Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Escuela Académica Profesional de Ingeniería de Sistemas

Alineamiento de Marco COBIT y Normas PCI para aplicarse al proceso de tarjeta de crédito en una entidad financiera

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Jessica Vallejos FUENTES RIVERA

ASESOR

Jorge Santiago PANTOJA COLLANTES

Lima, Perú

2010

Referencia bibliográfica

Fuentes, J. (2010). *Alineamiento de Marco COBIT y Normas PCI para aplicarse al proceso de tarjeta de crédito en una entidad financiera.* Tesina para optar el título profesional de Ingeniero de Sistemas. Escuela Académica Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Dedico el presente trabajo a mi mamá, por ser mi inspiración.

AGRADECIMIENTOS

Al profesor Jorge Pantoja, por su orientación y dedicación para que este trabajo cumpla con los objetivos trazados.

Al profesor Jose Antonio Pérez Quintanilla, por la enseñanza metodológica del curso Auditoria de Sistemas, para la elaboración de este trabajo.

Al equipo de Auditoria de Sistema y Tecnología del Banco en el cual laboro, por la formación profesional y oportunidades brindadas.

A la Facultad de Ingeniería de Sistemas – UNMSM, por la formación académica brindada durante los años de estudios.

A Dios.

Alineamiento de Marco COBIT y Normas PCI para aplicarse al proceso Tarjeta de Crédito en una Entidad Financiera

RESUMEN

El proceso de tarjeta de crédito reúne una serie de debilidades correspondientes a la seguridad de la información, las entidades financieras no son ajenas a diferentes tipos de ataques, entre ellos incluidos el fraude interno, el cual afecta a la imagen del negocio.

Este trabajo busca alinear los requisitos normados por la industria de tarjeta de pago (PCI) con el marco conceptual COBIT, con el propósito de optimizar los procesos de tarjeta de crédito obteniendo una matriz de asignación de responsabilidades, un modelo de madurez y una gestión de prevención de los riesgos del fraude y así mantener la información que la empresa necesita para lograr sus objetivos.

Palabras Claves: Información, seguridad, tarjeta, negocio, organización, fraude

Aligning COBIT Framework and PCI standards to apply to process credit card at a Financial Institution

ABSTRACT

The credit card processing has a number of weaknesses related to information security, financial institutions are not immune to different types of attacks, including including internal fraud, which affects the image of the business.

This paper seeks to align the requirements regulated by the Payment Card Industry (PCI) with the COBIT framework, in order to optimize the process of obtaining a credit card a matrix of accountability, a model of maturity and management preventing the risks of fraud and so maintain the information the company needs to achieve its objectives.

Keywords: Information security, card, business, organization, fraud

ÍNDICE

Lista de figuras

Lista de tablas

Capítulo 1: Introducción

Hasta ahora, el proceso de seguridad de la información de las tarjetas de crédito en las entidades financieras no se encuentra completamente formalizado, puesto que se evidencia casos de fuga de información para llevar a cabo el fraude interno y externo lo que conlleva a poner en riesgo la credibilidad e imagen de las entidades financieras.

Las marcas más importantes de tarjeta de crédito crearon una serie de requisitos para aquellos comerciantes o proveedores que realizan transacciones o almacenan información de los tarjetahabientes, debido a ellos se regularizaron algunos temas de seguridad. Sin embargo, cada marca tenía requisitos diferentes una de las otras lo que dificulta implementar estos procedimientos en los negocios antes mencionados por la diversidad y compromiso con cada una de las marcas.

Gracias a la industria de tarjeta de pago, se creó la norma para la seguridad de los datos de los tarjetahabientes la cual reúne los requisitos consensuados de las cinco marcas más importantes de tarjeta de crédito, la seguridad electrónica esta normada pero poder conducirla para beneficio del negocio y evitar multas de dicha industria se deben tomar en cuenta una gestión optima de tecnología de información en la entidad financiera como proveedor de las marcas.

De otro lado, la existencia de un marco teórico para tecnologías de información con el respaldo de las principales normas técnicas internacionales, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en TI que son necesarias para alinear TI con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización.

Para reforzar el proceso de tarjeta de crédito, se ha estimado el alineamiento de los requisitos de la industria de tarjeta de pago con el marco teórico de tecnología de información para obtener las mejoras antes mencionadas para el negocio bancario.

1.1 Antecedentes

Quienes intervienen en una Transacción con Tarjeta

Comercio: cualquier negocio que cumple con los estándares de calificación de una marca de pago, y que se encuentra aprobado por cualquier adquiriente. El negocio acepta tarjetas de pago a cambio de algún bien o servicio. Ejem. Supermercados, estaciones de servicio.

Adquiriente: Miembro de una marca de pago que mantiene relaciones y cuentas para los comercios que aceptan tarjeta de pago. Sirve como un intermediario entre los comercios y las marcas. Ejemplo: banco x que mantiene la cuenta del supermercado Y, acepta todas las tarjetas de crédito de todos los bancos.

Proveedor de Servicio: Negocio que no es miembro de una marca de pago o comercio que se encuentra directamente relacionado al procesamiento, almacenamiento, transmisión, e intercambio de información de la transacción o del tarjetahabiente.

Incluye a las organización que proveen servicios a los comercios, organizaciones que controlan o pueden impactar en la seguridad de la información del tarjetahabiente (ej. proveedores de administración de firewalls, IDS, etc.).

Marca: organización de procesamiento que licencia a los miembros y comercios la emisión y aceptación de tarjetas de crédito respectivamente. La organización es un intermediario entre los adquirientes y emisores.

Emisor: Institución financiera (miembro licenciado de una marca de pago) que mantiene contratos y emisiones de tarjetas con los tarjetahabientes. Es la responsable de la administración de las cuentas de los tarjetahabientes y aprobar las solicitudes de autorización.

Ejemplo: banco x que emite la tarjeta VISA, AMEX, MC, etc.

Proceso de una transacción

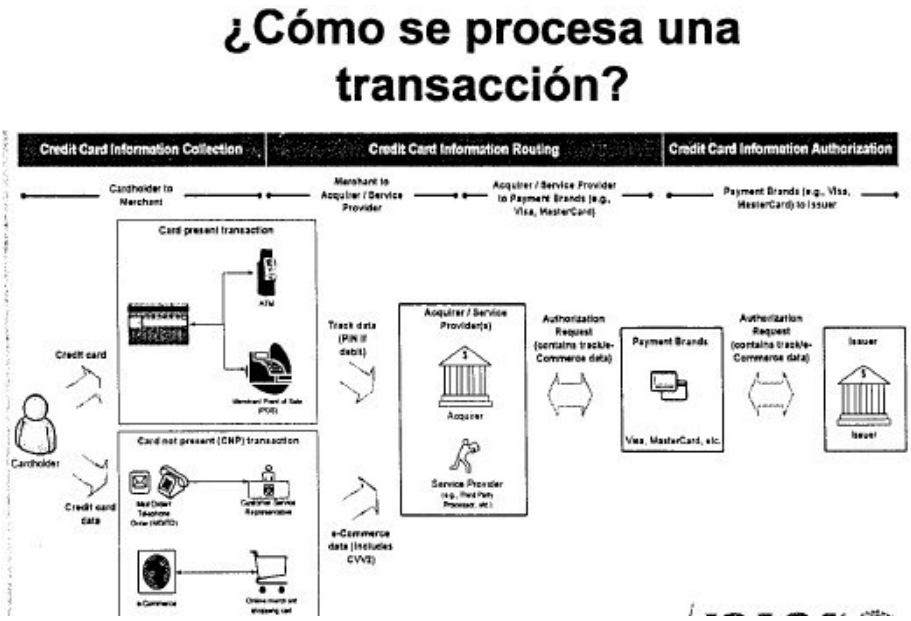


Figura 1: Proceso de una Trx

Localización de Información

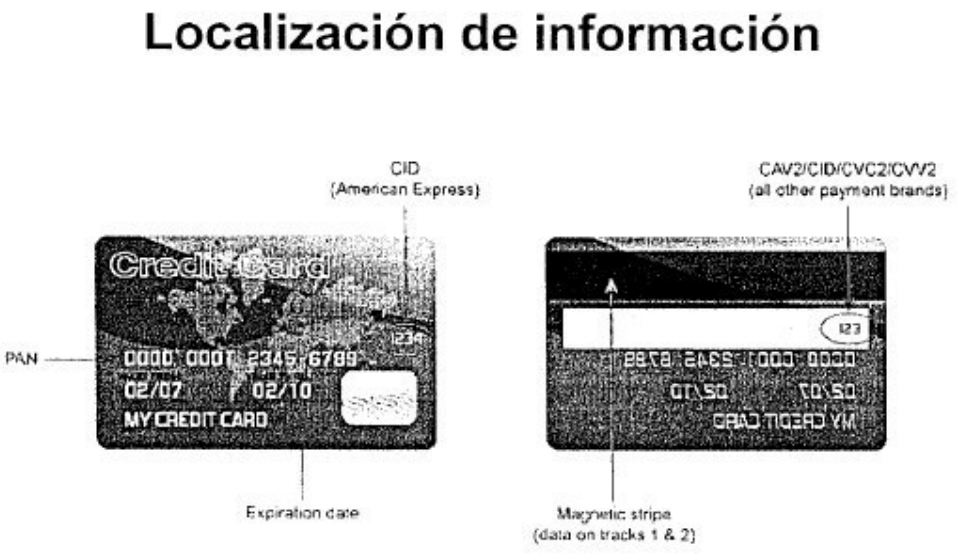


Figura 2: Localización de información en Tarjeta

Información almacenada en la tarjeta

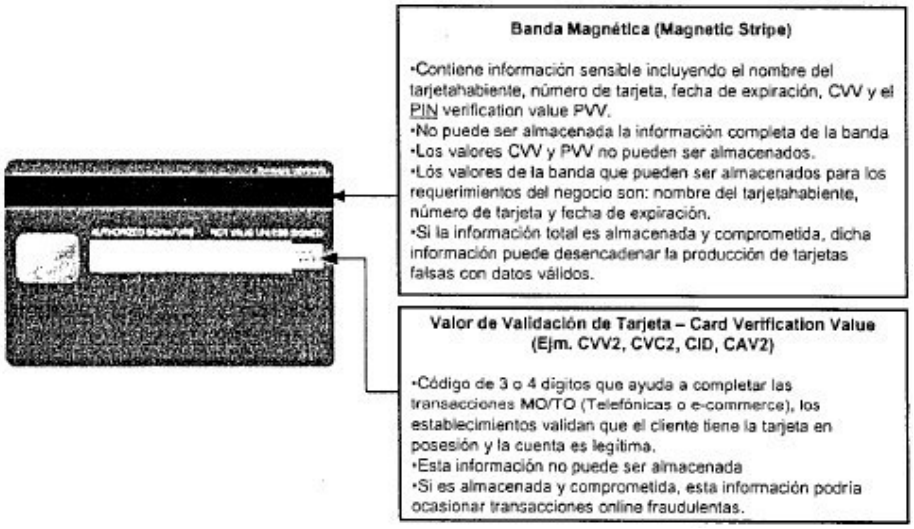


Figura 3: Reverso de Tarjeta

Información sobre la aplicabilidad de las DSS de la PCI

La siguiente tabla ilustra los elementos de los datos de titulares de tarjetas y los datos confidenciales de autenticación que habitualmente se utilizan; independientemente de que esté permitido o prohibido el almacenamiento de dichos datos o de que esos datos deban estar protegidos. Esta tabla no es exhaustiva, sino que tiene por objeto ilustrar distintos tipos de requisitos que se le aplican a cada elemento de datos.

Tabla 1: Datos de Tarjeta

	Elemento de datos	Almacenamiento permitido	Protección requerida	PCI DSS req. 3.4
Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí	Sí	Sí
	Nombre del titular de la tarjeta [1]	Sí	Sí [1]	No
	Código de servicio [1]	Sí	Sí [1]	No
	Fecha de vencimiento [1]	Sí	Sí [1]	No
Datos confidenciales de autenticación [2]	Datos completos de la banda magnética [3]	No	N/C	N/C
	CAV2/CVC2/CVV2/CID	No	N/C	N/C
	PIN/Bloqueo de PIN	No	N/C	N/C

1 Estos elementos de datos deben quedar protegidos si se los almacena con el PAN. Esta protección debe brindarse por cada requisito de las DSS de la PCI, a fin de asegurar una protección integral del entorno de los datos del titular de la tarjeta. Además, es posible que otras leyes (por ejemplo, las leyes relacionadas con la protección, la privacidad, el robo de identidad o la seguridad de los datos personales del consumidor) exijan protección específica de esos datos o la debida divulgación de las prácticas de una empresa en caso de que se recopilen datos personales sobre el consumidor durante el transcurso de los negocios.

Sin embargo, las DSS de la PCI no rigen si no se almacenan, procesan ni transmiten los PAN.

2 No se deben almacenar los datos confidenciales de autenticación después de la autorización (incluso si están cifrados).

3 Contenido completo de la pista de banda magnética, imagen de la banda magnética que está en el chip o en cualquier otro dispositivo.

PCI

PCI DSS, en su idioma nativo (Inglés): *Payment Card Industry Data Security Standard*, significa Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.

Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (*Payment Card Industry Security Standards Council*) como una guía que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago débito y crédito.

Las compañías que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o arriesgan la pérdida de sus permisos para procesar las tarjetas de crédito y débito (Perdida de franquicias), enfrentar auditorías rigurosas o pagos de multas[1] Los Comerciantes y proveedores de servicios de tarjetas de crédito y débito, deben validar su cumplimiento al estándar en forma periódica.

Figura 4: Estándar PCI

Cumplimiento PCI

Al ser PCI DSS un estándar de la industria, las marcas de pago, y no el PCI Security Standard Council, son responsables de la aceptación o negación de las recomendaciones de cumplimiento de los Qualified Security Assessors (QSAs) y Approved Scanning Vendors (ASVs).

Para ser considerado como PCI Compliant, la entidad debe cumplir con todos los requerimientos del PCI DSS (directamente o a través de los controles compensatorios)

Los requerimientos de validación de cumplimiento varían dependiendo del programa de la marca de pago y del nivel del proveedor de servicios o comercio (nivel 1 a 4) – cantidad de transacciones.

El nivel de asignación PCI se basa en el número de transacciones anuales que procesa el comercio o proveedor de servicios. Sin embargo, cualquier comercio que presente una brecha de seguridad que comprometa la información de los tarjetahabientes, o que sea considerado de nivel 1 por alguna de las marcas de pago, es automáticamente considerado de nivel 1 por todas las marcas de pago.

Contratación de Qualified Security Assessors (QSAs) y Approved Scanning Vendors (ASVs)

Figura 5: Requerimientos

1.2 Definición del Problema

Existen razones para almacenar los datos de los tarjetahabientes, como el perfilamiento de clientes, análisis y pronósticos de compras, para la identificación y seguimiento a los clientes, realizar un análisis de fraudes, intercambiar información con socios de negocio, otra razón también seria no tener una razón aparente solo en caso que se necesiten en el futuro.

Sin embargo, este procedimiento puede generar brechas de seguridad y un compromiso de información por inadecuado almacenamiento de información/ datos, porque no existen procedimientos documentados ni divulgados, aplicaciones inseguras, inadecuada segmentación entre redes, no existe una estrategia de almacenamiento y revisión de logs (trazabilidad), contraseñas por defecto en los equipos.

Como consecuencia, se visiona una exposición de información sensible lo que conlleva a la pérdida de confianza de los clientes de la entidad financiera, perdida de socios de negocio, despido de personal, multas por no cumplimiento con PCI u otras regulaciones, gastos por investigadores forenses, mayores costos para cumplimiento con PCI (requerimientos más complejos), fin de relación comercial con marcas de pago, costo de re-emision de nuevas tarjetas, perdidas por fraude

Figura 6: Costos de no cumplir PCI

1.3 Objetivos

1.3.1 General

Establecer el alineamiento para el cumplimiento de la norma PCI a una entidad financiera utilizando como marco de referencia COBIT para optimizar la seguridad de TI con respecto al servicio tarjeta de crédito.

1.3.2 Específicos

- Mantener el proceso para seguridad de la información enfocando los requisitos de la Norma PCI en el marco COBIT.

- Estructurar procedimientos y matriz de asignación de responsabilidades para la aplicación de la norma PCI en el servicio tarjeta de crédito.
- Establecer Metas y Métricas del proceso tarjeta de crédito para cada requisito de la norma PCI.
- Establecer un Método para la evaluación de los riesgos para el proceso de Tarjeta de Crédito.

1.4 Justificación

Debido al aumento del compromiso de información de tarjetas de crédito a nivel mundial, las cinco principales tarjetas de crédito (VISA, Master Card, American Express, JCB y Discover) han conformado el concilio PCI y éste creo la norma PCI DSS. PCI Data Security Standard es un estándar de seguridad que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el tratamiento, procesado o almacenamiento de información de tarjetas de crédito.

Su finalidad es la reducción del fraude relacionado con las tarjetas de crédito e incrementar la seguridad de estos datos, los principales fraudes reconocidos son:

Fraude en los Cajeros Automáticos.

- El ladrón consigue ver el número que usted teclea. Lo utiliza posteriormente, robándole la tarjeta.
- **Manipulación del cajero** mediante dispositivos en la ranura de la maquina y una cámara oculta. Al introducir la tarjeta se graban los datos de la tarjeta y al marcar los números se quedan grabados.
- **Bloqueo de la tarjeta en el cajero**. Un extraño le dice que vuelva a introducir el número. Este lo memoriza y lo utiliza después con la tarjeta todavía bloqueada.

Fraude por teléfono

- Cuando recibe alguna llamada ofreciéndole algo, y **le piden su información de su tarjeta.**
- Pueden hacerse pasar por la entidad emisora de la tarjeta y solicitar algunos datos de confirmación.
- De otra entidad, ofreciéndole una oferta, para lo cual necesitan trasnferir los fondos a la nueva tarjeta.
- Decirle que ha ganado un premio y necesita sus datos para cobrarle los gastos de envío.

Fraude por Clonación

La clonación se produce mediante el **copiado de la banda magnética con el fin de hacer una copia ilegal** de una tarjeta de crédito.

Se usan máquinas pequeñas llamadas “skimmers" para leer la información de las bandas magnéticas.

Fraude por internet

Fraude con tarjeta de crédito a través de internet. Fraude con tarjeta de crédito vía correo electrónico. Todos lo relacionado con tarjeta de crédito internet

La importancia de este trabajo radica en que, utilizando el alineamiento del marco COBIT con la Norma PCI se generen procedimientos para el servicio de tarjeta de crédito de una entidad financiera, puesto que este producto está enteramente relacionado al área de TI el cual es el responsable de la seguridad de la información.

De esta manera se aplicaran los controles necesarios y orientados al negocio.

1.5 Propuesta

Para alcanzar a desarrollar la propuesta de solución, se ha realizado una investigación sobre los principales procesos automáticos y/o manuales de las transacciones bancarias de Tarjeta de Crédito. Esto servirá de base para determinar los parámetros relevantes para realizar el alineamiento.

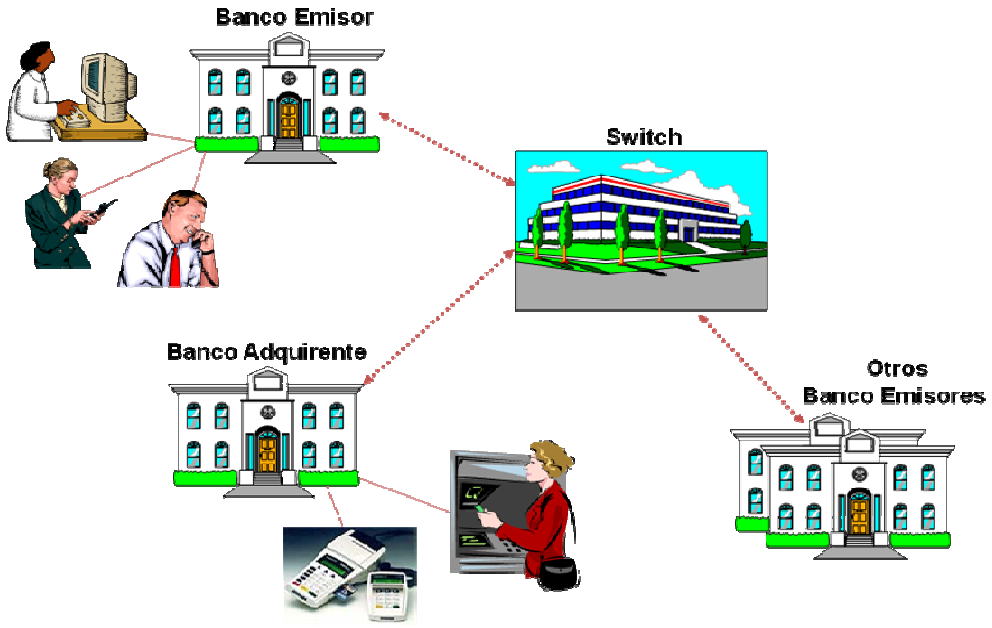


Figura 7: Proceso de Trx con Tarjeta

Así mismo se investigó sobre los parámetros de seguridad de información considerados por las marcas de pago y la norma PCI

De otro lado, se realizó el estudio sobre el marco COBIT porque contribuye a establecer un vínculo con los requerimientos del negocio, a organizar las actividades de TI en un modelo de procesos generalmente aceptado, a identificar los principales recursos de TI a ser utilizados y definir los objetivos de control gerenciales a ser considerados.

Con esta información se desarrollarán los controles para la administración del producto tarjeta de crédito.

1.6 Organización de la Tesina

Para presentar el presente trabajo de manera entendible, se ha dividido en capítulos. En el capítulo 2 se presenta el Marco Teórico, dividido en Definiciones Teóricas y Marco Conceptual. En el capítulo 3 se presenta el Estado del Arte de la norma PCI alineada al Marco teórico COBIT. En el capítulo 4 capítulo Aplicación para identificar riesgos, gestionar recursos y el nivel de madurez de los procesos

de tarjeta de crédito en la organización. En el capítulo 5 se encuentran las conclusiones y trabajos futuros; en el capítulo 6, el glosario de términos y finalmente, en el capítulo 7, las referencias bibliográficas.

