema de gestión de seguridad de la información, por sus siglas SGSI. Adicionalmente implementa y opera controles clave para manejar los riesgos de seguridad de la información (Iso/Iec, 2013).

Coso Erm

Estándar Internacional que brinda un proceso permanente realizado por la junta directiva, la gerencia y demás personal de la entidad basado en el establecimiento de estrategias para toda la empresa. Está diseñada para identificar eventos potenciales que puedan afectar a la entidad, y gerenciar los riesgos dentro del apetito de riesgo.

Iso 22301

Estándar Internacional que especifica requerimientos para establecer y gestionar un efectivo sistema de gestión de Continuidad del Negocio (SGCN). El estándar aplica el ciclo Plan – Do – Check – Act a la planeación, establecimiento, monitoreo y mejoramiento del SGCN de una organización (Normalización, 2012).

Cisa Isaca

Manual que contiene las definiciones, objetivos y conocimientos para una adecuada gestión de gobierno tecnológico, riesgos, seguridad de la información, continuidad de la información (Isaca, 2015).

Itil

Conjunto de “buenas prácticas” a gestión de la seguridad de la información, gestión de niveles de servicio, perspectiva de negocio, gestión de activos software y gestión de aplicaciones.

Estas buenas prácticas provienen de las mejores soluciones posibles que diversos expertos han puesto en marcha en sus organizaciones a la hora de entregar de servicios TI (Información, 2011).

Pmbok

La Guía de los fundamentos para la dirección de proyectos es un libro en el que se presentan estándares, pautas y normas para la gestión de proyectos. La Guía del PMBOK proporciona y promueve lineamientos para analizar, escribir y aplicar la dirección de proyectos (Institute, 2017).

METODOLOGÍA

El objetivo principal de este trabajo, es desarrollar un marco de referencia de buenas prácticas (medidas de seguridad en canales electrónicos) que sirva a las instituciones financieras dar cumplimiento a la normativa SB-JB-3066 emitida por la Superintendencia de Bancos, antes de la supervisión in situ que en cualquier momento el ente de control pueda realizar, para verificar el cumplimiento de dicha normativa y evitar cualquier tipo de sanción o multas en caso de incumplimientos a la misma.

Como método de elaboración de esta investigación , se revisaron normativas aceptadas para la práctica de gobierno tecnológico, gobierno de seguridad de la información, gestión de riesgos, continuidad del negocio identificando requerimientos mínimos que contribuyan incrementar el funcionamiento adecuado del sistema de control interno con la finalidad de garantizar que las transacciones realizadas por medio de los canales electrónicos cuenten con los controles, medidas y elementos de seguridad

necesarios para evitar el cometimiento de eventos fraudulentos. En adición, establecer las prácticas necesarias y adecuadas que den una certeza aceptable a las instituciones financieras para el cumplimiento de la normativa y antes de la visita en situ para verificar el cumplimiento por parte del ente de control.

Las buenas prácticas utilizadas para el desarrollo del marco de referencia son los siguientes:

- ✓ PCI DSS
- ✓ Cobit 5.0
- ✓ ISO 27002:2013
- ✓ COSO ERM
- ✓ ISO 22301
- ✓ CISA ISACA
- ✓ ITIL
- ✓ PMBOK

Cabe señalar que este marco de referencia se limitó a la investigación de las buenas prácticas antes descritas para el cumplimiento de los aspectos importantes registrados en la normativa, y para los siguientes canales electrónicos que la mayor parte de las instituciones financieras manejan como soporte a sus servicios, entre las cuales se detallan las siguientes: Cajeros Automáticos, Dispositivos de Puntos de Venta, Comercio Electrónico, Banca Electrónica, Banca móvil, Tarjetas de crédito.