Capítulo 2: Marco Teórico

En este capítulo se describirán los conceptos fundamentales relacionados a la infraestructura del Marco COBIT, la Norma PCI y a la solución propuesta. (agregar la historia ISO 17999 + 27001+27002

2.1 Definiciones Teóricas

2.1.1 COBIT

HISTORIA Y EVOLUCIÓN DEL COBIT.

El proyecto COBIT se emprendió por primera vez en el año 1995, con el fin de crear un mayor producto global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, así como sobre los controles de los sistemas de información implantados. La primera edición del COBIT, fue publicada en 1996 y fue vendida en 98 países de todo el mundo. La segunda edición (tema de estudio en este informe) publicada en Abril de 1998, desarrolla y mejora lo que poseía la anterior mediante la incorporación de un mayor número de documentos de referencia fundamentales, nuevos y revisados (de forma detallada) objetivos de control de alto nivel, intensificando las líneas maestras de auditoría, introduciendo un conjunto de herramientas de implementación, así como un CD-ROM completamente organizado el cual contiene la totalidad de los contenidos de esta segunda edición.

Evolución del producto COBIT

El COBIT evolucionará a través de los años y será el fundamento de investigaciones futuras, por lo que se generará una familia de productos COBIT. Al ocurrir esto, las tareas y actividades que sirven como la estructura para organizar los Objetivos de Control de TI, serán refinadas posteriormente, siendo también revisado el balance entre los dominios y los procesos a la luz de los cambios en la industria.

Una temprana adición significativa visualizada para la familia de productos COBIT, es el desarrollo de las Guías de Gerencia que incluyen Factores Críticos de Éxito, Indicadores Clave de Desempeño y Medidas Comparativas. Los Factores Críticos de Éxito, identificarán los aspectos o acciones más importantes para la administración y poder tomar, así, dichas acciones o considerar los aspectos para lograr control sobre sus procesos de TI. Los Indicadores Clave de Desempeño proporcionarán medidas de éxito que permitirán a la gerencia conocer si un proceso de TI está alcanzando los requerimientos de negocio. La Medidas Comparativas definirán niveles de madurez que pueden ser utilizadas por la gerencia para: determinar el nivel actual de madurez de la empresa; determinar el nivel de madurez que se desea lograr, como una función de sus riesgos y objetivos; y proporcionar una base de comparación de sus prácticas de control de TI contra empresas similares o normas de la industria. Esta adición, proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 Objetivos de Control de alto nivel de COBIT.

En definitiva, la organización ISACF (creadora, como ya se ha comentado, de la norma) espera que el COBIT sea adoptado por las comunidades de auditoría y negocio como un estándar generalmente aceptado para el control de las Tecnologías de la Información.

Desarrollo y Componentes del COBIT.

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información. El COBIT es, pues, una herramienta innovadora para el gobierno de las Tecnologías de la Información.

El COBIT se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulativos y específicos para la industria, tanto los ya existentes como los que están surgiendo en la actualidad. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término "generalmente aplicables y aceptados" es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, "buenas prácticas" significa consenso por parte de los expertos.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

El desarrollo de COBIT ha traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

Se determinó que las mejoras a los objetivos de control originales deberían consistir en:

- El desarrollo de un marco referencial para el control en tecnologías de la información como fundamento para los objetivos de control en TI, y como una guía para la investigación consistente en auditoría y control de las tecnologías de la información;
- Una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho;
- Una revisión crítica de las diferentes actividades y tareas que conforman los dominios de control en tecnología de información y, cuando fuese posible, la especificación de indicadores de desempeño relevantes (normas, reglas, etc.), así como una revisión crítica y una actualización de las guías actuales para el desarrollo de auditorías de los sistemas de información.

Componentes del COBIT 2ª Edición

El desarrollo del COBIT (2ª Edición), ha resultado en la publicación de los siguientes

componentes: Un Resumen Ejecutivo (Executive Sumary), el cual consiste en una síntesis ejecutiva que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios del COBIT; un Marco Referencial (Framework), el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios del COBIT, e identifica los cuatro dominios de COBIT describiendo en detalle, además, los 34 objetivos de control de alto nivel e identificando los

requerimientos de negocio para la información y los recursos de las Tecnologías de la Información que son impactados en forma primaria por cada objetivo de control; los Objetivos de Control (Control Objetives), los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de las Tecnologías de la Información;

las Guías de Auditoría (Audit Guidelines), las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o unas recomendaciones para mejorar; un Conjunto de Herramientas de Implementación (Implementation Tool Set), el cual proporciona las lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo. Este conjunto de herramientas de implementación incluye la Síntesis Ejecutiva, proporcionando a la alta gerencia conciencia y entendimiento del COBIT. También incluye una guía de implementación con dos útiles herramientas: Diagnóstico de la Conciencia de la Gerencia y el Diagnóstico de Control de TI, para proporcionar asistencia en el análisis del ambiente de control en TI de una organización. También se incluyen varios casos de estudio que detallan como organizaciones en todo el mundo han implementado COBIT exitosamente. Adicionalmente, se incluyen respuestas a las 25 preguntas más frecuentes acerca del COBIT, así como varias presentaciones para distintos niveles jerárquicos y audiencias dentro de las organizaciones.

2.1.2 PCI

PCI DSS soporte para la **Industria de la Tarjeta de Pago - Estándar de la Seguridad de Datos**. Fue desarrollado por el grupo de compañías de tarjeta de crédito como pauta para ayudar a las organizaciones que emiten dichas tarjetas en los procesos de los pagos de dicho producto con el fin de prevenir el fraude, las vulnerabilidades y las amenazas en la seguridad. Una compañía que procesa, almacena tarjetas o datos de la tarjeta de pago debe cumplir con la norma PCI DSS o arriesgar su capacidad de procesar pagos

con las tarjetas de crédito. Los comerciantes y proveedores de servicio de la tarjeta de de crédito deben validar su conformidad periódicamente de lo contrario será multado. Esta validación se realiza por los interventores - es decir las personas que integran el grupo PCI DSS quienes fueron calificados como asesores de la seguridad (QSAs). Aunque los informes de QSA sobre conformidad se pueden firmar solamente por un QSA individual a nombre de una consulta aprobada por el consejo del PCI. A las Compañías más pequeñas, que procesen *menos* de 80.000 transacciones al año, se les permiten realizar un cuestionario de autovaloración.

El PCI DSS comenzó originalmente con cinco compañías: Visa (Programa de la seguridad de la información de la tarjeta), Mastercard (Protección de los datos del sitio), American Express (Política de funcionamiento de la seguridad de datos), Discover (Información y conformidad), y JCB (Programa de la seguridad de datos). Las intenciones de cada compañía eran similares: crear un nivel adicional de protección para los clientes asegurándose de que los comerciantes resuelvan niveles mínimos de la seguridad cuando almacenan, procesan y transmitan los datos del titular de la tarjeta. Formaron el consejo PCI - DSS, y el 15 de diciembre 2004, estas compañías alinearon sus políticas individuales y crearon el estándar PCI

En Septiembre de 2006, el estándar del PCI fue puesto al día a la versión 1.1 para proporcionar la clarificación y revisiones de menor importancia a la versión 1.0.

En octubre de 2007, VISA internacional, anunció una nueva seguridad en las formas de pago, asigna por mandato "que las compañías deben alinearse al PCI." Los mandatos se deben poner en ejecución antes de 2010 llama a los "nuevos comerciantes que desean estar autorizados para las transacciones con las tarjetas de pago tendrán que utilizar solamente usos de Aplicaciones de Pago (PABP) validados." Estos nuevos mandatos quieren ayudar a las compañías a alcanzar la conformidad en la mejor práctica en formas de pago (PABP), una puesta en práctica de PCI DSS en el software del vendedor.

2.1.3 ISO 17999

La seguridad siempre ha sido una preocupación para el hombre, los deseos de proteger la información de una manera segura no es una preocupación exclusiva de esta era; por

el contrario, a lo largo de la historia del hombre se han usado diversos mecanismos para alcanzar este cometido.

La trascendencia de la seguridad de la información en las organizaciones públicas o privadas radica en que: (i) el volumen de información crece día a día; (ii) la información es un intangible con un valor bastante apreciable en la economía actual; (iii) la información es una ventaja estratégica en el mercado, que la convierte en algo atractivo para la competencia, como elemento generador de riqueza, (iv) la frecuencia de los ataques a los activos de una organización es cada vez mayor, cualquiera que sea el medio al que se acuda, y (v) no existe una cultura de seguridad en los usuarios de la información, lo que conduce a que las organizaciones empiecen a incorporar prácticas seguras de protección de la información, advirtiendo que este proceso habrá de impactar la cultura de la organización; aspecto que requiere de tiempo y compromiso, empezando por la dirección de la misma.

El origen reciente de la seguridad la información, entendida como un proceso que se debe gestionar, nace en el Reino Unido, donde el Departamento de Industria y Comercio y las empresas del sector privado trabajaron de manera conjunta en esta problemática, lo cual dio origen a la norma BS7799 en el primer lustro de la década pasada; norma que no pretendía ser más que un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información.

A finales de la década pasada esta norma fue actualizada y complementada, lo cual dio como resultado una norma que establecía las recomendaciones para que una empresa evaluará y certificará su sistema de gestión de seguridad de la información. Esta nueva versión de la norma se convirtió en la norma ISO 17999 de diciembre de 2000, la cual estaba alineada con las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico) en materia de privacidad, seguridad de la información y Criptología, hecho de gran trascendencia, pues le otorgaba un carácter global a la norma. En el 2002, la norma adquiere la denominación de ISO 27001, luego de una nueva actualización

2.1.4 27001

El estándar para la seguridad de la información **ISO/IEC 27001** (*Information technology - Security techniques - Information security management systems - Requirements*) fue aprobado y publicado como estándar internacional en Octubre de 2005 por International Organization for Standardization y por la comisión 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 "Ciclo de Deming": PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Evolución

España

En el año 2004 se publicó la UNE 71502 titulada *Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)* y que fue elaborada por el comité técnico AEN/CTN 71. Es una adaptación nacional de la norma británica British Standard BS 7799-2:2002.

Con la publicación de UNE-ISO/IEC 27001 (traducción al español del original inglés) dejó de estar vigente la UNE 71502 y las empresas nacionales certificadas en esta última están pasando progresivamente sus certificaciones a UNE-ISO/IEC 27001.

Implantación

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a

estar sometido al Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) elegido. En general, es recomendable la ayuda de consultores externos.

Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos (p.ej., en España la conocida LOPD y sus normas de desarrollo, siendo el más importante el Real Decreto 1720/2007, de 21 de Diciembre de desarrollo de la Ley Orgánica de Protección de Datos) o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI).

Certificación

La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

Antes de la publicación del estándar ISO 27001, las organizaciones interesadas eran certificadas según el estándar británico BS 7799-2.

Desde finales de 2005, las organizaciones ya pueden obtener la certificación ISO/IEC 27001 en su primera certificación con éxito o mediante su recertificación trienal, puesto que la certificación BS 7799-2 ha quedado reemplazada.

El Anexo C de la norma muestra las correspondencias del Sistema de Gestión de la Seguridad de la Información (SGSI) con el Sistema de Gestión de la Calidad según ISO 9001:2000 y con el Sistema de Gestión Medio Ambiental según ISO 14001:2004 (ver

ISO 14000), hasta el punto de poder llegar a certificar una organización en varias normas y en base a un sistema de gestión común.

La Serie 27000

La seguridad de la información tiene asignada la serie 27000 dentro de los estándares ISO/IEC:

- ISO 27000: Actualmente en fase de desarrollo. Contendrá términos y definiciones que se emplean en toda la serie 27000.
- UNE-ISO/IEC 27001:2007 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Fecha de la de la versión española 29 Noviembre de 2007. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO17799).
- ISO 27002: (anteriormente denominada ISO17799).Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.
- ISO 27003: En fase de desarrollo; probable publicación en 2009. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
- ISO 27004: Publicada en diciembre 2009. Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados.
- ISO 27005: Publicada en Junio de 2008. Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.

- ISO 27006: Publicada en Febrero de 2007. Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

2.2 Marco Conceptual

2.2.1 DS5 Garantizar la Seguridad de los Sistemas

2.2.1.1 Seguridad de la red

Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes [Cobit]

2.2.1.2 Administración de Llaves Criptográficas

Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizada. [Cobit]

2.2.1.3 Prevención, Detección y Corrección de Software Malicioso

Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura) [Cobit]

2.2.1.4 Administración de Identidad

Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobad responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

2.2.1.5 Administración de Cuentas de Usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados. [Cobit]

2.2.1.6 Definición de Incidente de Seguridad

Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas. [Cobit]

2.2.1.7 Intercambio de Datos Sensitivos

Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.[Cobit]

2.2.1.8 Administración de la Seguridad de TI

Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio. [Cobit]

La administración de seguridad no se detiene con la prevención. Las cosas pueden salir mal, independientemente de qué tan bien se controlen las amenazas y las vulnerabilidades, y se implementen los controles de acceso. Una administración de seguridad prudente refleja que la empresa asume la posibilidad de que alguna vez existan fallas dentro de su infraestructura de TI. Las fallas no se limitan a las violaciones de la seguridad, aunque, los desastres naturales, las fallas eléctricas, el funcionamiento defectuoso del hardware y las fallas del software pueden afectar la habilidad de la organización para funcionar. La continuidad del servicio es la práctica o preparación para dichas complicaciones y la creación de estrategias para recuperar con el mínimo impacto posible las operaciones de la empresa. Los principales aspectos de las prácticas para la continuidad del servicio son:

- Identificar los requisitos de la empresa para la continuidad del servicio
- Formular planes de respaldo y recuperación

- Explorar las mejores prácticas para mantener la continuidad del servicio

Como sucede con otras áreas de la administración de seguridad, la continuidad de los servicios y otras operaciones de TI se superponen en gran medida. En el caso de la continuidad del servicio, gran parte pertenece al área de administración de almacenamiento. Por supuesto, la administración de almacenamiento no trata sólo de la continuidad del servicio, así como la administración de seguridad abarca más que la continuidad del servicio. Las dos, sin embargo, están estrechamente combinadas, y las técnicas desarrolladas en ambas áreas se complementan entre sí para proporcionar un enfoque integral destinado a la planificación de la continuidad del servicio.

El primer paso para comprender el alcance de los requisitos de la continuidad del servicio es comprender los datos y activos necesarios para mantener las operaciones de la organización. La planificación de la continuidad del servicio no consiste simplemente en el respaldo de todos los datos, en el almacenamiento de medios de respaldo fuera del sitio o en la restauración de los datos según sea necesario. Aunque ese enfoque puede funcionar para empresas muy pequeñas, la mayoría de las organizaciones con infraestructuras de TI han evolucionado hacia entornos más complejos que requieren una amplia gama de soluciones.

El nivel básico de la funcionalidad incluye aquellos servicios necesarios para asegurar las operaciones esenciales (los sistemas operativos y los hardware básicos también se incluyen dentro del punto de recuperación), así como también aquellos que se encuentran adjuntos a los flujos de ingresos o que requieren por norma. Si estos sistemas no funcionan, la empresa no puede llevar a cabo sus operaciones de negocio.

2.2.1.9 Evaluación de Riesgos

La evaluación de riesgos debe identificar, cuantificar y priorizar riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos. El proceso de evaluación de riesgos y de seleccionar controles puede requerir que sea realizado un número de veces con el fin de cubrir diferentes partes de la organización o sistemas de información individuales. [INDECOPI07]

2.2.1.10 Plan de Seguridad de TI

Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios. [Cobit]

2.2.2 DS12 Garantizar la Seguridad Física

2.2.2.1 Acceso Físico

Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona. [Cobit]

2.2.3 Otros

2.2.3.1 Criterios de Información de CobIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en Cobit como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y seguridad, se definieron los siguientes siete criterios de información:

Efectividad: tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

Eficiencia: consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.

Confidencialidad: se refiere a la protección de información sensitiva contra revelación no autorizada.

Integridad: está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

Disponibilidad: se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

Cumplimiento: tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

Confiabilidad: se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno. [Cobit]

2.2.3.2 Modelos de Madurez

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que consideren qué tan bien se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información. Aunque pocos argumentarían que esto no es algo bueno, se debe considerar el equilibrio del costo beneficio y éstas preguntas relacionadas:

• ¿Qué está haciendo nuestra competencia en la industria, y cómo estamos posicionados en relación a ellos?

• ¿Cuáles son las mejores prácticas aceptables en la industria, y cómo estamos posicionados con respecto a estas prácticas?

• Con base en estas comparaciones, ¿se puede decir que estamos haciendo lo suficiente?

• ¿Cómo identificamos lo que se requiere hacer para alcanzar un nivel adecuado de administración y control sobre nuestros procesos de TI?

Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La gerencia de TI está buscando constantemente herramientas de evaluación para benchmarking y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el dueño del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control. Esto responde a tres necesidades:

1. Una medición relativa de dónde se encuentra la empresa

2. Una manera de decidir hacia dónde ir de forma eficiente

3. Una herramienta para medir el avance contra la meta

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de

software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control. [Cobit]

2.2.3.3 Recursos de TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. Estos recursos, junto con los procesos, constituyen una arquitectura empresarial para TI Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (Ej., un sistema de planeación de recursos empresariales [ERP]) para dar soporte a la capacidad del negocio (Ej., implementando una cadena de suministro) que genere el resultado deseado (Ej., mayores ventas y beneficios financieros).

Los recursos de TI identificados en COBIT se pueden definir como sigue:

• Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

• La información son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

• La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

• Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios

de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran. [Cobit]

2.2.3.4 Matriz RACI

Es una técnica sistemática y participativa para identificar todas las funciones (actividades, tareas, y decisiones) que se tienen que cumplir para una efectiva operación y ejecución, aclarar roles y niveles individuales de participación en relación a cada una de estas funciones e identificar los mejores métodos para que el personal llene estos roles [PMI] (se utiliza en varios estándares revisar)

2.3 Requisitos de las DSS de la PCI y procedimientos de evaluación de seguridad detallados

2.3.1 Desarrollar y mantener una red segura

Requisito 1: Instale y mantenga una configuración de firewalls para proteger los datos de los titulares de las tarjetas

Los firewalls son dispositivos computarizados que controlan el tránsito permitido en la red de una empresa (interna) y de redes no confiables (externas) así como el tránsito de entrada y salida a áreas más sensibles dentro de la red interna confidencial de la empresa. El entorno del titular de la tarjeta es un ejemplo de un área más confidencial dentro de la red confiable de la empresa.

El firewall evalúa todo el tránsito de la red y bloquea las transmisiones que no cumplen con los criterios especificados de seguridad.

Es necesario proteger todos los sistemas contra el acceso no autorizado desde redes no confiables, ya sea que ingresen al sistema a través de Internet como comercio electrónico, del acceso a Internet desde las computadoras de mesa de los empleados, del acceso al correo electrónico de los empleados, de conexiones dedicadas como conexiones de empresa a empresa mediante redes inalámbricas o a través de otras fuentes. Con frecuencia, algunas vías de conexión hacia y

desde redes no confiables aparentemente insignificantes pueden proporcionar un acceso sin protección a sistemas clave. Los firewalls son un mecanismo de protección esencial para cualquier red de computadores.

(lo de abajo ponerlo en el Anexo I) utilizar para la metodología

Requisito 2: No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.

Los delincuentes (externos e internos a la empresa), por lo general, utilizan las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine para afectar los sistemas. Estas contraseñas y parámetros son conocidos entre las comunidades de hackers y se establecen fácilmente por medio de información pública.

2.3.2 Proteja los datos del titular de la tarjeta

Requisito 3: Proteja los datos del titular de la tarjeta que fueron almacenados

Los métodos de protección como el cifrado, el truncamiento, el ocultamiento y la refundición son importantes componentes de la protección de datos del titular de la tarjeta. Si un intruso viola otros controles de seguridad de red y obtiene acceso a los datos cifrados, sin las claves criptográficas adecuadas no podrá leer ni utilizar esos datos. Los otros métodos eficaces para proteger los datos almacenados deberían considerarse oportunidades para mitigar el riesgo posible. Por ejemplo, los métodos para minimizar el riesgo incluyen no almacenar datos de los titulares de la tarjeta salvo que sea absolutamente necesario, truncar los datos de los titulares de la tarjeta si no se necesita el PAN completo y no enviar el PAN en correos electrónicos no cifrados.

Consulte el *Glosario de términos, abreviaturas y acrónimos de las DSS de la PCI*para obtener definiciones de "criptografía sólida" y otros términos de las DSS de la PCI.

Requisito 4: Codifique la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.

La información confidencial se debe codificar durante su transmisión a través de redes a las que delincuentes puedan acceder fácilmente. Las redes inalámbricas mal configuradas y las vulnerabilidades en cifrados herederos y protocolos de autenticación pueden ser los objetivos de delincuentes que explotan estas vulnerabilidades a los efectos de acceder a los entornos de datos de los titulares de las tarjetas.

2.3.3 Desarrolle un programa de administración de vulnerabilidad

Requisito 5: Utilice y actualice regularmente el software o los programas antivirus

El software malicioso, llamado "malware", incluidos los virus, los gusanos (worm) y los troyanos (Trojan), ingresa a la red durante muchas actividades comerciales aprobadas incluidos los correos electrónicos de los trabajadores y la utilización de Internet, de computadoras portátiles y de dispositivos de almacenamiento y explota las vulnerabilidades del sistema. El software antivirus deberá utilizarse en todos los sistemas que el malware, por lo general, afecta para proteger los sistemas contra las amenazas de software maliciosos actuales o que eventualmente se desarrollen.

Requisito 6: Desarrolle y mantenga sistemas y aplicaciones seguras

Las personas sin escrúpulos utilizan las vulnerabilidades de seguridad para obtener acceso privilegiado a los sistemas. Muchas de estas vulnerabilidades se pueden subsanar mediante parches de seguridad proporcionados por los proveedores. Las entidades que administran los sistemas deben instalar estos parches. Todos los sistemas importantes deben poseer la última versión de los parches adecuados para estar protegidos contra la explotación de los datos de los titulares de las tarjetas y el riego que representan los delincuentes y el software malicioso.

Nota: Los parches de software adecuados son aquéllos que se evaluaron y probaron para confirmar que no crean conflicto con las configuraciones de seguridad existentes. En el caso de las aplicaciones desarrolladas internamente por la institución, es posible evitar numerosas vulnerabilidades mediante la utilización de procesos estándares de desarrollo de sistemas y técnicas de codificación segura. Implemente medidas sólidas de control de acceso.

Requisito 7: Restrinja el acceso a los datos de los titulares de las tarjetas conforme a la necesidad de conocer de la empresa

A los efectos de asegurar que el personal autorizado sea el único que pueda acceder a los datos importantes, se deben implementar sistemas y procesos que limiten el acceso conforme a la necesidad de conocer y conforme a la responsabilidad del cargo.

"La necesidad de conocer" es la situación en que se otorgan derechos a la menor cantidad de datos y privilegios necesarios para realizar una tarea.

Requisito 8: Asigne una ID única a cada persona que tenga acceso a equipos.

La asignación de una identificación (ID) única a cada persona que tenga acceso garantiza que cada una de ellas es responsable de sus actos.

Cuando se ejerce dicha responsabilidad, las acciones en datos críticos y sistemas las realizan usuarios conocidos y autorizados, y además se pueden realizar seguimientos.

Requisito 9: Restrinja el acceso físico a datos de titulares de tarjetas.

Cualquier acceso físico a datos o sistemas que alojen datos de titulares de tarjetas permite el acceso a dispositivos y datos, así como también permite la eliminación de sistemas o copias en papel, y se Supervise y pruebe las redes con regularidad

Requisito 10: Rastree y supervise todo acceso a los recursos de red y datos de titulares de tarjetas.

Los mecanismos de registro y la posibilidad de rastrear las actividades del usuario son críticos para la prevención, detección o minimización del impacto de los riesgos de datos. La presencia de los registros en todos los entornos permite el rastreo, alertas y análisis cuando algo no funciona bien. La determinación de la causa de algún riesgo es muy difícil sin los registros de la actividad del sistema.

Requisito 11: Pruebe con regularidad los sistemas y procesos de seguridad.

Las vulnerabilidades ocasionadas por personas malintencionadas e investigadores se descubren continuamente, y se introducen mediante software nuevo. Los componentes, procesos y software personalizado del sistema se deben probar con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno dinámico

2.3.4 Mantenga una política de seguridad de la información

Requisito 12: Mantenga una política que aborde la seguridad de la información para empleados y contratistas.

Una política de seguridad sólida establece el grado de seguridad para toda la empresa e informa a los empleados lo que se espera de ellos. Todos los empleados deben estar al tanto de la confidencialidad de los datos y de su responsabilidad para protegerlos. A los fines de este requisito, “empleados” se refiere a personal de tiempo completo y parcial, personal temporal, y contratistas y consultores que “residan” en las instalaciones de la empresa.

Capítulo 3: Estado del Arte

Aquí se describe la situación actual de las normas y marcos teóricos que utilizaremos para atacar el problema y ver la solución, basado en los conceptos descritos en el Marco Teórico y Conceptual.

Cabe indicar que el alineamiento del Marco COBIT con la Norma PCI DSS no se ha realizado con anterioridad, en adelante presentamos los últimos alineamientos que se han realizado con el marco COBIT y la norma PCI con otros estándares o ISO's

3.1 ISO27001 vs PCI DSS

Como es sabido, la norma ISO/IEC 27001:2005 define los requerimientos para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de un SGSI (Sistema de Gestión de Seguridad de la Información). Es una norma certificable que se ha convertido en el estándar internacional en gestión de seguridad de la información. Uno de los aspectos que remarca ISO27001 en su cláusula 4.2.1)b)2) es que se deben tener en cuenta los requerimientos legales, regulatorios, de negocio y contractuales que deben ser cumplidos, por lo que podríamos encajar PCI DSS como uno de los requerimientos a cumplir como parte del SGSI que opera en la organización.

Por otro lado, ISO27001 exige que las medidas de seguridad que se implanten estén justificadas en base al riesgo que soporta la organización y en base al riesgo aceptable para ésta (apetito de riesgo), de manera que como resultado del análisis de riesgos se decidirán aquellos riesgos que se quieren gestionar y se determinarán los controles a implementar tomando como base los del Anexo A (ISO17799), aunque pueden utilizarse otros si se considera conveniente. Los objetivos de control que PCI DSS establece son de obligado cumplimiento y lo único que podemos hacer es utilizar controles compensatorios en caso de no poder cumplir un objetivo de control tal y como se especifica.

Aunque ISO27001 cubre los requerimientos PCI DSS, en algunos casos faltan detalles de implementación que PCI DSS sí que especifica. Por tanto, puede utilizarse ISO27001 para gestionar el cumplimiento de PCI DSS, pero a la hora de implementar este cumplimiento se deberá analizar y seguir exactamente lo que PCI DSS especifica que

debe hacerse para cumplir cada requerimiento. Una alternativa podría ser definir el SGSI con un ámbito (scope) muy específico, y que sería el que afecta a la transmisión, almacenamiento y tratamiento de datos de tarjetas de crédito, el ámbito de PCI DSS. El objetivo de hacer esto sería obtener la certificación ISO27001 dentro de este alcance concreto y aprovechar el trabajo realizado para cumplir PCI DSS como base para reducir el tiempo y coste necesario de implantar ISO27001.

3.2 ITIL vs COBIT

Quizás sea COBiT la que más puntos de confluencia presente con ITIL, aunque se presenten como complementarias. Incluso COBiT puede que tenga mayor alcance que ITIL ya que abarca todo el espectro de actividades de IT, mientras que ITIL está centrado solo en "Service Management" (gestión del servicio).

Ambos modelos son también complementarios y se pueden usar juntos: ITIL para lograr efectividad y eficiencia en los servicios TI y COBIT para verificar la conformidad en cuanto a disponibilidad, rendimiento, eficiencia y riesgos asociados de dichos servicios con los objetivos y estrategias de la compañía, usando para ello métricas claves y cuadros de mando que reporten dicha información.

- Habilitadores de negocio en el uso de mejores prácticas
- Concientización de los ejecutivos del negocio
- Importancia de las mejores prácticas en la organización
- Overview de las mejores prácticas de ITIL y COBIT y lo que ellas proveen

Mapeo de los dominios de COBIT a procesos de ITIL:
- Plan and Organize (PO)
- Acquire and Implement (AI)
- Deliver and Support (DS)
- Monitor and Evaluate (ME)

Mapeo del ciclo de vida ITIL a los dominioes de COBIT:
- Service Strategy (SS)
- Service Design (SD)
- Service Transition (ST)

- Service Operation (SO)
- Continual Service Improvement (CSI)

3.3 VAL IT Vs. COBIT

Val IT está muy fuertemente integrado con COBIT. En realidad Val IT extiende y complementa a COBIT, el cual provee un marco de trabajo completo para el gobierno y control de las TI. Particularmente, Val IT se enfoca en la decisiones de inversión (responde a la pregunta: "¿Estamos haciendo las cosas correctas?") y la obtención de beneficios (responde a la pregunta: "¿Estamos consiguiendo los beneficios esperados?"), mientras que COBIT se enfoca en la calidad y la ejecución (responde a las preguntas:"¿Estamos haciendo estas cosas de la manera correcta?" y "¿Las estamos haciendo bien?").

Por ello, ambos estándares son complementarios: Use COBIT para controlar y medir los servicios e infraestructura de TI y Val IT para complementar dichas mediciones desde el punto de vista financiero.

3.4 COSO vs PCI

PCI DSS, estándar desarrollado por el PCI Security Standard Council (organismo creado por VISA, Mastercard, AMEX, JCB y DISCOVER), debe ser implantado por entidades bancarias, proveedores de servicio y comercios que tratan con datos de tarjetas de pago. Entre ellos se encuentra Local Billing, que concienciado de la necesidad de implementar mejoras de seguridad de forma continuada ha cumplido con las normas establecidas por el sector de las tarjetas de pago. Este cumplimiento del estándar de seguridad PCI DSS, permite a Local Billing mejorar el servicio a sus clientes garantizando, si cabe aún más, la seguridad de sus datos bancarios en todos los procesos en que trata con tarjetas de pago.

El estándar define el conjunto de requerimientos que permiten gestionar la seguridad y definir las políticas y los procedimientos de seguridad necesarios tanto a nivel de infraestructura, diseño de red o arquitectura de sistemas.

Servicios de Local Billing

Local Billing proporciona servicios de intermediación en el procesamiento de pagos en línea. Se estructura en varias áreas o grupos: el grupo de procesamiento de pagos, el grupo de servicio de atención al cliente y el grupo de consultoría. El grupo de Procesamiento de Pagos permite optimizar la aceptación del pago para comercios que desean vender sus productos en línea (software, información, música, vídeos, etc.)

Su plataforma de procesamiento de pago es capaz de transferir el tráfico a varios proveedores para maximizar el número de métodos de pago aceptados y optimizar el tiempo de actividad de sus comerciantes. La política de la compañía es garantizar un mínimo de dos proveedores de pago por cada método de pago y así poder garantizar la estabilidad y fiabilidad a sus clientes.

Local Billing, como proveedor de servicios que recoge, almacena, procesa y transmite datos de tarjetas de pago, adelantándose a la solicitud por parte de sus clientes, decidió apostar una vez más por el beneficio de éstos y entre sus prioridades decidió incluir la implantación de este estándar de seguridad que le ha permitido verificar, corregir y mejorar el correcto procesamiento, transmisión y almacenamiento de los datos relativos a tarjetas de pago. Para ello ha contado con el soporte de Internet Security Auditors,. empresa experta en seguridad que le ha proporcionado el asesoramiento y soporte necesarios para implantar con éxito los proyectos que le han permitido alcanzar el cumplimiento del estándar PCI DSS. Internet Security Auditors posee las certificaciones de QSA 2 (Qualified Security Assessor) y de ASV 3 (Approved Scanning Vendor) concedidas por el PCI SSC, siendo avalado por todas las marcas de tarjetas de pago que apoyan éste organismo común

El proyecto se ha desarrollado formando un equipo multidisciplinar formado por personal de Local Billing relacionado con departamentos técnicos de desarrollo, sistemas y base de datos, así como responsables de medios de pago, seguridad y cumplimiento normativo, complementando el equipo con consultores QSA de Internet Security Auditors.

Previo a emprender el proyecto se realizaron tareas formativas en PCI DSS con el objetivo de que todo el personal conociera el estándar y lo entendiera lo mejor posible, determinando también las herramientas de soporte a utilizar.

Como herramienta clave para todo el proyecto se decidió utilizar la Wiki corporativa con gestión de roles y permisos. El uso de esta herramienta se escogió por varios motivos: facilidad de uso, ya que todo el personal de Local Billing está acostumbrado a utilizarla en otros proyectos y por tanto no requería formación; es un repositorio ideal para centralizar la información y gestionar el ciclo de vida de la documentación; es accesible por todo el personal de Local Billing repartido geográficamente por todo el mundo; facilita el trabajo en equipo; y junto con otras herramientas de gestión de proyectos se utilizó también para centralizar las tareas que se definieron como parte de la implantación del estándar.

Tras establecer el entorno de trabajo, la primera tarea que se realizó fue analizar los procesos de negocio y establecer el ámbito de Local Billing sobre el que era necesario implementar los requerimientos PCI DSS. Posteriormente se analizaron cada uno de los requerimientos y se definieron las acciones necesarias para su cumplimiento, definiendo el **programa de cumplimiento** a ejecutar para la implantación y mantenimiento del estándar. (Ver **Figura 1**: Fases Implantación PCI DSS)

Figura 8: Fases Implantacion PCI DSS

Minimización del ámbito de aplicación

La estrategia principal que se determinó necesaria e imprescindible para alcanzar con éxito la implantación del estándar, fue **minimizar al máximo el ámbito de aplicación** de PCI DSS. Esto implicó la necesidad de realizar cambios a nivel de segmentación de red entre los entornos de producción/preproducción situados

en el CPD de Amsterdam y el entorno de desarrollo localizado en Barcelona. Requirió establecer controles de acceso estrictos a los componentes de sistemas localizados en el CPD de Amsterdam, para así poder garantizar los niveles de seguridad necesarios sobre los empleados de Local Billing así como para los usuarios de los proveedores de servicios que se conectan remotamente al entorno de producción donde se guardaban los datos de tarjetas.

Una medida que se determinó como obligatoria por el beneficio que aportaba, a pesar del gran esfuerzo que suponía y que aunque se trata uno de los requerimientos primarios del estándar en muchos casos se cubre con controles compensatorios debido a la complejidad de modificar las aplicaciones y bases de datos, fue el cifrado del PAN (Primary Account Number) en base de datos. Para ello se rediseñó la base de datos para contener los datos de tarjetas en formato truncado, hash y finalmente cifrado. Esto se hizo dado que el número de tarjeta completo, o PAN, se necesita únicamente para el procesamiento de los pagos y los empleados de Local Billing y Comercios no necesitan conocer nunca el PAN completo; por lo que ese dato, en lugar de ser enmascarado en su visualización, se extrae directamente truncado de la base de datos.

Para el cifrado se creó un módulo específico que permite gestionar los procesos de cifrado/descifrado del PAN cumpliendo los requerimientos de PCI DSS, acompañado de los procedimientos para la gestión de claves que garantizan la seguridad de las claves de cifrado (creación, regeneración, eliminación, custodia, etc.)

La finalidad fue eliminar, lo máximo posible, la necesidad de implementar requerimientos PCI DSS en los componentes de sistemas ubicados en las oficinas centrales en Barcelona y sobre los cuales era más complicado establecer unas medidas de seguridad tan exigentes como las que impone PCI DSS en algunos casos.

Además de los aspectos técnicos que se han implementado para el cumplimiento de PCI DSS, los aspectos referentes a la gestión y mantenimiento del cumplimiento con el estándar, se han cubierto definiendo procesos y procedimientos orientados a ser simples, fáciles de entender por todos los afectados, definiendo puntos de control para su correcta aplicación y accesibles a través de la Wiki.

Todo el personal de Local Billing y proveedores implicados han sido agrupados bajo roles de acceso y se les ha formado en las funciones y responsabilidades ligadas a PCI DSS. Se ha proporcionado formación en desarrollo seguro a los programadores por miembros expertos del equipo de Internet Security Auditors y se han definido materiales para realizar sesiones de concienciación en seguridad y en el buen uso de los datos de tarjetas de pago.

Local Billing es consciente de que el cumplimiento de PCI DSS es un proceso continuo por lo que se ha creado la figura de PCI Manager para garantizar dicho cumplimiento. (Ver **Figura 2**: PDCA PCI DSS).

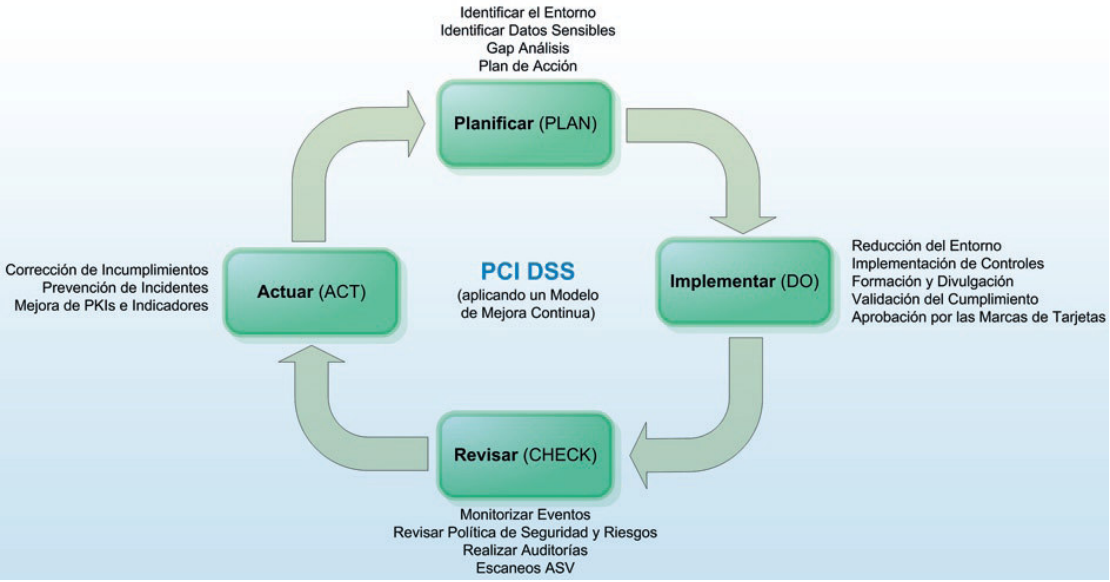


Figura 9: PDCA PCI DSS

Aspectos clave

Local Billing trabaja con un gran número de empresas a las que subcontrata servicios de espacio físico de CPD, mantenimiento de sistemas y dispositivos de red, pasarelas de pago, desarrollo de software, etc. Esto ha supuesto que la gestión del cumplimiento de los diferentes proveedores con PCI DSS haya sido un aspecto clave para garantizar el cumplimiento y la certificación de Local Billing, llegando a ser necesario rescindir el contrato con pasarelas de pago que no cumplían con el estándar PCI DSS.

Entre otros problemas que se tuvieron que solventar nos encontramos con proveedores de pasarela de pago que requerían el envío del CVV2 en cada transacción, con lo que

obligaba a Local Billing a almacenar dicho dato en su base de datos y por tanto incumplir PCI DSS. Este inconveniente se pudo solventar redefiniendo junto con el proveedor de pasarela de pago el protocolo utilizado. Tras la implantación satisfactoria del programa de cumplimiento se realizó, por parte de un auditor QSA (Qualified Security Assessor) de Internet Security Auditors, la auditoría necesaria para poder validar ante Visa y Mastercard el cumplimiento de PCI DSS. El equipo auditor QSA definió y ejecutó las pruebas de auditoría mediante obtención de evidencias revisando documentación, analizando componentes de sistemas y entrevistando al personal de Local Billing, así como a personal de los proveedores más críticos para el cumplimiento de PCI DSS, incluyendo el personal en Amsterdam.

Gracias a la gran colaboración y disposición del equipo de Local Billing durante la implantación, la auditoría sólo detectó algunos problemas menores, principalmente de detalle de configuración de sistemas, que tras ser corregidos en pocos días permitieron obtener un informe de auditoría satisfactorio. Estos problemas de configuración tas de proveedores de servicio certificados, siendo el primer proveedor de servicios multinacional con sede en España incluido en estas listas

Capítulo 4: Aplicación del Alineamiento de Marco Cobit con Norma PCI

En este capítulo se aplica el alineamiento para la matriz de asignación de responsabilidades, modelos de madurez y gestión de prevención del fraude.