Además, la revisión y desarrollo de las buenas prácticas se enmarcó en las siguientes secciones de la normativa SB-JB-3066 detalladas a continuación y en distintos componentes relacionados con la tecnología de la información (Ver figura 1 Componentes tecnológicos):

- ✓ Sección 4.3 Tecnología de la información
- ✓ Sección 4.3.5 Medidas de seguridad en canales electrónicos
- ✓ Sección 4.3.6. Cajeros automáticos
- ✓ Sección 4.3.7. Puntos de venta (POS y PIN Pad)
- ✓ Sección 4.3.8. Banca electrónica
- ✓ Sección 4.3.9. Banca móvil
- ✓ Sección 4.3.10. Sistemas de audio respuestas (IVR)
- ✓ Sección IV Continuidad del negocio
- ✓ SecciónV Responsabilidades en la administración del riesgo operativo
- ✓ Sección VI Servicios provistos por terceros
- ✓ Sección VII Seguridad de la información

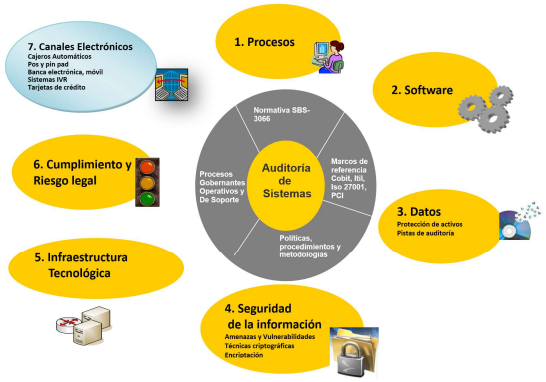

Figura 1 Componentes tecnológicos

Elaborado por: Juan Gualsaquí

Una vez desarrollado el marco de referencia para cada una de las secciones de la normativa, se realizó su medición en una institución bancaria del país sujeta al control y evaluación de la Superintendencia de Bancos. Esta institución deberá concentrarse en implementar los requerimientos mínimos necesarios en los puntos que en su evaluación no cumplan con lo requerido en la normativa emitida por este ente de control y en relación con la aplicación del marco de referencia realizado.

Este cumplimiento garantizará que la información sea confiable, integra, disponible y evitará cualquier tipo de sanción o multas en caso de incumplimientos a la misma.

Para la evaluación se utilizó herramientas conocidas como checklist que contienen cada uno de los puntos de la normativa 3066 identificándose los requerimientos mínimos necesarios que debe poseer la institución bancaria para el cumplimiento de la normativa. Es importante mencionar que para la evaluación de cada uno de los puntos de la normativa se consideraron los siguientes estados de cumplimiento (Ver Tabla 1: Nivel de Cumplimiento Evaluación Normativa 3066):

1. Cumplimiento Efectivo: Los procesos y/o requerimientos mínimos relacionados con el punto cumplen en su totalidad con lo requerido con la norma.

2. Cumplimiento Parcial: Los procesos y/o requerimientos mínimos relacionados con el punto cumplen de manera parcial con lo requerido con la norma.

3. Incumplimiento: Los procesos y/o requerimientos mínimos relacionados con el punto no cumplen con lo requerido con la norma.

4. Cumplimiento no aplica: Los procesos y/o requerimientos mínimos relacionados con el punto no son aplicables para evaluación de lo requerido con la norma.

Posteriormente, aplicando la revisión punto por punto registrado en el checklist se realizaron

indagaciones in situ con el personal encargado de validar cualquier pregunta respecto a la evaluación, entre los cuales detallamos a continuación los principales:

Personal del área de Tecnología, Personal del área de Riesgos, Oficial de Seguridad de la Información, Especialistas de Continuidad de Negocio

Finalmente, como sustento de la evaluación nos basamos en la evidencia documental (entregada por el personal clave de manera física o enviado vía correo electrónico) y por lo mencionado por el personal de las áreas antes referidas. Cabe señalar que el formato utilizado del checklist utilizado para la determinación de los estados de cumplimiento de la normativa 3066 se encuentra en la sección Anexos "Anexo 1 Formato de Checklist" en este documento.