4.1 Directrices Gerenciales

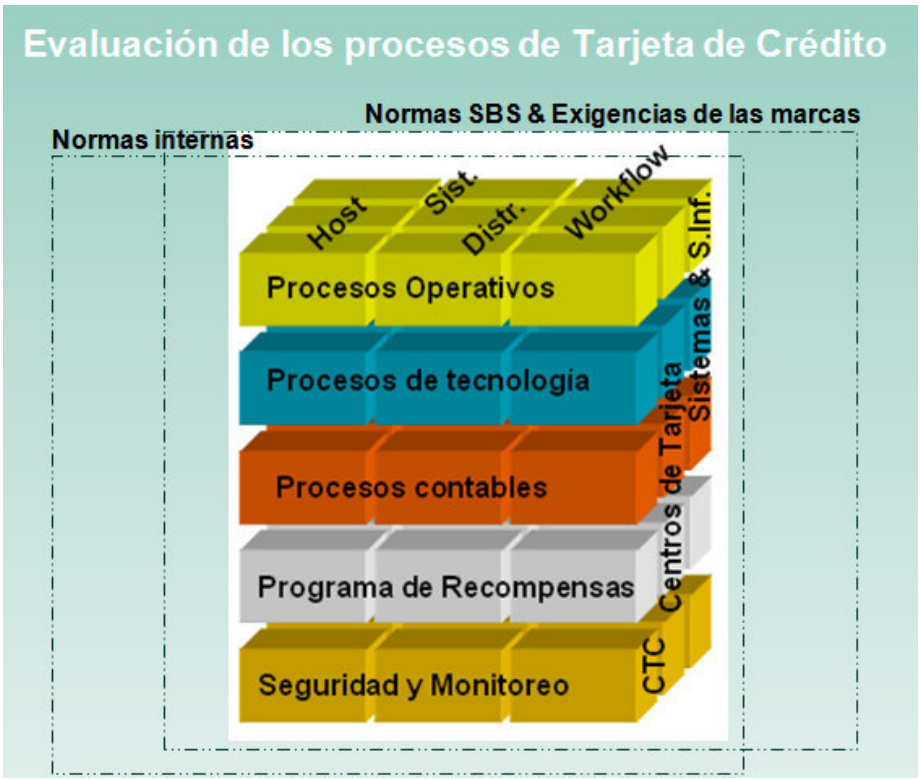


Figura 10: Evaluación de los Procesos de Tarjeta

4.1.1 Entradas

PO2: Arquitectura de información clasificación de datos asignados

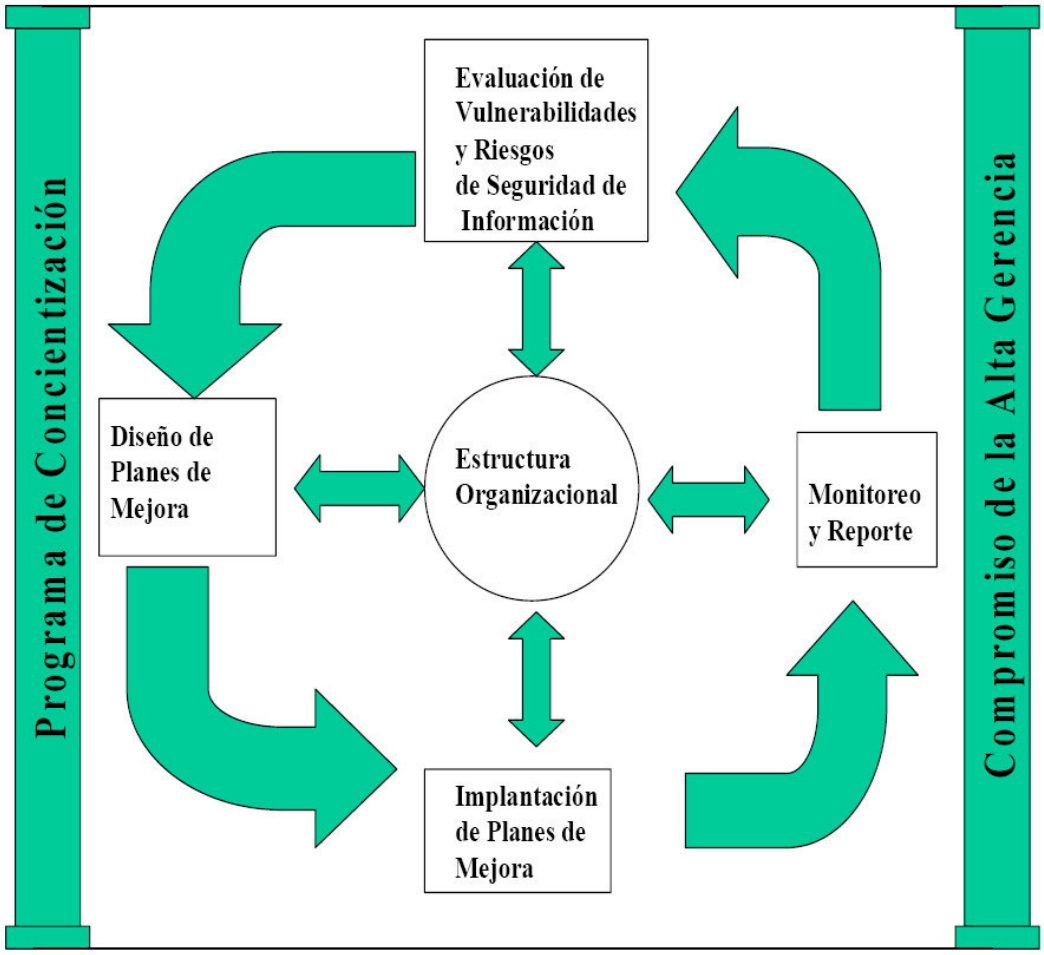


Figura 11: Estructura de Evaluación

PO3: Estándares de tecnología

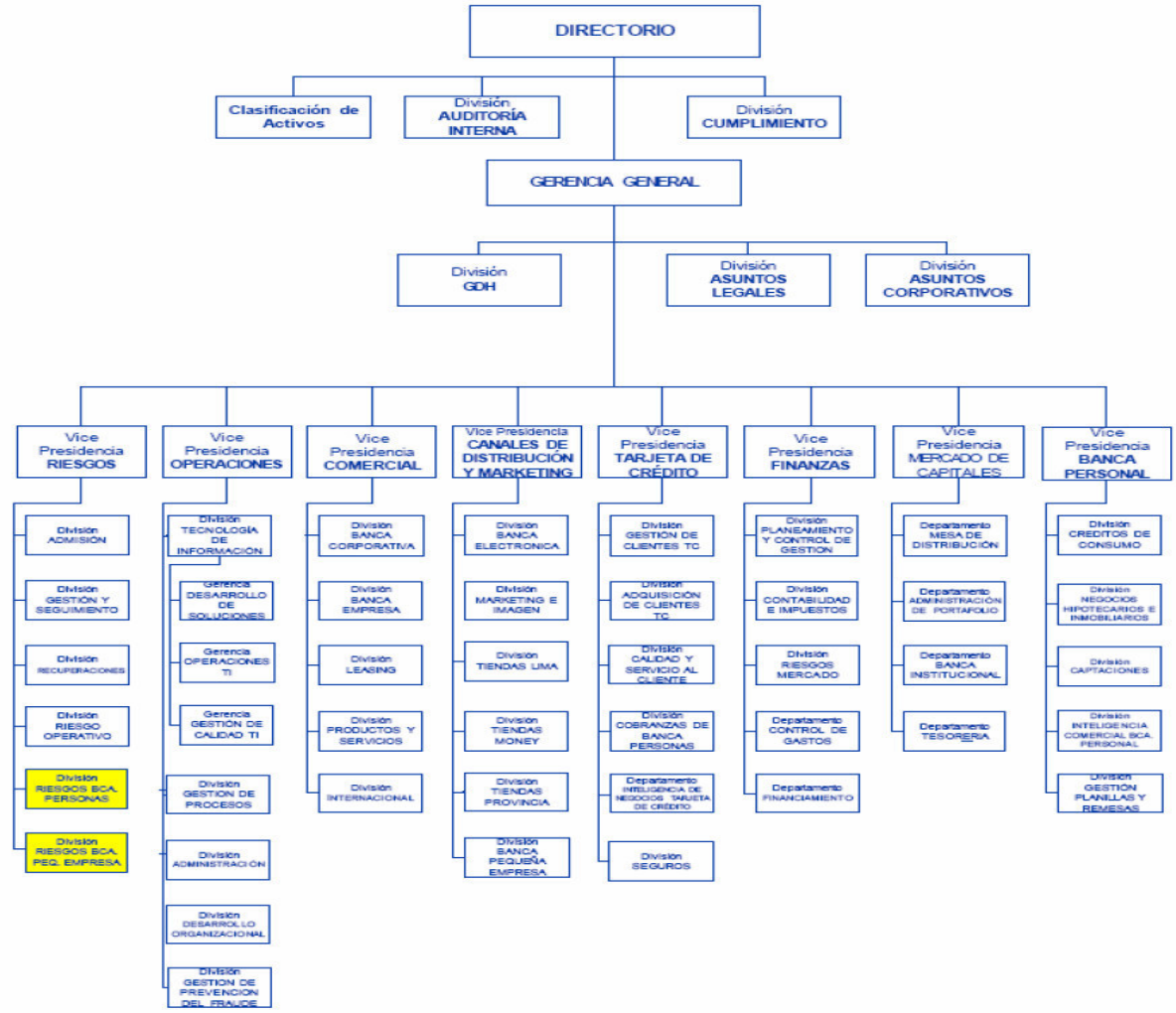
PO9: Evaluación de Riesgo

AI2: Especificaciones de controles de seguridad en las aplicaciones

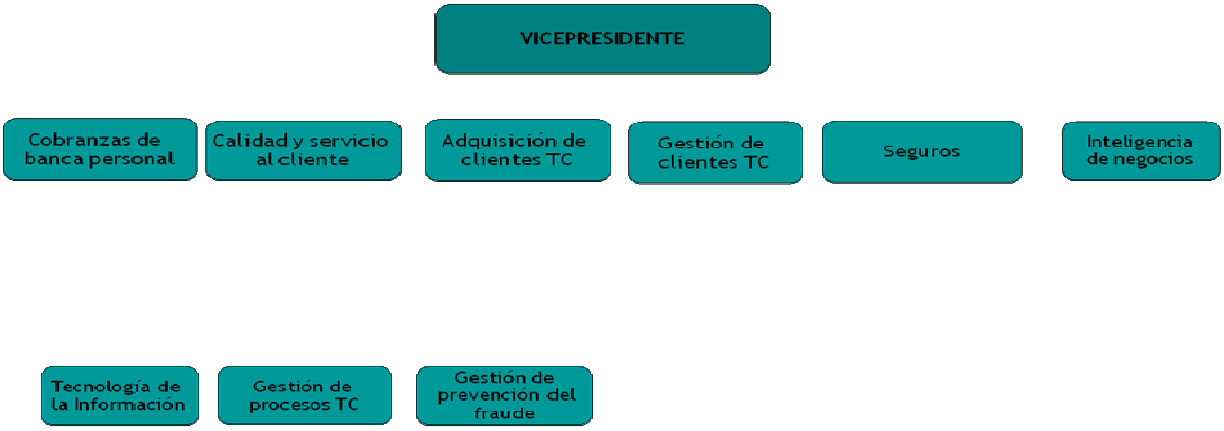
DS1: OLAs

4.2 Organización

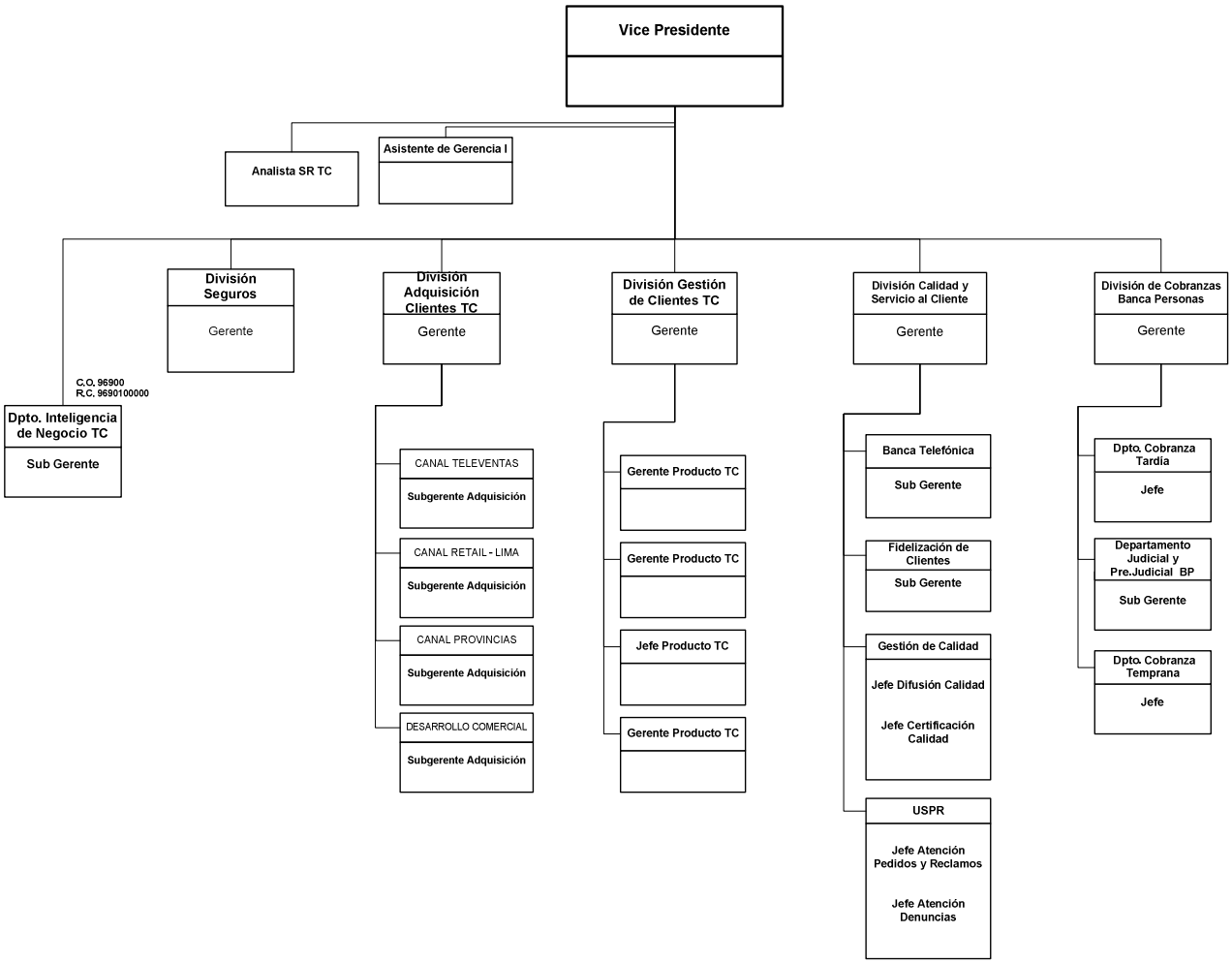
ORGANIGRAMA GENERAL



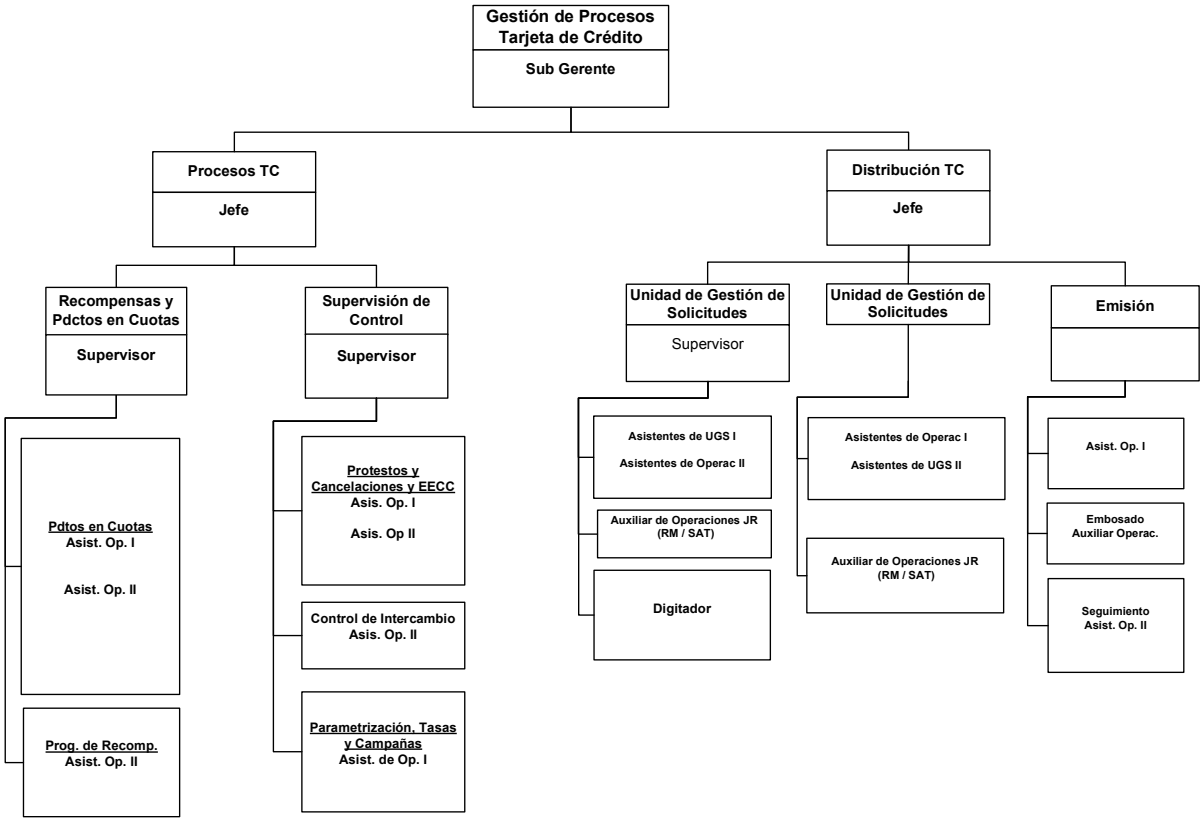
ORGANIZACIÓN TARJETA DE CRÉDITO



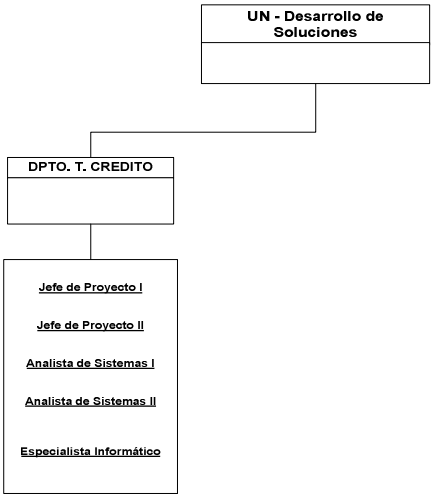
VICEPRESIDENCIA TARJETA DE CREDITO



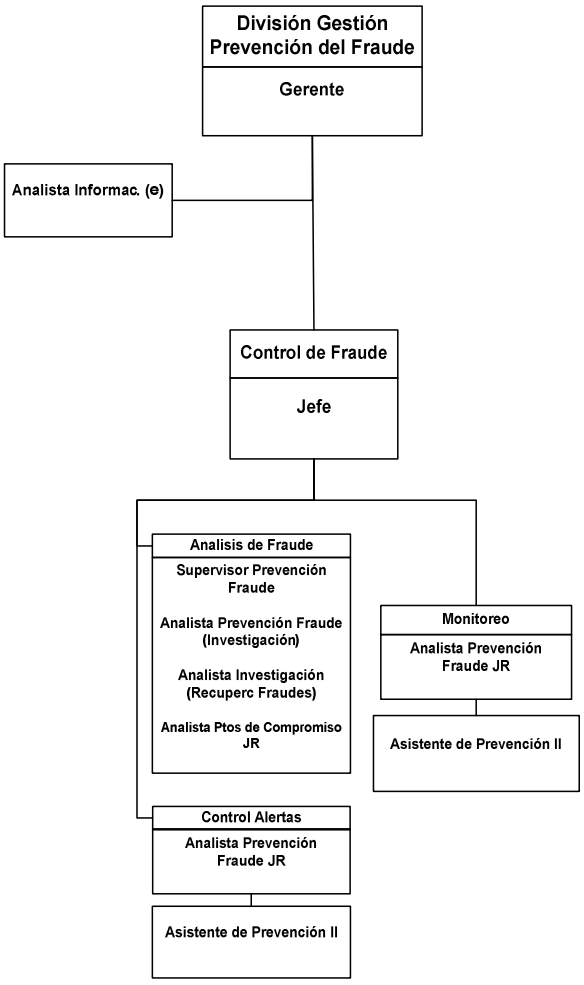
DEPARTAMENTO GESTION PROCESOS
TARJETA DE CREDITO



UN - DESARROLLO DE SOLUCIONES (TI)



DIVISION GESTION PREVENCION DEL FRAUDE



4.2.1 MATRIZ RACI ALINEADA A ORGANIZACION DE ENTIDAD FINANCIERA Y REQUISITOS NORMA PCI (ver Anexo)

	CEO (GG)	CFO	Ejecutivo del negocio	CIO (VICEPRESIDENTE TC)	Dueño de Proceso del negocio	Jefe de Operaciones (Sub-Gte. Gestión Procesos TC)	Arquitecto en Jefe (Jefe Unidad Proy. Soluciones)	Jefe de Desarrollo (Gerente de proyecto Data TC)	Jefe de Administración de TI (Gte Tecnología Información)	PMO	Cumplimiento, Auditoria, Riesgo y Seguridad (GRE TC) *
Definir y mantener un plan de seguridad de TI **(DS5.1, 2, 7)** **(Norma PCI DSS – Requisito 6, 12)**	I	C	C	A	C	C	C	C	I	I	R
Definir, establecer y operar un proceso de administración de identidad (cuentas) **(DS5.3, 4)** **(Norma PCI DSS – Requisito 7, 8)**			I	A	C	R	R	I			C
Monitorear incidentes de seguridad reales y potenciales **(DS5.6)** **(Norma PCI DSS – Requisito 11)**				A	I	R	C	C			R
Revisar y validad periódicamente los privilegios y derechos de				I	A	C					R

acceso de los usuarios **(DS5.3) (Norma PCI DSS – Requisito 8)**											
Establecer y mantener procedimientos para mantener y salvaguardar las llaves criptográficas **(DS5.8, 11) (Norma PCI DSS – Requisito 3, 4)**				A		R			I		C
Implementar y mantener controles técnicos y de procedimientos para proteger el flujo de información a través de la red **(DS5.10) (Norma PCI DSS – Requisito 1, 2, 10, 11)**				A	C	C	R	R			C
Realizar evaluaciones de vulnerabilidad de manera regular **(DS5.5, 9) (Norma PCI DSS – Requisito 5)**		I		A	I	C	C	C			R

	CEO (GG)	CFO	Ejecutivo del negocio	CIO (VICEPRESIDENTE TC)	Dueño de Proceso del negocio	Jefe de Operaciones (Sub-Gte. Gestión Procesos TC)	Arquitecto en Jefe (Jefe Unidad Des. Soluciones)	Jefe de Desarrollo (Gerente de proyecto Dpto. TC)	Jefe de Administración de TI (Gte Tecnología Información)	PMO	Cumplimiento, Auditoria, Riesgo y Seguridad (GPF TC) *
Implementar medidas de ambiente físico **(DS12.3)** **(Norma PCI DSS –Requisito 9)**					I	A/R	I	I			C
Administrar el ambiente físico (mantenimiento, monitoreo y reportes incluidos) **(DS12.3)** **(Norma PCI DSS –Requisito 9)**						A/R	C				
Definir e implementar procesos para mantenimiento y autorización de acceso físico **(DS12.3)** **(Norma PCI DSS –Requisito 9)**				C	I	A/R	I	I	I		C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Responsabilidades

Vicepresidencia Tarjeta de Crédito

Es la encargada de desarrollar y promover el negocio de Tarjeta de Crédito y Débito del Banco, con el objetivo de alcanzar la completa satisfacción del cliente, cumpliendo con las políticas de riesgos y metas de rentabilidad establecidas, así como en la implementación de un Sistema de Calidad Integral. Tiene a su cargo la gestión de riesgos de Banca Personal a nivel de todos los productos de colocación a clientes personas naturales y el área de servicio al cliente (contact center y atención de pedidos y reclamos) para todos los clientes del Banco.

La Vice Presidencia de Tarjeta de Crédito es un órgano de línea y reporta a la Gerencia General. Tiene a su cargo la División de Gestión de Clientes, División de Adquisición de Clientes de Tarjeta de Crédito, Cobranzas de Banca Personas, Calidad y Servicio al Cliente, Seguros y el Departamento de Inteligencia de Negocios de Tarjeta de Crédito.

Soporte

Gerencia de Desarrollo de Soluciones

Es responsable del desarrollo y soporte tecnológico a los diversos productos y servicios del negocio.

Sus funciones son:

• Participar en las definiciones comerciales o usuarias que permitan obtener planteamientos concretos o alternativas de implementación adecuadas a nuestra factibilidad técnica.

• Analizar, diseñar y desarrollar soluciones tecnológicas según los requerimientos recibidos.

• Supervisar y coordinar con otras áreas o con proveedores validando diseños, tecnologías y herramientas propuestas así como las inversiones requeridas.

• Administrar proyectos, asignando prioridades y recursos.

• Realizar seguimiento de los niveles de eficiencia y performance de los sistemas, elaborando planes para mejorar la eficiencia y performance de los mismos.

• Coordinar y gestionar los diversos proyectos que las marcas generan para mejora de sus productos o de los niveles de seguridad requeridos.

• Distribuir los costos de implementación de proyectos y de los servicios de tecnología hacia las unidades usuarias.

• Definir, promover e implantar prácticas y estándares de calidad de productos y servicios de tecnología.

• Cumplir con las demás funciones que le asigne la División de Tecnología de Información, dentro del campo de su competencia.

División Gestión de Procesos

Se encarga de brindar soporte operativo centralizado a la totalidad de los productos y servicios que ofrece el Banco, buscando la optimización constante de sus procesos para poder brindar el mejor servicio a los clientes con el menor costo posible para el banco. Así mismo, efectúa el proceso de control de créditos validando que se enmarquen dentro de las políticas y procedimientos establecidos para su ejecución.

Sus funciones son:

• Registrar y controlar las líneas de crédito debidamente aprobadas y formalizadas.

• Verificar que las propuestas de crédito que recibe cumplan con todos los requisitos y requerimientos de autonomías, formalización y límites legales correspondientes; luego de lo cual efectuará el desembolso de las mismas.

• Registrar, administrar y contabilizar las garantías que amparan las operaciones de créditos aprobadas así como su liberación.

• Efectuar la valorización de los bienes a tomar en garantía, así como mantener actualizados sus valores según las políticas establecidas por el Banco, informando cualquier desfase en la relación deuda – garantía.

• Efectuar revisiones periódicas del desempeño del staff de peritos, a fin de tomar las acciones correctivas necesarias.

• Realizar las transferencias vía BCR a otros Bancos, transferencia de sucursales o cuenta a cuenta a solicitud del cliente.

• Administrar y controlar las transferencias de fondos por caja.

• Realizar el proceso de canje del Banco.

• Evaluar los procesos operativos y dar soporte centralizado a la Red de Tiendas, identificando áreas de mejora y coordinando la implementación de las mismas.

• Emitir periódicamente el Reporte de Información Crediticio Confidencial para la de Banca y Seguros dentro de las normas establecidas por ésta.

• Administrar el envío de remesas de efectivo tanto hacia la Red de Tiendas como hacia la Red de ATMs del Banco, negociando con las compañías transportadoras de valores las mejores condiciones en precio y servicio, buscando siempre un eficiente manejo del efectivo del Banco

• Velar por el funcionamiento, cuadre y contabilización de los aplicativos - productos que le han sido encargados. Así como administrar los parámetros que se encuentran definidos en éstos.

• Administrar la base de datos de clientes del Banco, diseñando los controles pertinentes que aseguren la calidad de la información ingresada a la misma.

• Ejecutar los procesos de alta en el sistema por las solicitudes aprobadas, verificando el cumplimiento de los niveles de autonomía.

• Realizar el embozado de las Tarjetas de Crédito y Débito, coordinar su distribución a través de un courier o funcionarios debidamente autorizados y realizar finalmente la activación de las mismas.

• Mantener el control de las necesidades de stock de Tarjetas de Débito de cada Tienda, coordinando su entrega a través de un courier. Así como, administrar el archivo de solicitudes e instrucciones firmadas por el cliente y custodiar el stock de plásticos sin utilizar.

• Realizar análisis y seguimiento a los cargos y comisiones que genera cada marca de Tarjetas de Crédito y controlar la adecuada ejecución de los procesos de facturación.

• Procesar instrucciones de bloqueo o modificación de la situación de las Tarjetas, así como toda actualización de datos demográficos de los clientes.

• Ejecutar la emisión y entrega de cartas de notificación de deuda para clientes con mora en los niveles establecidos y gestionar con las Notarías el protesto que se requiere para iniciar las acciones de cobranza judicial

• Administrar los procesos relacionados con la compensación e intercambio con las marcas internacionales y privadas con las que el Banco mantiene acuerdos para la emisión de Tarjetas de Crédito o Débito.

• Cumplir con las demás funciones que le asigne la Vice Presidencia de Operaciones, dentro del campo de su competencia.

Gerencia de TI

Es responsable de la entrega de servicios de TI. Vela permanentemente por la calidad, confiabilidad y oportunidad de la información que brinda al Banco y es responsable de brindarle las herramientas tecnológicas que le aseguren una posición de vanguardia en el mercado.

Sus funciones son:

• Diseñar el plan tecnológico del Banco, velando por su ejecución dentro del presupuesto aprobado de inversiones y gastos en tecnología.

• Efectuar la investigación de nuevas tecnologías en la industria e identificar la factibilidad y oportunidad de su aplicación

• Liderar los proyectos de tecnología de información de acuerdo a los planes estratégicos definidos

• Participar activamente en el desarrollo de los proyectos de tecnología de la información liderados por otras divisiones del banco

• Suscribir y administrar los contratos acordados con terceras partes para la provisión de servicios de tecnología que necesite el Banco.

• Asesorar a las unidades de negocio y operativas sobre la utilización y aplicación de las tecnologías disponibles en el Banco y de la base de información ya instalada.

• Asesorar respecto de las áreas de conocimiento que deben ser reforzadas a los diferentes grupos de usuarios sobre temas específicos.

• Registrar y mantener la situación de las iniciativas de automatización de procesos o generación de productos, traducidas en proyectos de tecnología.

• Definir, promover e implantar una estructura de seguridad de información consistente con las metas y objetivos estratégicos del Banco.

• Evaluar y adquirir los sistemas y productos informáticos disponibles en el mercado de acuerdo a las políticas y metodología aprobadas.

• Velar por la correcta ejecución de los procesos informáticos centrales en producción.

• Administrar los sistemas operativos y sistemas de base en las diversas plataformas tecnológicas del Banco.

• Velar por el correcto funcionamiento y disponibilidad de la red de servidores y computadoras personales del Banco a nivel nacional.

• Administrar la red de comunicaciones del Banco.

• Brindar soporte permanente a los usuarios y clientes a través del Centro de Servicios

• Realizar actividades de mantenimiento correctivo y preventivo de los equipos de cómputo del Banco.

• Conducir periódicamente análisis y evaluaciones de planeamiento de capacidad a los diferentes componentes tecnológicos de la organización.

• Atender los requerimientos de compra de equipos de cómputo y accesorios que las diferentes unidades organizativas requieran y que sean sustentadas de acuerdo a las políticas, presupuestos y procedimientos establecidos.

• Administrar las licencias de uso de los componentes de software que se utilizan en el banco.

• Mantener el inventario de activos de tecnología del Banco.

División de Gestión de Prevención del Fraude

La División de Gestión de Prevención del Fraude se encarga de las acciones de mitigación del riesgo de fraude en los productos y servicios que ofrece la entidad financiera, con criterios de pro actividad en la prevención y efectividad en la detección, proponiendo y apoyando la implantación de mejores prácticas para reducir el impacto del fraude en la rentabilidad del banco, generando al mismo

tiempo, percepción de calidad en el servicio ofrecido a nuestros clientes. Participa de manera activa en el despliegue del Programa de Continuidad de Negocio del Banco, en caso de ser requerido.

Sus funciones son:

• Coordinar con órganos de control y de apoyo, internos y externos, las acciones de prevención y de recuperación de pérdidas por fraude.

• Coordinar con las marcas de medios de pago, así como con los emisores y adquirentes de medios de pago, locales e internacionales, el cumplimiento de requerimientos operativos, generación de estadísticas periódicas y administración de riesgos de fraude, según corresponda.

• Dirigir el Comité de Prevención de Fraudes del banco.

Seguridad

Es responsable de los procesos administrativos de la institución referidos a la logística: abastecimientos, mantenimiento, servicios generales, obras y remodelaciones, administración inmobiliaria y seguridad física /electrónica del recurso humano e instalaciones a nivel nacional garantizando la calidad y eficacia de los servicios que prestan al Banco. Participa activamente en la implementación y despliegue del Programa de Continuidad de Negocios del Banco en aquellos aspectos que son de su competencia. Es un órgano de línea y reporta directamente a la Vicepresidencia de Operaciones y Tecnología.

Funciones

• Responder por el control y supervisión del cumplimiento de las normas y procedimientos de seguridad establecidos en los manuales y normativos dictados por el Banco y proponer las modificaciones a las políticas de seguridad para su permanente adecuación a las necesidades del negocio, a la par de las nuevas variables de riesgos de seguridad que vayan apareciendo en el entorno financiero.

• Planear y controlar las operaciones de protección que se ejecutan en resguardo de los bienes patrimoniales del Banco e integridad física de nuestro recurso humano a nivel nacional.

• Evaluar las necesidades de protección vinculadas a la puesta en marcha de nuevos productos y/o servicios financieros ofrecidos por el Banco.

• Desarrollar la ingeniería para los proyectos de seguridad electrónica requeridos para toda nueva locación o punto de negocio instalado por el Banco a nivel nacional.

• Programar los planes de mantenimiento y programas de pruebas requeridos para el funcionamiento óptimo de los componentes y sistemas instalados en las locaciones del Banco a nivel nacional.

• Organizar, programar y dirigir los concursos para la adquisición de servicios de seguridad física y electrónica, fijando de manera clara y objetiva los parámetros de calificación requeridos para mantener un adecuado estándar de protección en todas nuestras locaciones a nivel nacional.

• Supervisar el ejercicio de las actividades cumplidas por las empresas de seguridad contratadas por el Banco y vigila el cumplimiento de las condiciones contractuales pactadas con los proveedores de seguridad física y electrónica.

• Monitorear de los eventos transmitidos a través del sistema de alarmas de todas las locaciones a nivel nacional incluyendo ATMs, verificando las señales emitidas para el control de ingreso a tiendas, apertura de bóvedas y cajas fuertes, control de los sistemas de tiempo de retardo y activando de manera oportuna procedimientos de respuesta frente a condiciones de alarma generadas por eventos de intrusión, aniegos e incendios.

• Manejar el sistema de apertura remota de cajas fuertes para las Tiendas, validando la conformidad en la operación por parte de los usuarios autorizados y fijando las restricciones de tiempo establecidas dentro de las políticas de seguridad bancaria.

• Proponer y dirigir actividades orientadas a la prevención del fraude interno y externo y realiza las investigaciones frente a siniestros originados por estos

motivos; movilizando los recursos internos y externos necesarios para el esclarecimiento y resolución de los hechos reportados.

• Preparar el programa de capacitación de seguridad dirigido a colaboradores de la Red de Tiendas, organizando en coordinación con el Centro de Aprendizaje de la entidad financiera las charlas, seminarios o talleres que sean requeridos.

• Brindar soporte de seguridad en el tratamiento de bienes adjudicados a solicitud de la División de Recuperaciones, desde la etapa de evaluación y definición de las opciones de custodia, hasta la atención en el pago de sus servicios básicos y solución de necesidades de mantenimiento.

• Mediante la maximización del empleo de los recursos destinados a la supervisión de servicios de custodia armada, intervenir en el mantenimiento de primer escalón a los ATMs de puntos neutros que cuenta con atención compartida; en coordinación con las Divisiones de Banca Electrónica y Gestión de Procesos.

4.3 Modelos de Madurez (Ver Anexo)

4.3.1 DS5 Garantizar la Seguridad de los Sistemas

La administración del proceso de Garantizar la seguridad de los sistemas que satisfaga el requerimiento de negocio de TI de mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad es:

0 No Existente: Cuando la organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.

1 Inicial / Ad Hoc: Cuando la organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.

2 Repetible pero Intuitivo: Cuando Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La habilitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.

3 Definido: Cuando existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe habilitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.

4 Administrado y Medible: Cuando las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en

seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La habilitación sobre seguridad se imparte tanto para TI como para el negocio. La habilitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.

5 Optimizado: Cuando la seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización. Los KGIs y KPIs para administración de seguridad son recopilados y comunicados. La gerencia utiliza los KGIs y KPIs para ajustar el plan de seguridad en un proceso de mejora continua.

4.3.2 DS12 Administración del Ambiente Físico

La administración del proceso de Administrar el ambiente físico que satisface el requerimiento del negocio de TI de proteger los activos de TI y la información del negocio y minimizar el riesgo de interrupciones en el negocio es:

0 No Existente: cuando No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean

1 Inicial / Ad Hoc: Cuando la organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.

2 Repetible pero Intuitivo: Cuando Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. Las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.

3 Definido: Cuando se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con un presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al

cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.

4 Administrado y Medible: Cuando se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, los cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas. Se acordaron los KPIs y KGIs para la supervisión del servicio.

5 Optimizado: Cuando hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente computo de la organización. Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistema eléctricos y mecánicos, protección contra factores ambientales (por ejemplo, fuego, rayos, inundaciones, etc.). se clasifican y se hacen inventarios de todas las instalaciones de acuerdo con el proceso continuo de administración de riesgos de la organización. El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. El ambiente se monitorea y controla por medio de equipo especializado y las salas de equipo funcionan un estricto apego a los horarios y se aplican pruebas regulares a los equipos sensibles. Las estrategias de instalaciones y de estándares están alineadas con las metas de disponibilidad de los servicios de TI y están integradas con la administración de crisis y con la planeación de continuidad del negocio. La gerencia revisa y optimiza las instalaciones utilizando los KPIs y KGIs de manera continua, capitalizando oportunidades para mejorar la contribución al negocio.

4.3.3 Atributos de Madurez

Conciencia y Comunicación

1. Surge el reconocimiento de la necesidad del proceso. Existe comunicación esporádica de los problemas.
2. Existe conciencia de la necesidad de actuar. La gerencia comunica los problemas generales.
3. Existe el entendimiento de la necesidad de actuar. La gerencia es más formal y estructurada en su comunicación.
4. Hay entendimiento de los requerimientos completos. Se aplican técnicas maduras de comunicación y se usan herramientas estándar de comunicación.
5. Existe un entendimiento avanzado y a futuro de los requerimientos. Existe una comunicación proactiva de los problemas, basada en las tendencias, se aplican técnicas maduras de comunicación y se usan herramientas integradas de comunicación

Políticas, Estándares y Procedimientos

1. Existen enfoques ad hoc hacia los procesos y las prácticas. Los procesos y las prácticas no están definidos
2. Surgen procesos similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual. Algunos aspectos de los procesos son repetibles debido a la experiencia individual, y puede existir alguna documentación y entendimiento informal de políticas y procedimientos.
3. Surge el uso de buenas prácticas. Los procesos, políticas y procedimientos están definidos y documentados para todas las actividades clave.

4. El proceso es sólido y completo; se aplican las mejores prácticas internas. Todos los aspectos del proceso están documentados y son repetibles. La dirección ha terminado y aprobado las políticas. Se adoptan y siguen estándares para el desarrollo y mantenimiento.
5. Se aplican las mejores prácticas y estándares externos. La documentación de procesos ha evolucionado a flujos de trabajo automatizados. Los procesos, las políticas y los procedimientos están estandarizados e integrados para permitir una administración y mejora extremo a extremo.

Herramientas y Automatización

1. Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio. No existe un enfoque planeado para el uso de herramientas
2. Existen enfoques comunes para el uso de herramientas pero se basan en soluciones desarrolladas por individuos clave. Pueden haberse adquirido herramientas de proveedores, pero probablemente no se aplican de forma correcta o incluso no usarse.
3. Existe un plan para el uso y estandarización de las herramientas para automatizar el proceso. Se usan herramientas por su propósito básico, pero pueden no estar de acuerdo al plan acordado, y
4. Se implantan las herramientas de acuerdo a un plan estándar y algunas se han integrado con otras herramientas relacionadas. Se usan herramientas en las principales áreas para automatizar la administración del proceso y monitorear las actividades y controles.
5. Se usan juegos de herramientas estandarizados a lo largo de la empresa. Las herramientas están completamente integradas con otras herramientas relacionadas para permitir un soporte integral de los procesos. Se usan las herramientas para dar soporte a la mejora de los procesos y automáticamente detectar excepciones a los controles.

Habilidades y Experiencia

1. No están definidas las habilidades requeridas para el proceso. No existe un plan de entrenamiento y no hay entrenamiento formal.
2. Se identifican los requerimientos mínimos de habilidades para áreas críticas. Se da entrenamiento como respuesta a las necesidades, en lugar de hacerlo con base en un plan acordado. Existe entrenamiento informal sobre la marcha.
3. Se definen y documentan los requerimientos y habilidades para todas las áreas. Existe un plan de entrenamiento formal pero todavía se basa en iniciativas individuales.
4. Los requerimientos de habilidades se actualizan rutinariamente para todas las áreas, se asegura la capacidad para todas las áreas críticas y se fomenta la certificación. Se aplican técnicas maduras de entrenamiento de acuerdo al plan de entrenamiento y se fomenta la compartición del conocimiento.
5. La organización fomenta de manera formal la mejora continua de las habilidades, con base en metas personales y organizacionales claramente definidas. El entrenamiento y la educación dan soporte a las mejores prácticas externas y al uso de conceptos y técnicas. Compartir el conocimiento es una cultura empresarial, y se están desarrollando sistemas basados en el conocimiento. Expertos externos y líderes industriales se emplean como guía.

Responsabilidad y Rendición de Cuentas

1. No existe definición de responsabilidades y de rendición de cuentas. Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva.
2. Un individuo asume su responsabilidad, y por lo general debe rendir cuentas aún si esto no está acordado de modo formal. Existe confusión acerca de la responsabilidad cuando ocurren problemas y una cultura de culpas tiende a existir.

3. La responsabilidad y la rendición de cuentas sobre los procesos están definidas y se han identificado a los dueños de los procesos de negocio. Es poco probable que el dueño del proceso tenga la autoridad plena para
4. Las responsabilidades y la rendición de cuentas sobre los procesos están aceptadas y funcionan de modo que se permite al dueño del proceso descargar sus responsabilidades. Existe una cultura de recompensas que activa la acción positiva.
5. Los dueños de procesos tienen la facultad de tomar decisiones y medidas. La aceptación de la responsabilidad ha descendido en cascada a través de la organización de forma consistente.

Establecimiento y Medición de Metas

1. Las metas no están claras y no existen las mediciones.
2. Existen algunas metas; se establecen algunas mediciones financieras pero solo las conoce la alta dirección. Hay monitoreo inconsistente en áreas aisladas.
3. Se establecen algunas mediciones y metas de efectividad, pero no se comunican, y existe una relación clara con las metas del negocio. Surgen los procesos de medición pero no se aplican de modo consistente. Se adoptan ideas de
4. La eficiencia y la efectividad se miden y comunican y están ligadas a las metas del negocio y al plan estratégico de TI. Se implementa el balanced scorecard de TI en algunas áreas, con excepciones conocidas por la gerencia y se está estandarizando el análisis
5. Existe un sistema de medición de desempeño integrado que liga al desempeño de TI con las metas del negocio por la aplicación global del balanced scorecard de TI. La dirección nota las excepciones de forma global y consistente y el análisis de causas raíz

Desarrollar y mantener una red segura (ver Anexo I, Norma PCI, req. 1,2)

Supervise y pruebe redes con regularidad (ver Anexo I, Norma PCI, req. 10,11)

Puntos de Atención de evaluación realizada a la entidad financiera sobre los requisitos antes mencionados

1. El plan tecnológico en la infraestructura de comunicaciones

    1.1. Los servidores utilizados forman parte de un Plan de Infraestructura Tecnológica y/o el modelo de Arquitectura de Información.

    1.2. Existe una estrategia o políticas referidas a la infraestructura de servidores innovador, seguidor, austero.

    1.3. Existe un proceso de revisión de la infraestructura actual y un análisis de las nuevas tecnologías. Análisis de fortalezas y debilidades de la infraestructura. Informes

    1.4. Existen propuestas de compra o cambio de tecnología para apoyar al negocio o incluso generar nuevos negocios

    1.5. Los proveedores, marcas y modelos utilizados en los servidores forman parte de estándares definidos y aprobados.

    1.6. Las políticas y estándares son aprobados por un comité al interior de la División de Tecnología y Sistemas o equivalente

    Descripción de puesto: Administrador de Redes I

    Investigar sobre nuevas tecnologías de IT

2. Evaluación de desempeño y la capacidad de la red

    - Monitoreo de la capacidad actual comparándolos con las especificaciones del proveedor
    - Informe y planes de acción resultado del monitoreo

3. Los procedimientos de adquisición y mantenimiento

    Reglamento de control de gastos. 1.2.2. AR. Elaborar el presupuesto de su rubro de gasto y velar por su cumplimiento.