Para el desarrollo de este trabajo, hemos seleccionada a la institución bancaria cuyo nombre la llamaremos "Banco", empresa líder en ofrecer una amplia gama de servicios financieros como financiamiento, inversiones, seguros, y tarjetas de crédito, medio de pago que facilita las transacciones de los tarjetahabientes, reemplazando el uso de efectivo y generando una alternativa de pago fácil y segura.

Actualmente, la organización crece en número de usuarios, servicios y recursos, lo que hace indispensable disponer de proyectos y soluciones tecnológicas innovadoras que den soporte y cubran la demanda de sus clientes. El Banco, fundamenta y apoya a la innovación y protección de la tecnología de la información, componente indispensable para el logro de los objetivos organizacionales.

Además, al ser una entidad financiera regulada por entidades locales e internacionales, se ve en la obligación de cumplir con normativas para gestionar la seguridad de la información tales como: El estándar de seguridad de datos de la Industria de Tarjetas de Pago PCI DSS, la normativa de Canales Electrónicos de la Superintendencia de Bancos SBS-JB-3066, el Estándar Internacional Norma ISO 27001, entre otros.

Así mismo, concentra su mayor esfuerzo en proteger la información de las tarjetas habientes, información que se procesa, almacena y distribuye a través de su infraestructura tecnológica como apoyo a los procesos de negocio, operaciones y estratégicos de la organización.

Para el soporte y demanda de sus servicios posee los siguientes activos de información en donde se detalla de manera general su infraestructura tecnológica (Ver figura 2 Activos de Información):

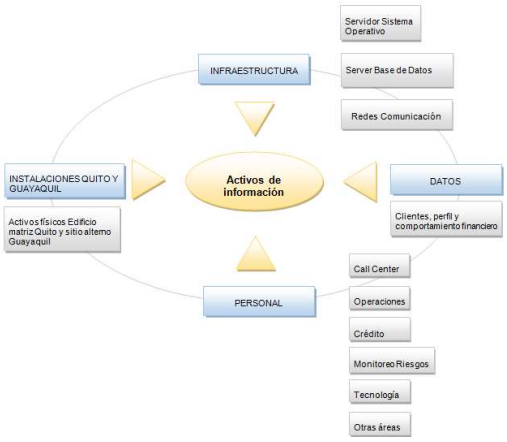

Figura 2: Activos de Información

Elaborado por: Juan Gualsaquí

Los principales canales electrónicos de la entidad son la banca electrónica, dispositivos móviles, comercio electrónico. Se encuentra en proyecto de implementación la respuesta de voz interactiva (IVR) para la atención a clientes. Además, tecnología POS y cajeros automáticos es de total administración de proveedores de servicios externos para la interacción con la tarjeta de crédito. Por tal razón estás tecnologías no son parte de la evaluación al Banco para el cumplimiento de la normativa. Sin embargo, en el marco de referencia se especifican los requerimientos mínimos que se necesitan para el cumplimiento en caso de disponer de este tipo de tecnologías.

ANÁLISIS

Como método que permita determinar el nivel de cumplimiento de la institución bancaria seleccionada, para cada uno de los puntos definimos tal como lo describimos en la sección metodología de este documento cuatro niveles de cumplimiento, siendo el nivel llamado Cumplimiento Efectivo y nivel Cumplimiento Parcial los aceptados por la gerencia para tener una certeza razonable de que se cumple con lo estipulado por la normativa 3066 (Ver Tabla 1):

NIVELES DE CUMPLIMIENTO EVALUACIÓN NORMATIVA 3066

Nivel Cumplimiento (Observado)		Nivel mínimo aceptable (NMA)
Nivel 1	Cumplimiento Efectivo: Los procesos y/o requerimientos mínimos relacionados con el punto cumplen en su totalidad con lo requerido con la norma.	
Nivel 2	Cumplimiento Parcial: Los procesos y/o requerimientos mínimos relacionados con el punto cumplen de manera parcial con lo requerido con la norma. Se requerirá de implementación de requerimientos adicionales para el cumplimiento total	
Nivel 3	Incumplimiento: Los procesos y/o requerimientos mínimos relacionados con el punto no cumplen con lo requerido con la norma.	NO
Nivel 4	Cumplimiento no aplica: Los procesos y/o requerimientos mínimos relacionados con el punto no son aplicables para evaluación de lo requerido con la norma.	N/A

Tabla 1: Nivel de Cumplimiento Evaluación Normativa 3066

Elaborado por: Juan Gualsaquí

Los resultados de los niveles de cumplimiento observado en la institución financiera para los puntos de la normativa SB-JB-3066 fueron los siguientes:

NIVELES DE CUMPLIMIENTO EVALUACIÓN ENTIDAD BANCARIA	*% PORCENTAJE DE CUMPLIMIENTO*
Nivel 1: Cumplimiento Efectivo: Los procesos y/o requerimientos mínimos relacionados con el punto cumplen en su totalidad con lo requerido con la norma.	***86.5% (116 puntos)***
Nivel 2: Cumplimiento Parcial: Los procesos y/o requerimientos mínimos relacionados con el punto cumplen de manera parcial con lo requerido con la norma. Se requerirá de implementación de requerimientos adicionales para el cumplimiento total	**4.5% (6 puntos)**
Nivel 3: Incumplimiento: Los procesos y/o requerimientos mínimos relacionados con el punto no cumplen con lo requerido con la norma.	**0**
Nivel 4: Cumplimiento no aplica: Los procesos y/o requerimientos mínimos relacionados con el punto no son aplicables para evaluación de lo requerido con la norma.	***8.95% (12 puntos)***

Con base en la evaluación de los niveles de cumplimiento observados exponemos a continuación los siguientes análisis:

De manera general los procesos y/o requerimientos mínimos relacionados con los puntos cumplen en su totalidad con lo requerido con la norma, es decir se encuentran en el nivel 1 'Cumplimiento Efectivo" alcanzando un 86.5% del total de puntos evaluados. El 4.5% de puntos se encuentran en cumplimiento Parcial, es decir que los procesos y/o requerimientos mínimos relacionados con el punto cumplen de manera parcial con lo requerido con la norma por lo que se requiere la implementación de requerimientos adicionales para el cumplimiento total. Estos puntos se refieren a los siguientes aspectos:

- ✓ no pudimos obtener evidencia de que se hagan pruebas periódicas de restauración de las cintas de respaldo con la finalidad de verificar recuperaciones exitosas de información.
- ✓ el personal de TI ha sido capacitado en la guía OWASP para técnicas de desarrollo seguro. Sin embargo, no se evidencia el escaneo de vulnerabilidades en código fuente de manera periódica con la finalidad de identificar riesgo en las aplicaciones en desarrollo y puestas en producción.
- ✓ No existe el monitoreo que incluye límites y alertas para base de datos.
- ✓ Si bien los procesos de envío del PAN (número de cuenta principal) se encuentran protegidos mediante criptografía sólida, no todo el 100% de envíos de números de tarjeta se lo efectúa de forma enmascarada.
- ✓ Se dispone de un área de call center la cual con su personal atiende las llamadas de los clientes las 24 horas. Actualmente el Banco tiene pensado la implementación de sistemas de audio respuestas, pero no ha se ha definido lineamientos o decisiones al respecto

Además, el 8.95% de puntos tienen un Nivel 4, es decir los procesos y/o requerimientos mínimos relacionados con el punto no son aplicables para evaluación de lo requerido con la norma. Este porcentaje se refiere a que el Banco no dispone y/o administra tecnología de cajeros automáticos, POS, Pin Pad y sistemas IVR como parte de su infraestructura tecnológica.