    Reglamento de Gastos Operativo

Políticas administrativas

Nivel de obsolescencia

Verificación de los boletines de obsolescencia de equipos

Mantenimiento

- Procedimientos de: recolección, análisis, decisión, plan de acción; referidos a los boletines con anuncios de actualizaciones, parches, releases del software de base de los servidores
- Respaldo previo al mantenimiento
- El mantenimiento es realizado por proveedores, en caso, afirmativo, son ellos quienes conocen las contraseñas de administración
- Existen informes del mantenimiento de los equipos de comunicación
- Existen ambientes de prueba para la instalación y mantenimiento

Servidores:

Transactor

SNA

Correo

Blackberry

SQL

Oracle

Antivirus

Actualización

Manual de Administración de Seguridad de Información

Manual de Seguridad de Información - 2.10 Registros de Actividad El Banco evaluará la activación de registros de actividad en aquellas aplicaciones y

plataformas tecnológicas de producción que no cuenten con la misma. Esta evaluación se realizará siguiendo criterios de costo beneficio y exposición al riesgo.

Manual de Seguridad de Información - 2.12 La División de Sistemas y Tecnología realizará revisiones periódicas sobre la utilización de las computadoras personales, laptops y servidores del Banco, para asegurar que éstas cumplan con los acuerdos de licencias de software.

Manual de Seguridad de Información – 3.3 – Administración de Operaciones

Todos los relojes de las diversas plataformas tecnológicas del Banco, deben estar sincronizados de acuerdo a la hora oficial peruana.

Manual de Seguridad de Información - 3.1.2 d) Acceso privilegiados

La creación de cuentas de usuarios con accesos privilegiados se encuentra restringida a requerimientos de administración y operación a nivel de plataforma tecnológica y de administración, operación o emergencia a nivel de sistema de información. Los privilegios de acceso especiales son: por ejemplo, administradores de servidores, system programmers, administradores de seguridad, etc. Estos privilegios sólo pueden ser otorgados de manera restringida y razonable. Toda excepción a esta política debe ser aprobada por el Gerente de Sistemas y Tecnología y por el área de Seguridad de Información.

Manual de Seguridad de Información - 3.3.1 Programas antivirus

Todos los servidores, computadoras personales y laptops deben contar con versiones actualizadas de antivirus activadas.

Los detectores de virus deben ser instalados en todos las plataformas que lo requieran (Servidores, estaciones de trabajo y red) como parte de la instalación inicial. Estos programas deben ser actualizados regularmente para detectar nuevos virus.

Los usuarios deben abstenerse de ejecutar o abrir archivos ejecutables recibidos por correo electrónico o Internet. El área de Administración de Redes y Soporte Informático deben actualizar periódicamente los tipos de archivos que pueden ser recibidos por medio de correo electrónico, con el fin de reducir la infección de virus por este medio.

Manual de Seguridad de Información - 3.3.2 Correo electrónico

El Área de Administración de Redes tiene la facultad de limitar el tamaño de los mensajes de correo, en función del correcto uso de la infraestructura de comunicaciones del Banco.

Manual de Seguridad de Información - 3.3.4 Encriptación

Debe procurarse que los datos restringidos y confidenciales del Banco sean encriptados cuando son transmitidos por redes externas, utilizando para ello algoritmos o un software de encripción aprobado por Seguridad de Información.

Manual de Seguridad de Información - 3.3.7 Redes, Datos y Software

El personal que cuenta con acceso remoto a los servidores del Banco, debe adoptar medidas de seguridad adecuadas en dicho ambiente.

Manual de Seguridad de Información - 3.3.9 c Conexiones Extranets

Todas las conexiones de red del Banco con redes de Terceros deben pasar por un firewall o un servidor Proxy, cuya configuración de acuerdo a los estándares establecidos por el Banco.

Manual de Seguridad de Información - 3.4.4 Seguridad del Centro de Cómputo y de los equipos del Centro de Cómputo

En el caso que los servidores no se encuentran ubicados dentro del Centro de Cómputo, se deben establecer las mismas medidas de Seguridad.

4. Procedimientos de respaldo / restauración y contingencias

Manual de Seguridad de Información - 3.5.2 Respaldo y Recuperación de la Información de los Servidores de Red y de los Sistemas de Información del Banco.

Los encargados de las plataformas de Banca Electrónica, Ingeniería de Sistemas, Redes y Comunicaciones, deben establecer el cronograma de respaldo, retención, almacenamiento y rotación de las copias de respaldo resguardadas fuera del Banco, de los archivos que aseguren la operación de los computadores y servidores críticos del Banco.

Manual de Seguridad de Información - 3.5.3 Operaciones de copia de Respaldo y Recuperación de la Información de los Servidores de Red y de los Sistemas de Información del Banco.

Se deben tener documentados los procedimientos de copia de respaldo y restauración de la información de los servidores de red y sistemas de información. Cualquier adición o modificación de esos procedimientos deben integrarse dentro de las actividades relacionadas al Desarrollo y Mantenimiento de Proyectos e Infraestructura Tecnológica.

5. Instalación, Certificación y administración de cambio

Administración de cambio

- Roles y responsabilidades (unidades de negocio),
- Clasificación (infraestructura, software base, redes, aplicaciones, etc.)
- Priorización (negocio, técnico)
- Evaluación de impacto,
- Autorización,
- Seguimiento del estado de los cambios,
- Control de versiones,

- Registro de auditoría de los cambios
- Cierre del cambio.

Certificación e Instalación de soluciones y cambios

- Entrenamiento
- Planificación de las pruebas
- Plan de implementación
- Ambiente de prueba
- Migración de la infraestructura y migración de datos
- Ejecución de las prueba de los cambios
- Prueba de Aceptación Final
- Promoción a producción
- Revisión post-implementación

6. Supervisión de servicios provistos por terceros: servicios de comunicación de datos o equipos de comunicación o relacionados

- Relación de servicios provistos por terceros
- Definición de criterios para evaluación del proveedor
- Verificación del cumplimiento de los informes del proveedor
- Revisión de los costos; comparándolos con las condiciones del mercado

(ver Anexo I, requisito 1 - 1.1.1)

A. Recomendaciones generales para la configuración del firewall.

1. No se recomienda la conexión remota al firewall. En caso de necesitarse, se debe implementar un protocolo seguro como IPSEC, utilizando 3DES o AES.

2. Se debe configurar el firewall como "fail closed", es decir en caso de que se produzca algún error, el firewall automáticamente cerrará todas las conexiones.

3. Se deben utilizar rutas estáticas en lugar de protocolos dinámicos como RIPv1, RIPv2 u OSPF.

4. El sistema operativo debe estar actualizado con las últimas versiones recomendadas por el fabricante (Ver estándares de configuración para el sistema operativo) con el fin de garantizar la seguridad en la plataforma y así evitar vulnerabilidades a diferentes tipos de ataques.

5. La aplicación del firewall debe estar con las últimas actualizaciones disponibles.

6. Se recomienda tener la última versión de la aplicación.

7. En caso de envío de información confidencial, esta debe pasar por el firewall en forma encriptada, usando algoritmos como: 3DES o AES.

8. Se recomienda implementar un mecanismo de contraseña única para los administradores del firewall.

Complejidad contraseñas

• Debe tener números, letras y caracteres especiales

• De conocimiento del administrador IT y su asistente

El sistema operativo donde esté funcionando el firewall deberá estar configurado en forma segura. (ver estándares de configuración del sistema operativo) y en lo posible durante su puesta en marcha, sólo instalar los servicios estrictamente requeridos.

B. Parámetros de Seguridad

1. Se deben deshabilitar puertos físicos no utilizados, si existiesen.

2. Se deberán deshabilitar todos los puertos lógicos que no se estén utilizando.

3. No se debe usar o habilitar los servicios de Telnet o FTP.

4. Se deben utilizar todas las posibles herramientas que posea el firewall para evitar ataques de negación de servicio. (DOS)

a. Habilitar función de detección de intrusos

5. Se deberán bloquear los accesos de JavaScript, VBScript, Applets y ActiveX a la red interna.

6. En caso de no necesitarse enrutamiento, se debe habilitar la función de stealth, para que el firewall no sea visible a posibles intrusos, y evitar así un ataque de negación de servicio.

7. Siempre se deberán utilizar reglas donde quede bien claro que máquina se puede conectar con otra y tratar de no utilizar reglas genéricas Source=ANY,

Destination=ANY.

8. Se deberá configurar el TCP Session Timeout en 800 segundos, para reducir el riesgo de recibir una negación de servicio.(DOS)

9. Se recomienda la inspección profunda en el paquete (Deep Packet Inspection) con el fin de evitar que ciertos virus o gusanos penetren en la red y causen pérdida de productividad o disponibilidad.

10. Las comunicaciones de terceros, contratistas u oficinas remotas, deben usar tecnología VPN, conjugando el uso de protocolos de encriptación y de autenticación. Además deben pasar por el firewall encriptadas o terminar en él.

11. Habilitar HTTP para navegar la Internet

12. Habilitar SMTP para el correo electrónico

13. Habilitar DNS

14. Habilitar SMTPS

15. Habilitar IKE client

C. Administración

1. Deshabilitar todo servicio relacionado con la administración que no se esté usando.

2. Cualquier actividad de modificación de una regla del firewall o configuración, debe estar soportada por un procedimiento formal y su respectiva autorización por parte del oficial de seguridad, además de documentarse amplia y detalladamente todas estas actividades.

3. Se debe utilizar alguna herramienta que permita monitorear o administrar los eventos ocurridos en el firewall, tales como intentos de violación en el acceso o de las reglas y esto se debe hacer semanalmente o cuando algún suceso así lo amerite.

D. Auditoría

1. Se deberá habilitar el servicio de registro de eventos, con su correspondiente huella de tiempo, además de definir el tamaño de la memoria a utilizar.

2. Se debe utilizar un servidor de registros (syslog).

3. En el servidor de registros; habilitar huella de tiempo (Timestamps) para facilitar la correlación de eventos a futuro.

4. Se deben hacer respaldo de los registros generados semanalmente.

5. Se deben hacer periódicamente pruebas de penetración sobre el firewall, para estimar su efectividad ante posibles nuevos ataques.

Estructura de Firewall (Ver Anexo I req 1 - 1.1.2 y 1.1.3)

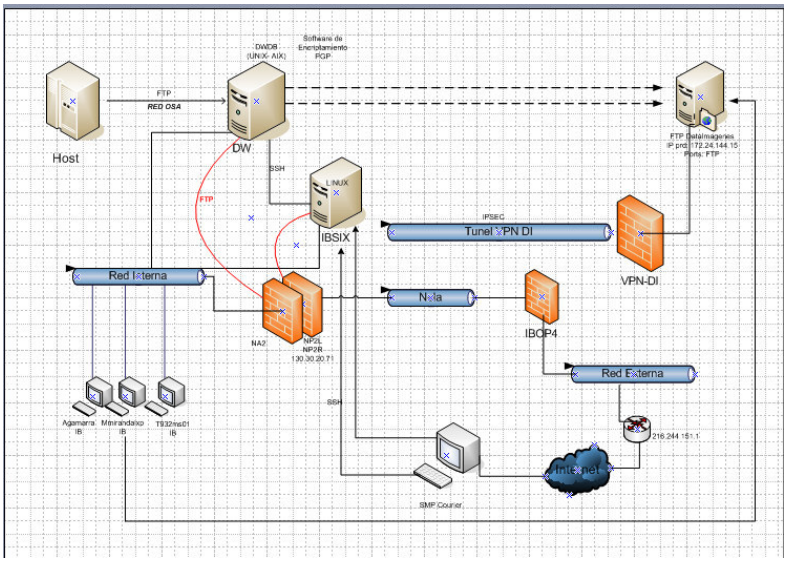


Figura 12: Estructura de Firewall

DMZ

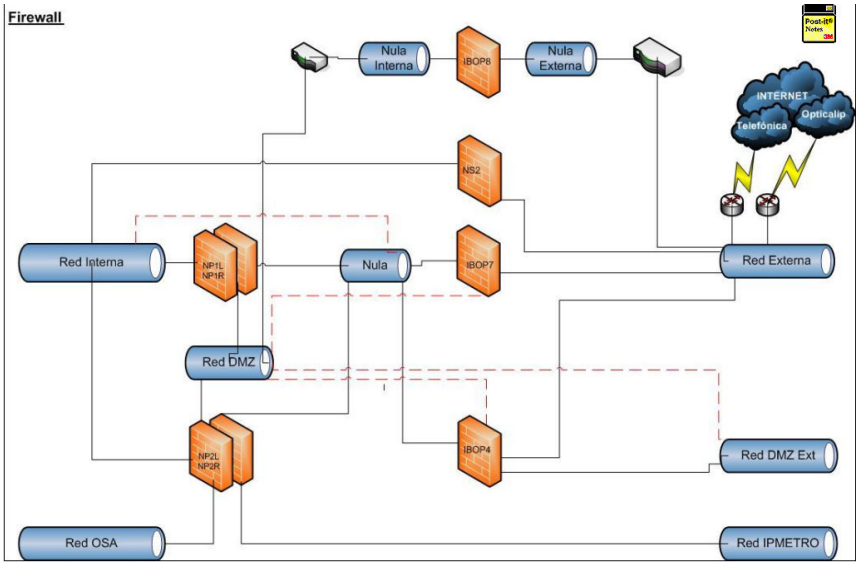


Figura 13: Estructura de Firewall

Responsables de la configuración (Ver Anexo I req. 1 - 1.1.4)

- Oficial de seguridad.
- Gerente de sistemas
- Administrador IT
- Comité de Seguridad

Proteja los datos del titular de la tarjeta (ver Anexo I, Norma PCI, req. 3,4)

Implemente medidas solidad de control de acceso (ver Anexo I, Norma PCI, req. 7, 8)

La Impresión y ensobrado automático de Estados de Cuenta Tarjetas de Crédito adoleció de ciertos controles durante su desarrollo

Del relevamiento de información realizado, observamos las siguientes situaciones:

- ✓ No se desarrolló especificaciones funcionales, ni flujos del nuevo proceso.
- ✓ No se generaron documentos/instructivos en los que se detallen los procedimientos a seguir en el nuevo proceso, así como los responsables de realizarlos antes de la puesta en producción del proceso

- ✓ No se generó matriz de riesgos del proyecto.
- ✓ No se generó reportes de control de cambios de los procesos inicialmente definidos.
- ✓ No se generó reportes de lista de necesidades y recursos.
- ✓ No se cuenta con documentación detallada de las pruebas de certificación realizadas (plan de pruebas, tipos de pruebas, sustento de la ejecución, conformidad de pruebas por parte del usuario, etc).
- ✓ No fue monitoreado por el área de Aseguramiento de Calidad de Proyectos

Cabe mencionar que cuando el proyecto entró en producción se presentaron algunos problemas originaron que se realicen cambios de emergencia y modificaciones en la arquitectura del sistema y en los procesos, por ejemplo:

- ✓ Errores en la transferencia de información desde el Servidor AIX del Banco hacia el servidor del proveedor, debido a caracteres especiales (Ñ, A acentuadas, controles de carro, etc). En la actualidad se ejecutan procesos adicionales que modifican la información que presenta estos problemas; para solucionar ésta situación se tiene previsto cambiar el servidor AIX por un servidor Windows, lo cual requiere tareas de implementación del mecanismo de transferencia del computador central al nuevo servidor, así como de la transferencia del servidor Windows al servidor de el proveedor y el Courier.

  Es importante mencionar que el cifrado de la información que se envía al proveedor se realiza mediante el software PGP utilizando una licencia libre que ya ha caducado y que para adquirirla se debe tener definido el tipo de servidor en donde se va a instalar.
- ✓ No se han definido controles para asegurar la transferencia de información desde el computador central al Servidor AIX y del Servidor AIX al servidor Ibsix al cual accede al Courier.
- ✓ No es posible realizar la transferencia información de los estados de cuenta (PDF's) que debe enviar el proveedor al Banco, utilizando la VPN instalada para el proceso (debido al tamaño de la información que se requiere transmitir). Ello ha originado

que se hayan definido procedimientos alternativos, que actualmente no se encuentran formalmente documentados, tales como:

- Utilización de un disco duro externo en el cual el proveedor graba la información (encriptada y comprimida), éste es transportado hacia el Banco utilizando los servicios del Centro de Control.
- Descifrado y descompresión manual de la información registrada en el disco duro externo, por parte del personal del Centro de Cómputo para finalmente grabarlo en la red del Banco, lo que origina recarga de trabajo y dependencia de dicho personal.
- Eliminación de la información del disco duro externo por el personal de Seguridad de Información.

Adicionalmente, hemos identificado las siguientes situaciones en el proceso actual:

- Ausencia de controles de verificación de la información reportada por el proveedor referente a preformatos, impresiones, sobres, cargos.
- No se verifica que la cantidad de impresiones facturadas por el proveedor corresponda a lo realmente impreso. El control utilizado consiste en verificar que la diferencia entre la cantidad de estados de cuenta y de hojas impresas no exceda al 10% del total de estados de cuenta. Cabe indicar que no se nos proporcionó sustento de cómo se calculó este indicador de control.

✓ No se ha realizado la evaluación de riesgos operativos del proceso actual de impresión ejecutado por el proveedor. A la fecha de nuestra evaluación la División de Riesgo Operativo no había recibido solicitud alguna de parte del coordinador de riesgos de Tarjeta de Crédito para iniciar la revisión del nuevo proceso e identificar los riesgos operativos asociados.

✓ Durante el mes de noviembre y diciembre, los indicadores de tiempo definidos para medir el proceso no superaron los tiempos definidos como óptimos. Cabe indicar que aún no se tenían calculados los indicadores de tiempo del mes de Enero.

Tabla 2: Matriz de Riesgos

1. Evaluar efectividad de las políticas y procedimientos para la administración de los accesos en todos los ambientes del computador central

PO3.4 Estándares tecnológicos				
• Evaluar la existencia de estándares relacionado a los accesos de los sistemas de información. • Comprobar si se viene midiendo el cumplimiento de los mismos. Documentación: • Estándares de TI (Pedido Nro.1 – pto. 4) *Comentarios del Auditor* **Existen estábdares, sin embargo se encontró incumplimiento de algunos estándares – Obs 2 (P.Trab. R4)**	**MEDIO**	AQ	E1.81/86 E1.87/96 E1.97/108	

PO4.14 Políticas y procedimientos para personal contratado				
Evaluar si las políticas y procedimientos de personal contratado permiten controlar las actividades de los consultores y otro personal contratado por la función de TI para garantizar la protección de los activos de información de la empresa y satisfacer los requerimientos contractuales. Documentación: • Políticas y procedimientos de personal contratado (División de Gestión y Desarrollo Humano - GDH). Información obtenida de la evaluación de Controles Generales. *Comentarios del Auditor* **Si bien existen procedimientos de solicitud de acceso, no se realiza un monitoreo para la depuración de estos – Obs 4.a - (P.Trab. R5)**	**MEDIO**	AQ	E2.1.48/49 E2.2.108	

DS5.2 Plan de seguridad de TI				
Verificar que los requerimientos de información del negocio, la configuración de TI, **los planes de acción del riesgo de la información** y la cultura sobre la seguridad en la información se trasladen a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios. Documentación: • Plan de Trabajo 2008 del área de Seguridad de Información (Pedido Nro.1 – pto.2) • Circular G-105-2002 – Art. 5 Administración de la Seguridad de Información. *Comentarios del Auditor* **No se pudo determinar la existencia de un plan general de seguridad de la información, que contemple en forma integral los riesgos que podrían impactar a las distintas plataformas tecnológicas con que cuenta el Banco – Obs. 1 c - - (P.Trab. R3).** **Adicionalmente se hizo unas sugerencias para que las consideren en su oportunidad. (P.Trab. R11)**	**MEDIO**	AQ	E1.4/11	

PROCEDIMIENTO	RIES	RES	W/P	ORD

DS5.3 Administración de identidad; DS5.4 Administración de cuentas del usuario				
• Comprobar si las políticas y procedimientos indican que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) sean identificados de manera única. Los derechos de acceso del usuario a sistemas y datos estén alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso. • Validar que el procedimiento garantice que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Verificar si el procedimiento de accesos contempla la revisión regular de todas las cuentas y los privilegios asociados por parte de las gerencias responsables de los productos. Documentación: • Manual de Procesos de la Administración de la Seguridad de Información (Hoja de Ruta) – Cap.5. Procedimientos relativos a la Operación de la Seguridad de Información • Manual de Administración de la Seguridad de Información – 3. Políticas específicas de Seguridad de Información – 3.1 Políticas de Control de Accesos. • Circular G-105-2002 – Art.7. Aspectos de la Seguridad de Información – 7.1.Seguridad Lógica. • Políticas y procedimientos para la definición de perfiles y usuarios RACF e IB00 (Pedido Nro.1 – pto. 5.1) *Comentarios del Auditor* **Existen políticas, pero no existe monitoreo para la depuración de los mismos. Obs 3 y 4 - (P.Trab. R4 y R5)**	**MEDIO**	AQ	E1.23/39 NI.17/40 E1.61/73 E2.1.45/47 E2.1.50 E2.2.105/107 E2.2.109	

PROCEDIMIENTO	RIES	RES	W/P	ORD

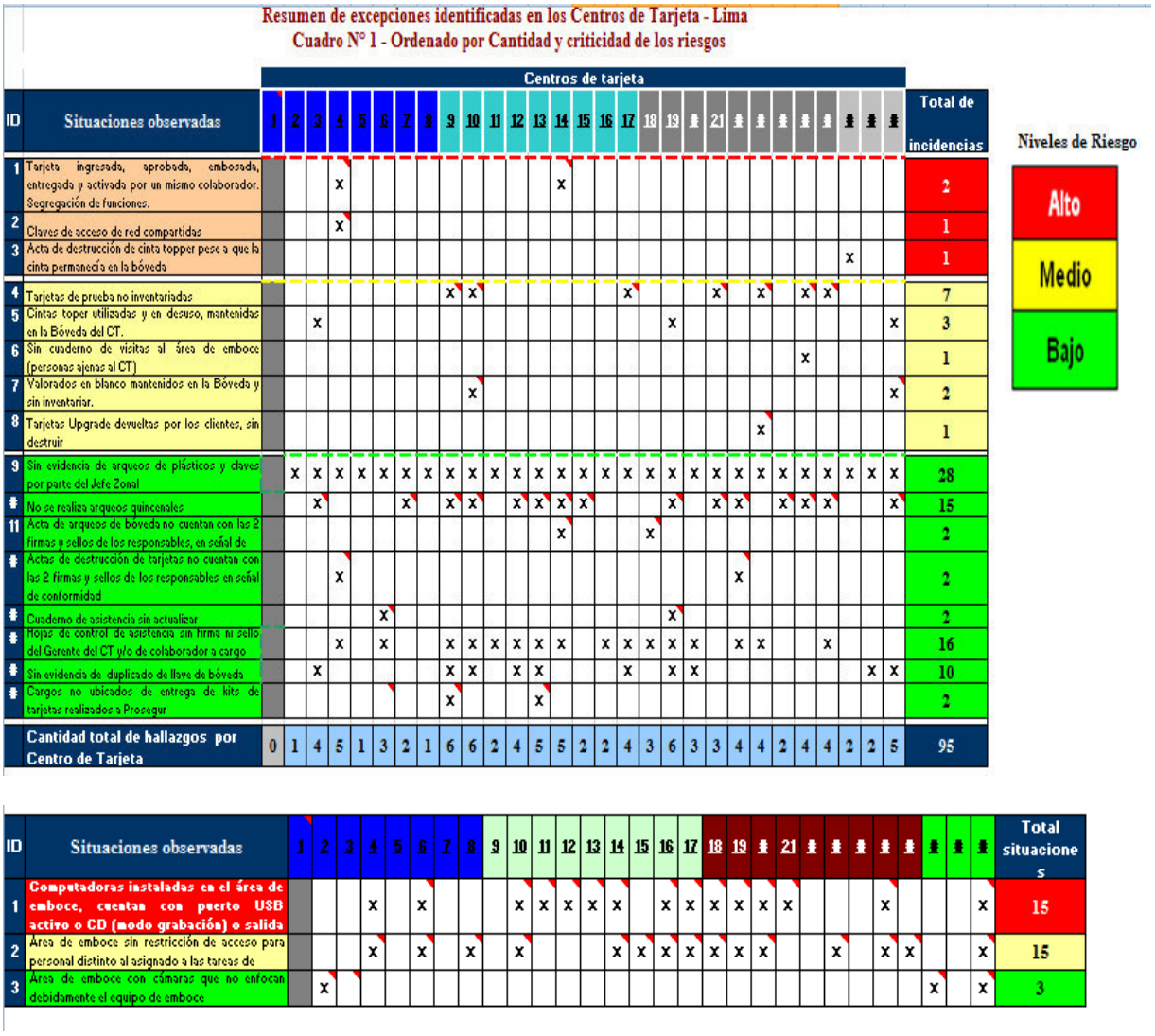
2. Revisar la configuración del sistema de seguridad Resource Access Control Facility (RACF) y del sistema de control de acceso IB00.