En lo que respecto a cajeros automáticos y tecnología POS es recomendable que la organización efectué un seguimiento a los proveedores de servicio administradores de este servicio, para determinar si estos cumplen con los aspectos relacionados en la normativa (SuperIntendencia de Bancos y Seguros, 2014).

Finalmente, es importante mencionar que luego de la evaluación ningún punto se encuentra en un nivel 3 o de "Incumplimiento" es decir que, si el ente de control realizará una revisión de la norma, la institución mantiene su sistema de control interno funcionando razonablemente en relación a lo requerido por la norma. Es importante indicar que el detalle de la evaluación para cada uno de los puntos de la norma 3066 se encuentra detallado en el Anexo 2 Checklist de evaluación.

CONCLUSIONES

Para el desarrollo del marco de referencia para el cumplimiento de la normativa SBS-JB-3066 se utilizaron las siguientes normativas internacionales: ISO 27002:2013, ISO 22301, COBIT 5.0, PCI DSS, COSO ERM, PMBOK, CISA, ITIL. A través de este marco se aplicaron sus lineamientos y guías de buenas prácticas en una entidad bancaria del país concluyendo que su sistema de control interno contiene y cumple razonablemente con los requerimientos mínimos relacionados con lo requerido con la norma 3066 de la Superintendencia de Bancos.

Es decir, ante una revisión in situ por parte del ente de control, la entidad pasaría la revisión sin que se presenten observaciones a considerar.

Por otra parte, se recomienda que el Banco implemente procedimientos de restauración de respaldos y posteriormente monitoree la ejecución de pruebas periódicas de restauración de cintas de respaldo.

Así mismo, implemente una herramienta o solución de escaneo de vulnerabilidades en el código fuente de los desarrollos tanto en las etapas de producción, pruebas y desarrollo.

También implementar herramientas para el monitoreo y emisión de alertas respecto a la modificación en la configuración de bases de datos.

Se recomienda analizar el costo beneficio de implementar un proyecto de enmascaramiento total del número de tarjetas y definir lineamientos respecto a la implementación de sistemas de audio respuesta

Con base en estas implementaciones estos aspectos alcanzarán un nivel 1 de cumplimiento efectivo y de esta manera se evitaría cualquier incumplimiento u observación por parte del ente de control.

Cabe señalar que ciertos puntos no se aplicaron para evaluación del Banco al no administrar tecnología como cajeros automáticos, POS, Pin Pad y sistemas IVR. Sin embargo, se recomienda que la entidad realice el seguimiento de lo requerido por la norma a los proveedores de servicio que administran este tipo de tecnologías y siguiendo con lo establecido en el marco de referencia desarrollado.

Otro aspecto a mencionar es que el guión o checklist desarrollado facilitó el trabajo de campo de evaluación en la entidad financiera, principalmente en las indagaciones que realizamos con el personal clave en solventar cada una de las inquietudes.

Así también, este marco de referencia servirá de guía para que la alta gerencia de las instituciones bajo normativa de la Superintendencia de Bancos se apoye y apliquen un diagnóstico actual a su gobierno tecnológico, continuidad del negocio, seguridad en canales electrónicos, administración de riesgo operativo y seguridad de la información.

De esta manera, se tendrá una evidencia razonable de cuales serían las debilidades que tendrían de cumplimiento y por otra parte desarrollar planes de acción para remediar los procesos que no cumplan totalmente con lo requerido por la norma.

Cabe indicar que como limitaciones para esta evaluación fue el tiempo de atención por parte del personal clave de la empresa ya que debían atender las necesidades y actividades propias de su gestión diaria en la institución bancaria.

Además, por ser una institución bancaria no tuvimos acceso de manera íntegra o en su totalidad a la información proporcionada por temas de confidencialidad de la información. Incluso no podemos mencionar el nombre de la institución por temas de sigilo bancario. Sin embargo, las evidencias obtenidas reflejan y sirven de manera adecuada para el sustento de la evaluación de cumplimiento de los distintos puntos de la norma.