AI6.1 Estándares y procedimientos para cambios				
• Comprobar la existencia de procedimientos para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a procedimientos, procesos, **parámetros de sistema** / servicio de las diferentes plataformas del Banco. • Comprobar la existencia de mecanismos de control que permitan identificar cambios no autorizados en la configuración de componentes. Evaluar si existe una herramienta para el control y manejo de los cambios en las diferentes plataformas, así mismo, verificar si este cuenta con las medidas de seguridad (acceso) y controles adecuados (niveles de autorización) para actualizaciones y consultas. • Mantener pistas de auditoria de los resultados previos y posteriores al cambio. Documentación: • Manual de Procesos de la Administración de la Seguridad de Información (Hoja de Ruta) – Cap.4. Estándares Técnicos relativos a la Seguridad de Información – Configuración del Sistema. • Manual de Administración de la Seguridad de Información – 3. Políticas especificas de Seguridad de Información – 3.2.5. Seguridad para la implantación y mantenimiento de infraestructura tecnológica. *Comentarios del Auditor*	**MEDIO**	JS	E1.23/39 NI.17/40	

AI6.3 Cambios de emergencia; AI6.4 Seguimiento y reporte del estatus de cambio; AI6.5 Cierre y documentación del cambio				
• Verificar si existen procedimientos para autorizar cambios de emergencia que no sigan el proceso de cambio establecido, así como la documentación y pruebas que se deben efectuar. Revisar el cumplimiento de dichos procedimientos para una muestra en Host: RACF, OS/390, CICS, DB2. • Comprobar si existe un sistema de seguimiento y reporte que permita mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio. • Evaluar los procedimientos que se viene aplicando para la actualización de los sistemas, de los procedimientos y la documentación de sustento después de haberse realizado dichos cambios • Verificar si existe un procedimiento de revisión de los cambios que permitan garantizar la implantación completa de los mismos. Documentación: • Políticas y procedimientos (Pedido Nro.1 – pto. 12) • Relación de las actualizaciones realizadas durante los últimos seis(6) meses en el Mainframe al software base (Sistema Operativo, CICS, DB2, RACF). Versión y Fixes. (Pedido Nro.1 – pto. 13) *Comentarios del Auditor*	**MEDIO**	JS		

PROCEDIMIENTO	RIES	RES	W/P	ORD
DS5.3 Administración de identidad; DS5.4 Administración de cuentas del usuario				
• Verificar que los derechos de acceso del usuario a sistemas y datos desde RACF e IB00 estén alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso. • Comprobar si dentro de los procedimientos de accesos al RACF e IB00 se contempla la revisión regular de todas las cuentas y los privilegios asociados por parte de las gerencias responsables de los productos. Documentación: • Manual de Procesos de la Administración de la Seguridad de Información (Hoja de Ruta) – Cap.5. Procedimientos relativos a la Operación de la Seguridad de Información • Manual de Administración de la Seguridad de Información – 3. Políticas específicas de Seguridad de Información – 3.1 Políticas de Control de Accesos. • Circular G-105-2002 – Art.7. Aspectos de la Seguridad de Información – 7.1.Seguridad Lógica • Políticas y procedimientos para la definición de perfiles y usuarios RACF e IB00 (Pedido Nro.1 – pto. 5.1) • Aplicación de Programa de Trabajo de RACF e IB00. *Comentarios del Auditor* **Existen políticas, pero no existe monitoreo para la depuración de los mismos. Obs 3 y 4 - (P.Trab. R4 y R5)**	**ALTO**	JS	E1.23/39 NI.17/40 E1.61/73 E2.1.45/47 E2.1.50 E2.2.105/107 E2.2.109	
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad				
• Comprobar si se identifican, monitorean y reportan las vulnerabilidades e incidentes de Seguridad del RACF. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. • Verificar si se viene monitoreando los accesos otorgados al IB00 • Evaluar si se mantiene pistas de auditoria. Documentación: • Manual de Procesos de la Administración de la Seguridad de Información (Hoja de Ruta) – Cap.5. Procedimientos relativos a la Operación de la Seguridad de Información – 5.1.7. Depuración de Usuarios. • Manual de Administración de la Seguridad de Información – 3. Políticas específicas de Seguridad de Información – 3.1.2.b. Asignación de Perfiles de Acceso. • Manual de Administración de la Seguridad de Información – 3. Políticas específicas de Seguridad de Información – 3.3. Valores Predeterminados del sistema. • Herramientas tecnológicas que utiliza el área para el desarrollo de sus labores. Indicar la relación con los procesos y/o funciones que realizan actualmente. (Pedido Nro.1 – pto. 3) • Políticas y procedimientos para el monitoreo del RACF e IB00 (Pedido Nro.1 – pto. 5.2 y 5..3) • Relación de Reportes Panagon que muestran información de RACF e IB00 (indicando código del reporte, descripción y utilización). (Pedido Nro.1 – pto. 8). *Comentarios del Auditor* **No se viene efectuando un adecuado monitoreo de la seguridad en el computador central. Obs. 2 - (P.Trab. R4)**	**ALTO**	JS	E1.23/39 NI.17/40 E1.61/73 E1.77 E1.78	

Seguridad Física (ver Anexo I, Norma PCI, req. 9)



Resumen de excepciones identificadas en los Centros de Tarjeta - Lima
Cuadro N° 1 - Ordenado por Cantidad y criticidad de los riesgos

ID	Situaciones observadas	Centros de tarjeta																												Total de incidencias
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	#	21	#	#	#	#	#	#	#	
1	Tarjeta ingresada, aprobada, embosada, entregada y activada por un mismo colaborador. Segregación de funciones.				x										x															2
2	Claves de acceso de red compartidas				x																									1
3	Acta de destrucción de cinta topper pese a que la cinta permanecía en la bóveda																										x			1
4	Tarjetas de prueba no inventariadas									x	x							x				x		x		x	x			7
5	Cintas topper utilizadas y en desuso, mantenidas en la Bóveda del CT.			x																x										x	3
6	Sin cuaderno de visitas al área de emboce (personas ajenas al CT)																									x					1
7	Valorados en blanco mantenidos en la Bóveda y sin inventariar.										x																			x	2
8	Tarjetas Upgrade devueltas por los clientes, sin destruir																								x						1
9	Sin evidencia de arqueos de plásticos y claves por parte del Jefe Zonal		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	28
#	No se realiza arqueos quincenales			x			x			x	x		x	x	x	x				x		x	x		x	x	x			x	15
11	Acta de arqueos de bóveda no cuentan con las 2 firmas y sellos de los responsables, en señal de														x				x												2
#	Actas de destrucción de tarjetas no cuentan con las 2 firmas y sellos de los responsables en señal de conformidad				x																	x									2
#	Cuaderno de asistencia sin actualizar					x														x											2
#	Hojas de control de asistencia sin firma ni sello del Gerente del CT y/o de colaborador a cargo				x		x			x	x	x	x	x	x		x	x	x	x	x		x	x			x				16
#	Sin evidencia de duplicado de llave de bóveda			x						x	x		x	x					x		x	x							x	x	10
#	Cargos no ubicados de entrega de kits de tarjetas realizados a Prosegur									x				x																	2
	Cantidad total de hallazgos por Centro de Tarjeta	0	1	4	5	1	3	2	1	6	6	2	4	5	5	2	2	4	3	6	3	3	4	4	2	4	4	2	2	5	95

Niveles de Riesgo

Alto

Medio

Bajo

ID	Situaciones observadas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	#	21	#	#	#	#	#	#	#	Total situaciones
1	Computadoras instaladas en el área de emboce, cuentan con puerto USB activo o CD (modo grabación) o salida				x		x				x	x	x	x	x		x	x	x	x	x	x				x				x	15
2	Área de emboce sin restricción de acceso para personal distinto al asignado a las tareas de				x		x		x		x					x	x	x	x	x	x			x		x	x			x	15
3	Área de emboce con cámaras que no enfocan debidamente el equipo de emboce		x																									x		x	3

	Riesgos identificados
Muy Buena (MB)	Ninguno o muy pocos Riesgos Bajos (incluso, algunos no atribuibles al CT)
Buena (B)	Máximo 3 riesgos Medios o Bajos
Aceptable (A)	Más de 3 riesgos Medios o Bajos ó 1 riesgo Alto
Deficiente (D)	Más de 1 riesgo Alto

Figura 14: Estructura seguridad física en centros de Tarjeta

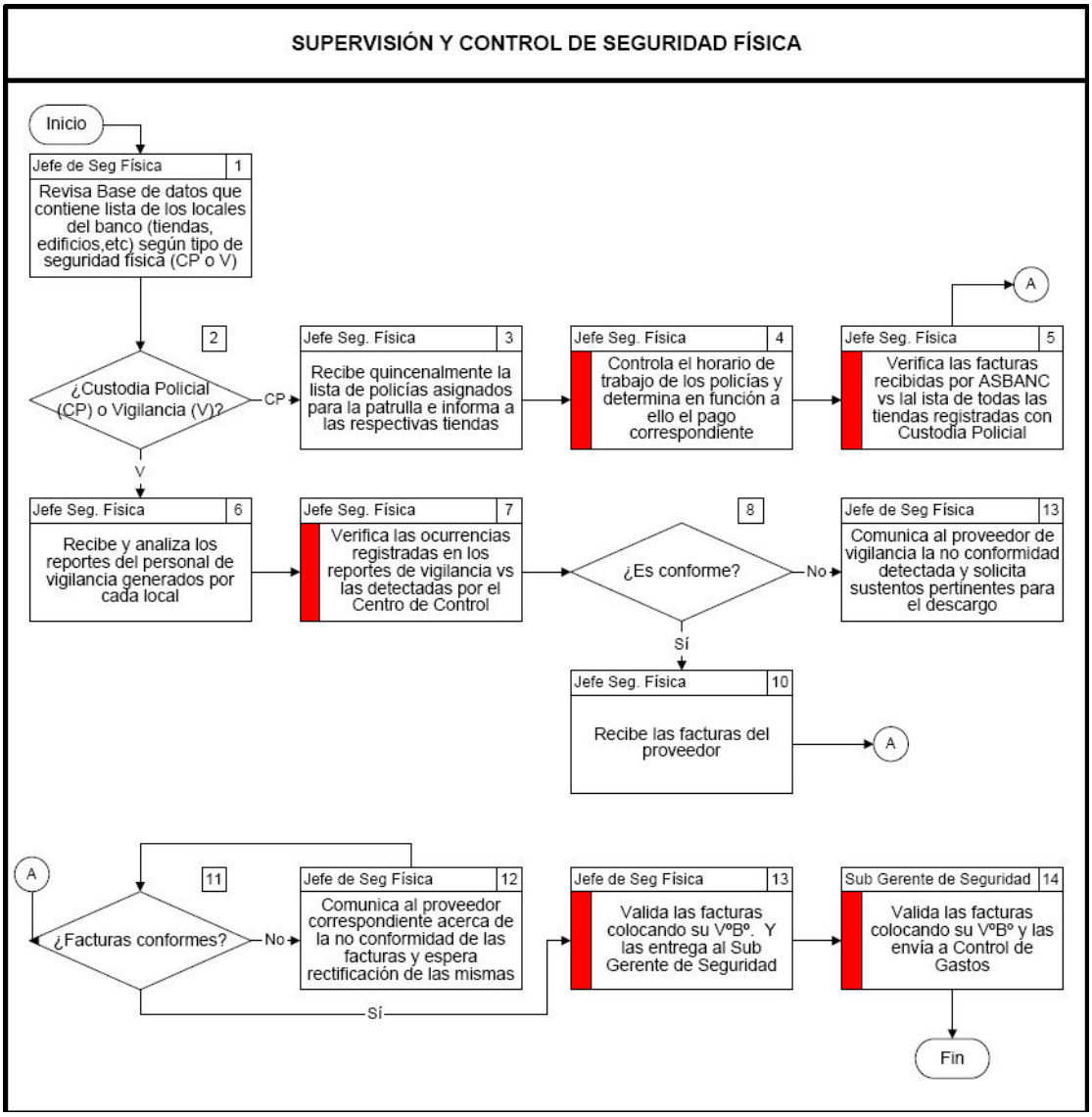


Figura 15: Proceso de Control y Seguridad Física

Mantenga una política de Seguridad de Información (Ver Anexo I, Norma PCI, req. 12)

El proceso de impresión de estados de cuenta de tarjeta de crédito, presenta algunos riesgos relacionados a la seguridad de información.

Citamos:

- No se ha establecido la realización de visitas periódicas de inspección por parte de entidad financiera a las instalaciones del proveedor, que permitan verificar, entre otros: i) la eliminación de los archivos con información de los

estados de cuenta en sus equipos (servidores y PC's), así como de archivos con información de pistas de auditoría (léase, archivos log) de los procesos, ii) los usuarios registrados y accesos que mantienen en los equipos utilizados en el proceso, iii) los controles para el procesamiento y protección (confidencialidad e integridad) de la información del Banco.

- No se tiene evidencia de procedimientos documentados y formalizados para la custodia y cambio periódico de las llaves pública y privada utilizadas para la encripción y desencripción de la información enviada y recibida entre entidad financiera y proveedor
- Proveedor no cuenta con un ambiente de prueba en sus instalaciones. Si bien, el banco cuenta con un ambiente de prueba en el que se certifican las modificaciones a los procesos ejecutados en el Banco, los archivos utilizados para dichas pruebas llegan al ambiente de producción del proveedor, lo cual podría originar errores en la identificación de los archivos y contraviene las prácticas sanas de control.
- 10 usuarios del Banco (5 con acceso de lectura/ejecución y 5 con acceso de lectura/ejecución/modificación), con acceso innecesario a las carpetas de red utilizadas para la carga y visualización de estados de cuenta en el aplicativo Visualización de Estados de Cuenta (VEC).
- 8 observaciones reportadas por Seguridad de Información que se encuentran pendientes de implementar por parte de proveedor
- Otras situaciones de riesgo (identificadas en las instalaciones de proveedor durante nuestra visita): i)las cámaras de seguridad instaladas en los ambientes donde se realiza el proceso no son monitoreadas, ii)cables de comunicación que se encuentran expuestos al medio ambiente (dentro de canaletas de metal abiertas) en el pasadizo del segundo piso, ingresando a la sala de servidores en este estado, iii) desde el mes de diciembre no viene realizándose la destrucción de mermas (impresiones dañadas de estados de cuenta, sobres, formatos, etc.); al respecto nos informaron que no existe un procedimiento formal y documentado para ésta actividad, iv)Usuarios de tipo

"operador", con acceso a los servidores de recepción de información (Servidor FTP - Linux) y de procesamiento de estados de cuenta (Servidor Doc1 - Windows-) son compartidos por más de una persona, al respecto nos informaron que ello se debe a que existen dos turnos de operación, v.) El equipo (PC) utilizado para la recepción de información tiene instalado y habilitado el correo electrónico, vi.)El servidor de impresión tiene definido un único usuario (de tipo "guest") para la ejecución de las impresiones, no obstante existen 9 operarios de impresión, ello no permite identificar individualmente en el log de dicho servidor las acciones realizadas por este personal.

Tabla 3: Observaciones en Seguridad Física

N°	RECOMENDACIONES	FECHA ESTIMADA	ESTADO
1	Software que deje un log del uso de los dispositivos(puertos USB en las PC´s de los operadores)	15/02/2010	Vencida
2	Habilitación de auditorías de carpetas	30/01/2010	Vencida. Implementación por falta de espacio en el servidor.
3	Cámaras de Seguridad y separación de ambientes en sala de impresión	30/01/2010	Superada
4	Rol de auditor y listados de las actividades, funciones y responsabilidades(Descripción del puesto)	30/01/2010	Superada
5	Informes pendientes: Permisos a nivel de servidores y de aplicación / Permisos PDF / Configuración de Doc1 / Árbol de carpetas en DOC1 / Controles en el intercambio de información y la transición en el procesamiento.	15/01/2010	Superada

7	Adquisición de una lectora adicional de código de barras	30/01/2010	Vencida
8	Configurar perfiles para la administración local del equipo: Deshabilitar opción de escritorio y conexión remota / Hardening aplica a las estaciones / Deshabilitar servicios que no se usen / Deshabilitar carpetas-archivos compartidos	28/02/2010	Vencida

Desarrolle un programa de administración de vulnerabilidad (ver Anexo I, Norma PCI, req.5, 6)

El análisis de vulnerabilidades que se realiza consta de 2 partes, análisis de vulnerabilidad del sistema operativo y análisis de vulnerabilidad de código.

Análisis de vulnerabilidad del Sistema Operativo

Se realiza utilizando una herramienta que analiza los puertos abiertos, protocolos utilizados, servicios iniciados, información expuesta del servidor, etc, el informe obtenido, cataloga las vulnerabilidades de la siguiente forma:

Open Ports	Puertos abiertos en el servidor
Low	Vulnerabilidades de riesgo bajo
Médium	Vulnerabilidades de riesgo medio
High	Vulnerabilidades de riesgo alto

Este análisis se realiza sobre servidores o dispositivo de networking, realizándose usualmente sobre equipos y servicios que se van a exponer en la DMZ con la finalidad de disminuir el riesgo de intrusión en los equipos.

Análisis de vulnerabilidad del Código en Servidores Web

La herramienta que usamos es Acunetix Web Vulnerability Scanner (Enterprice Edition) y realiza análisis de vulnerabilidades del código de programación de la Web como por ejemplo:

SQL Inyection

Es una vulnerabilidad informática en el nivel de la validación de las entradas a la base de datos de una aplicación. Una inyección SQL sucede cuando se inserta o "inyecta" un código SQL "invasor" dentro de otro código SQL para alterar su funcionamiento normal, y hacer que se ejecute maliciosamente el código "invasor" en la base de datos.

Cross Site Scripting (XSS)

Es un ataque basado en explotar vulnerabilidades del sistema de validación de HTML incrustado. Estos errores se pueden encontrar en cualquier aplicación HTML, no se limita a sitios web, ya que puede haber aplicaciones locales vulnerables a XSS, o incluso el navegador en sí. El problema está en que normalmente no se validan correctamente los datos de entrada que son usados en cierta aplicación.

El informe obtenido, cataloga las vulnerabilidades de la siguiente forma:

Informational	Vulnerabilidades informativas, que no representan ningún riesgo.
Low	Vulnerabilidades de riesgo bajo.
Médium	Vulnerabilidades de riesgo medio.
High	Vulnerabilidades de riesgo alto.

En la hoja Excel que se adjunta se muestra lo siguiente:

Acunetix(Resumen): Esta hoja muestra el resumen del análisis de vulnerabilidades de código realizado en los servidores y en las fechas que se indican, los informes fueron enviados a la persona que solicitó el análisis, en el caso de las páginas del banco, este año se ha realizado periódicamente, en los otros casos, cuando se va a lanzar una nueva página WEB. Cuando se envía el reporte, se solicita que antes de pasar a producción las páginas deben mitigarse por lo menos las vulnerabilidades identificadas con nivel Alto.