Finalmente, como trabajo futuro, se recomienda realizar esta evaluación de cumplimiento a empresas que faciliten evidencia o soporte documental que sustenten el trabajo realizado.

Bibliography

Amparo Sabater, Dolores Martínez, Luis Hernández, Fausto Montoya y Jaime Muñoz (2001). *Técnicas criptográficas de protección de datos -Segunda edición.* Madrid: Alfaomega Grupo Editor.

Calvo (2009). *Principios de seguridad en el comercio electrónico.* México Distrito Federal: Alfaomega.

Christof Paar y Jan Pelzl (2009). *Understanding Cryptpgraphy.* Bochum - Germany: Springer.

Cobit (2012). Cobit 5 Framework. Rolling Meadows, Estados Unidos.

Council (2016). Norma de Seguridad de datos PCI DSS.

Cremonini y Samarati (2008). Business Continuity Planning. *Handbook of Computer Networks: Distributed Networks*, 671-688.

Cybuski (2016). Business Continuity Management: Return on Investment. Aon Global Risk Consulting.

Deloitte Touche (2011). El futuro de la banca móvil en América Latina. Mexico. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/py/Documents/about-deloitte/Futuro_banca_movil2012.pdf

Fanjul Suárez y Valdunciel Bustos (2008). Impacto de las nuevas tecnologías en el negocio bancario español. España.

GrgBanking (2011). Best Practice for ATM Security -GRGBanking. Guagzhou, China.

Información (2011). ITIL.

Institute (2017). Guía de los Fundamentos de la Dirección de Proyectos (Guía del PMBOK®. EEUU.

Isaca (2015). Manual de Preparación al Examen Cisa 2015. Rolling Meadows, Ilinois.

Iso/Iec (2013). 27002:2013 International Standard Information Technology - Code of practice for information security controls.

Kahate (2008). *Cryptography and Network Security.*

Konheim (2007). *Computer Security and Cryptography.*

López (2010). *Criptografía y Seguridad en Computadores.* Jaén, Andalucía.

Madjid Nakhjiri y Mahsa Nakhjiri (2005). *AAA and Network Security for Mobile Access.* Chichester, England: Wiley.

Marc Farley, Tom Stearns y Jeffrey Hsu (1997). *Guía Lan Times de Seguridad e Integridad de Datos.* Mc Graw Hill.

Milanov (2009). Obtenido de https://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf

Navarro (2017). *El año de la transformación digital*.

Nickolett y Schmidt (2008). Business Continuity Planning description and framework. *Comprehenive Solutions*.

Normalización (2012). ISO 22301:2012 Sistemas de Continuidad del Negocio.

Organización de Estados Americanos (2018). *Critical Infraestructure Protection in Latin America and the Caribbean.* Washington D.C.

PriceWaterhouseCoopers (2016). *Encuesta Global de Seguridad de la Información.* Cordoba, Argentina.

Radware (2017). *Global Application & Network Security Report 2016-2017.*

Randall K Nichols y Panos C Lekkas (2003). *Seguridad para comunicaciones inalámbricas.* México Distrito Federal: Mc Graw Hill.

Schneier (2005). *Schneier on Security*. Obtenido de https://www.schneier.com/academic/blowfish/

Stallings, W. (2005). *Cryptography and Network Security.* Pearson Prentice Hall.

SuperIntendencia de Bancos y Seguros (2014). *Superintendencia de Bancos - Libro I Normas Generales para las Instituciones del Sistema Financiero - Título X De la Gestión y Administración de Riesgos.* Obtenido de sitio web de SBS: http://www.sbs.gob.ec:7778/practg/p_index

The IIA Research Foundation (2011). *What´s Next for Internal Auditing.* The IIA Research Foundation.

William Cheswick, Steven Bellovin y Aviel Rubin (2003). *Firewalls and Internet Security, Second Edition.* Boston: Addison Wesley.