Estadística Test de Penetración(Ethical hacking)

Tabla 4: Estadísticas de Ethical Hacking

Banco.com.pe	xx/xx/xxxx	xx/xx/xxxx	xx/xx/xxxx	xx/xx/xxxx	xx/xx/xxxx
High	185	28	59	84	148
Medium	9	1	2	3	3
Low	97	98	68	70	90
Informational	306	214	220	221	221
Total alerts found	597	341	349	378	462

Banco1	xx/xx/xxxx	06/03/2008	17/04/2008
High	52	50	0
Medium	3	2	0
Low	97	82	9
Informational	210	156	103
Total alerts found	362	290	112

ATM	xx/xx/xxxx	18/01/2008	06/03/2008	17/04/2008
High	0	0	0	0
Medium	0	0	0	0
Low	10	9	9	9
Informational	25	27	29	29
Total alerts found	35	36	38	38

http://ibuatexcelsys:8	xx/xx/xxxx	05/06/2009	06/06/2009	07/06/2009	17/01/2009	06/03/2009	17/04/2009	31/07/2009
High	0	0	0	0	306	331	331	28
Medium	0	8	0	8	6	7	7	3
Low	98	99	110	109	204	209	204	106
Informational	1	151	0	66	70	70	70	1
Total alerts found	99	258	110	183	586	617	612	138

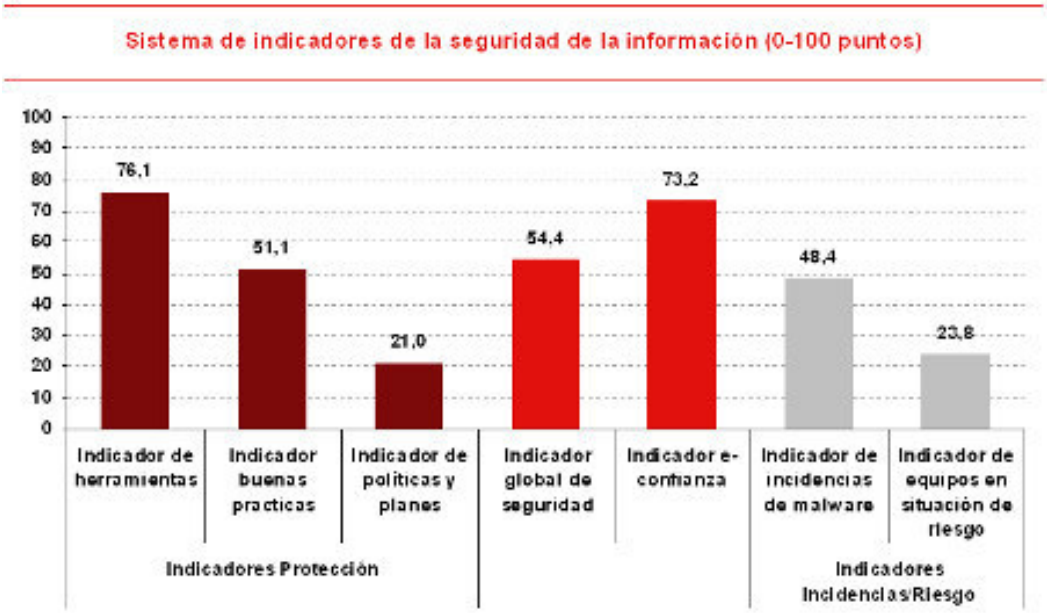


Figura 16: Indicadores de Seguridad de Indormación

Cuadro de valoración de atributos de madurez del marco COBIT efectuado al proceso tarjeta de crédito en base al cumplimiento de los requisitos de la Norma PCI

Norma PCI Req./ COBIT DS5, DS12	Modelo de Madurez (0, 1, 2, 3, 4, 5)	Conciencia y Comunicación	Políticas, estándares y procedimientos	Herramientas y automatización	Habilidades y Experiencia	Responsabilidades y Rendición de cuentas	Establecimiento y Medición de Metas
Req. 1 / DS5.10	4	4	3	4	4	5	3
Req. 2 / DS5.10	3	3	4	3	4	3	2
Req. 3 / DS5.8, 11	3	3	4	4	4	3	2
Req. 4 / DS5.8, 11	4	4	4	4	5	4	2
Req. 5 / DS5.9	3	4	4	3	4	4	1
Req. 6 / DS5.7, 9	4	3	4	4	4	4	3
Req. 7/ DS5.4	4	3	3	4	4	4	3
Req. 8 / DS5.3	4	4	5	4	5	5	1
Req. 9 / DS12.3	3	3	4	4	4	3	1
Req. 10 / DS5.10, 6, 11	4	3	4	4	4	3	2
Req. 11 / DS5.10, 6, 11	3	3	4	4	3	3	2
Req. 12 / DS5.2, 1	4	4	4	4	4	3	1

Capítulo 5: Método para la gestión de los riesgos de fraude

La metodología descrita en este documento tiene por finalidad detallar los lineamientos a ser considerados por el Banco, para la gestión de los riesgos de fraude que pudieran tener algún impacto en sus objetivos estratégicos, en su imagen, en su patrimonio, en sus clientes o en sus socios de negocios.

La aplicación de esta metodología, busca ser el punto de inicio para que el Banco logre una gestión integral adecuada de todas las fases que conforman la administración de los riesgos de fraude, lo que comprende: i) el establecimiento de un marco de control efectivo; ii) criterios seguidos para la prevención de los riesgos de fraude; iii) estrategias para la detección de fraudes; iv) lineamientos para la investigación de fraudes; v) estrategias desarrolladas para recuperación de eventos de fraude.

5.1 DEFINICIONES PRELIMINARES

Método de gestión de los riesgos de fraude

Documento que tiene por finalidad establecer los lineamientos, políticas, responsabilidades y procedimientos que deberían ser considerados por todas las áreas y colaboradores del Banco, en los temas relacionados con la gestión de los riesgos de fraude.

Riesgo

- La probabilidad de ocurrencia de un evento (esperado o fortuito) que podría tener un impacto negativo en los objetivos y metas del negocio.

- Comúnmente, responde a las preguntas: ¿qué puede ir mal? ¿qué puede fallar?

Fraude

- Engaño que se realiza eludiendo obligaciones legales o usurpando derechos de otros, con la finalidad de obtener un beneficio financiero.

- Acto cumplido intencionalmente con la finalidad de vulnerar los derechos e intereses de otros.

Control

- Políticas, procedimientos y acciones en general, adoptadas por el Banco para prevenir, detectar y/o mitigar el impacto ocasionado por un evento adverso.

- Procedimiento o actividad diseñados para prevenir o detectar errores que afecten algún proceso del negocio y/o a los registros contables.

Monitoreo

Toda actividad diseñada con el propósito de verificar que un proceso, actividad o tarea se viene realizando conforme a lo diseñado y previsto al momento de su implantación.

Recuperación

Conjunto de actividades, políticas y procedimientos establecidos por el Banco con la finalidad de:

- Minimizar al máximo la probabilidad de ocurrencia de un nuevo fraude bajo las mismas condiciones del fraude detectado. Corresponde a la fase de implementación de controles en los procesos de negocios comprometidos por el fraude.

- Recuperar los bienes y/o activos que pudieran haber sido comprometidos con ocasión de un fraude.

- Mantener o recuperar su buena imagen ante sus clientes, colaboradores, socios de negocios, entes reguladores y accionistas, luego de haberse detectado (y eventualmente, hecho público) un fraude.

- Resolver (interna y externamente) relaciones contractuales, legales y/o de litigio con colaboradores, socios de negocios y terceros, según corresponda, involucrados en hechos de fraude.

5.2 TIPOS DE FRAUDE CONSIDERADOS

5.2.1 Fuentes de amenazas de fraude incluidas en la metodología

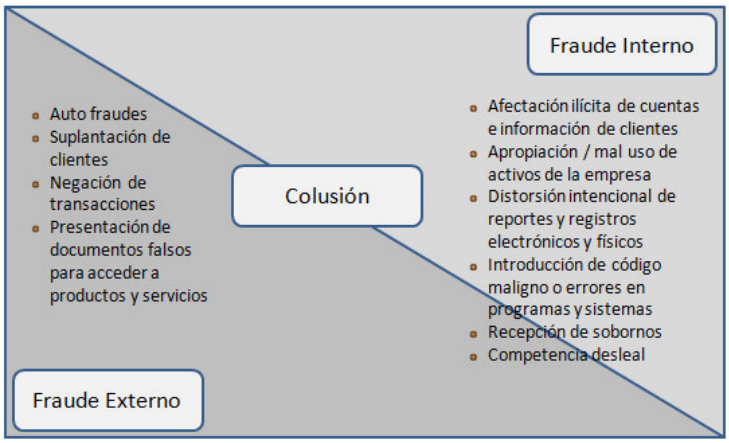
La magnitud de la amenaza de fraude es sólo una de las dimensiones de la problemática de fraude en el Banco, siendo necesario, para una mejor gestión antifraude, considerar las distintas fuentes de donde puede provenir un fraude.

- **Fuentes Internas:** i) Colaboradores que acceden a información confidencial de clientes o del Banco para la comisión de un fraude; ii) distorsión deliberada en reportes de gestión (ejemplo: adulteración de indicadores de desempeño y logro de metas); iii) alteración de programas de cómputo para generar un beneficio propio o de terceros; iv) alteración de registros electrónicos (contables y operativos); v) competencia desleal; vi) mal uso de los activos del Banco; vii) recepción de sobornos; viii) destrucción / apropiación ilícita de activos del Banco; ix) aprovechamiento de errores/ fallas en los procesos operativos y de sistemas del Banco; x) cualquier violación intencional a las normas vigentes (internas y externas) o código de conducta establecido por el

Banco con la finalidad de lograr un beneficio financiero en perjuicio de los intereses del Banco; entre otros.

- **Fuentes Externas:** i) falsificación o duplicación de facturas por parte de algún proveedor del Banco; ii) Acuerdo de competidores para establecer tarifas de productos y servicios fuera del mercado, con la finalidad de perjudicar al Banco; iii) clientes que pretenden desconocer una o más transacciones relacionadas con tarjeta de crédito; iv) esquemas de auto fraude por parte de clientes del Banco; v) Robo de identidad, suplantación y otras modalidades perpetradas por Hackers; entre otros.

El Banco reconoce que puede existir una combinación de fuentes internas y externas en la comisión de un fraude. El siguiente gráfico resume lo anterior:



5.2.2 Factores de riesgo de fraude

La presente metodología considera que los factores de riesgo de fraude se dividen en dos (2) grupos:

Genéricos: Cuando el riesgo de fraude no depende de un individuo o grupo de individuos al interior del Banco, sino que corresponden a fallas en su

estructura general de control. Ejemplos: Ausencia de autonomías para: pagos a proveedores; desembolso de créditos; emisión de cheques; etc.

Individuales: Cuando el riesgo de fraude varía de persona a persona. Es más difícil de controlar al interior del Banco. Se refieren principalmente a la **Moral** y la **Motivación** de cada individuo. Ejemplos: Ausencia o incumplimiento de políticas de rotación; concentración de funciones; etc.

5.2.3 Criterios a seguir para contrarrestar los factores de riesgo de fraude

De acuerdo a las mejores prácticas y estándares para la prevención y tratamiento del riesgo de fraude, se tiene los siguientes criterios:

- Seleccionar niveles aceptables de riesgo de fraude:
  - ✓ Se acepta el hecho que el riesgo de fraude no puede ser completamente eliminado.
  - ✓ El Banco considera que en cada caso debe prevalecer el análisis costo-beneficio en la decisión de mitigar un riesgo de fraude.
  - ✓ El análisis debe incluir también el estudio de probabilidad de ocurrencia del fraude y las oportunidades para su comisión.
- Desarrollar e implementar controles internos:
  - ✓ Controles básicos, mínimos e indispensables
  - ✓ Supervisión de controles
  - ✓ Auditoria
- Promover un ambiente ético:
  - ✓ Código de Ética
  - ✓ Código de Conducta
- Adoptar una política de Seguros (ejemplo: Póliza de deshonestidad)
- Desarrollar, implementar y mantener una estructura adecuada para la seguridad en el ambiente computarizado

5.2.4 Algunos perfiles posibles para un perpetrador de fraude

- Individuos con problemas personales (emocionales y financieros)
- Individuos con serios problemas de actitud y adaptación al ambiente de trabajo
- Individuos muy impulsivos y que se muestran reacios a rechazar cualquier tipo de acción que les signifique obtener algún dinero extra
- Personas con una presión muy alta para cumplir con las metas de negocio que les son impuestas

5.3 ESQUEMA DE LA METODOLOGÍA DE GESTIÓN DE LOS RIESGOS DE FRAUDE

- **Prevención:** Políticas y procedimientos establecidos por el Banco para prevenir en forma razonable la ocurrencia de fraudes.

- **Detección:** Políticas y procedimientos establecidos por el Banco para permitir la identificación oportuna de fraudes.

- **Investigación:** Criterios y pasos a seguir para investigar la naturaleza, oportunidad, impacto y responsabilidades ante la detección de un fraude.

- **Recuperación:** Lineamientos y acciones definidos por el Banco para restablecer el normal y correcto funcionamiento de un proceso, producto o servicio (en el sentido más amplio), así como para revertir el impacto de un fraude y gestionar acciones de naturaleza laboral y legal.

5.4 COMPONENTES DE LA METODO

La aplicación de la estrategia desarrollada para el Banco, requiere que se tome en cuenta los diversos componentes de la metodología que la sustenta y que son descritos a continuación:

5.4.1 Controles internos

Esta metodología es aplicable en el marco de un sistema de control interno eficaz y eficiente, el cual comprende, entre otros aspectos, lo siguiente:

- **Definición de objetivos de control interno**

  El Banco debe contar con una estructura de control interno confiable que le permita mantener en niveles razonables la posibilidad e impacto de un eventual fraude. Es el primer nivel en el sistema de control interno del Banco.

- **Controles Básicos**: La metodología desarrollada considera tres (3) categorías básicas de control interno a ser aplicados: i) Accesos; ii) Descripciones de puestos y iii) Análisis y reconciliación contable.

- **Supervisión**: Los procesos del negocio deben contar con mecanismos de supervisión, especialmente en aquellos casos que el Banco considera que existe un mayor nivel de riesgo.

  La supervisión es vital y representa una buena forma de prevenir el riesgo de fraude; siendo el segundo nivel del sistema de control interno del Banco. Se considerará dos componentes:

  - ✓ *Conciencia de fraude*: los colaboradores del Banco deberán estar conscientes que siempre existe la posibilidad de un fraude y, por lo tanto, deberán estar alertas y alineados con las directrices establecidas por el Banco en materia de prevención del fraude.

  - ✓ *Aprobación, revisión, doble chequeo y reproceso*: en este caso, deberá verificarse que existan y sean aplicadas buenas prácticas de control, que incluyan, entre otros, lo

siguiente: i) segregación de funciones; ii) control de valorados; iii) cuadres diarios de efectivo; iv) verificación periódica de accesos a dinero, documentos valorados, activos de información (programas, datos y reportes), etc.

- **Auditoría**: Desde la perspectiva de prevención de fraudes, la auditoría representa el tercer nivel del sistema de control interno del Banco.

  - ✓ *Auditoría Interna*: De acuerdo al Consejo para la Práctica 1210.A2-1: Identificación del Fraude[1] los auditores internos deberán tener suficientes conocimientos para identificar los indicadores de fraude; sin embargo, no se espera que éstos tengan conocimientos similares a los de aquellas personas cuya responsabilidad principal es la detección e investigación de fraudes.

  - ✓ *Auditoría Externa*: Orientadas a la revisión de estados financieros y otros aspectos en forma independiente. Aplican los criterios descritos en la Declaración sobre Estándares de Auditoría (SAS, por sus iniciales en inglés) N° 99 "Consideraciones de Fraude en una auditoría de estados financieros"; esto es: si un fraude es suficientemente material como para afectar los estados financieros de el Banco, y el auditor emite una opinión sobre dichos estados financieros, entonces los procedimientos de auditoría deberían haber sido diseñados para descubrirlo.

---

[1] The Institute of Internal Auditors (IIA), "Manual de Auditoría Interna, Primera Edición 2006", Págs. 235 - 238

5.4.2 Ambiente Ético

Un componente crítico en toda metodología de gestión de los riesgos de fraude, está constituido por el ambiente ético al interior del Banco. Para promover dicho ambiente ético debería considerarse lo siguiente:

- *Tono de la Gerencia*: Los colaboradores del Banco ven en el actuar de la Alta Dirección un claro alineamiento con las declaraciones y políticas para el comportamiento ético de todos los integrantes de la organización.

- *Código de Ética*: Debería incluir, entre otros:
  - ✓Código de Conducta Organizacional
  - ✓Conducta de los colaboradores
  - ✓Conflicto de intereses
  - ✓Actividades profesionales adicionales a las prestadas en el Banco
  - ✓Relaciones con clientes y proveedores
  - ✓Políticas de recompensas, regalos y otros beneficios
  - ✓Privacidad y confidencialidad de las operaciones e información
  - ✓Honestidad
  - ✓Lealtad
- *Capacitación***:** Entrenamiento en temas de seguridad, comportamiento ético, prevención de fraudes y conducta frente a un evento de fraude

5.4.3 Seguro contra fraudes

Una forma en que el Banco puede protegerse ante la comisión de un fraude es la contratación de pólizas de seguro que comprendan, entre otros: Deshonestidad de empleados o Robo de empleados.

- *Actos deshonestos o fraudulentos de colaboradores*: En el contexto de esta metodología, son entendidos como actos cometidos intencionalmente por un empleado con la finalidad manifiesta de: i) originar una pérdida para el Banco; ii) obtener un beneficio financiero propio o para terceras personas u organizaciones con la voluntad del empleado.

- *Pérdidas indirectas*: el Banco podrá considerar la conveniencia de contar con una provisión por pérdidas indirectas (ej: costo de investigación del fraude; pérdida de ingresos; intereses perdidos, fondos robados; oportunidades de negocios perdidas)

5.4.4 Seguridad en el ambiente computarizado

La tecnología de información desempeña un rol importante para el Banco, consecuentemente, cualquier acto de sabotaje o fraude realizado en cualquiera de sus componentes podrá tener un impacto adverso muy significativo (ej: robo de información confidencial; integridad de los datos e información; disponibilidad de los sistemas; integridad del código fuente de programas,

scripts y parámetros de las aplicaciones). Por ello, esta metodología de gestión de los riesgos de fraude incluye la atención de los siguientes aspectos:

- Seguridad en las comunicaciones de datos (teleproceso / proceso remoto/etc.)
- Estructura de la seguridad en las instalaciones
- Disponibilidad de los sistemas
- Seguridad física
- Controles de acceso físicos y lógicos (esto es, a instalaciones y a los sistemas)
- Riesgos inherentes a equipos portátiles
- Riesgos inherentes a proveedores de servicios de desarrollo y mantenimiento de sistemas y equipos de cómputo
- Seguridad en el ambiente de redes (servidores de aplicaciones y de datos; switches/ firewalls/ hubs)
- Seguridad de accesos remotos
- Seguridad de servicios basados en telefonía e internet
- Seguridad de datos (en línea, respaldos, data distribuida, datawarehouse)
- Seguridad de bibliotecas de programas sensitivos
- Controles para cambios en programas
- Diferenciación y segregación de ambientes de trabajo en el computador central
- Promoción de programas desde el ambiente de desarrollo al de producción
- Plan de continuidad de negocios (manejo de diversos escenarios)
- Concentración de funciones en el área de sistemas
- Dependencia funcional hacia programadores y/o encargados de soporte
- Nivel de documentación de las aplicaciones
- Indicadores de performance de las aplicaciones y equipos de cómputo
- Controles sobre los equipos dados de baja o enviados a mantenimiento

5.4.5 Políticas y procedimientos

Como en todos los procesos y actividades que realiza el Banco, deberá contarse con políticas y procedimientos que en forma centralizada o a través de las distintas normas establecidas internamente, contribuyan a un proceso efectivo para la gestión de los riesgos de fraude.

5.4.6 Escenarios de riesgo de fraude

El proceso de gestión de los riesgos de fraude es continuo y varía conforme evoluciona el Banco y se desarrollan nuevos productos y servicios. También, la tecnología de información está expuesta a cambios causados por la industria de software y hardware, lo que implica el surgimiento de nuevos riesgos, los cuales requieren ser examinados con una periodicidad adecuada.

En términos generales, esta metodología considera que los escenarios de fraude deberán ser desarrollados paulatinamente y enriqueciéndose con la experiencia que el personal designado para su análisis vaya adquiriendo.

Sin perjuicio de lo anterior, sería conveniente desarrollar sub proyectos unitarios en donde se analice los diversos escenarios de riesgo para un producto o servicio que se estime se encuentra expuesto a riesgos de fraude y una vez analizado y completado (incluyendo la adopción de controles para su mitigación) continuar con el siguiente producto o servicio.

La Alta Dirección podrá designar un Líder de Proyecto quien convocará a colaboradores de otras áreas del Banco para elaborar un plan de priorización

de aquellos productos y servicios que serán examinados como sub proyectos unitarios.

5.4.7 Roles y responsabilidades

Un proceso eficiente de gestión de los riesgos de fraude requiere necesariamente el compromiso y apoyo de la Alta Dirección del Banco y la designación de roles y responsabilidades para su correcto funcionamiento.

5.4.8 Gestión del conocimiento para casos de fraude ocurridos en el Banco o en competidores

Desde que en la metodología de gestión de los riesgos de fraude se introduce el concepto de sub proyectos unitarios para el análisis de riesgos de fraude relacionados a un producto o servicio en particular, será necesario aplicar criterios similares a los que se aplica en cualquier proyecto. Ello, incluye la creación de una base de conocimientos en donde se incluya las lecciones aprendidas en cada sub proyecto.

Asimismo, como se verá en el detalle de la estructura de esta metodología, podrá resultar conveniente documentar los eventos de fraude e incorporarlos en una base de datos de pérdidas (aprovechable para fines de gestión de riesgos de operación) y diferenciando si se trata de un fraude interno o externo, o si ocurrió en el Banco o sucedió en otra organización. En este último caso, deberá dársele el tratamiento de un escenario más a considerar en la casuística del producto o servicio correspondiente, siempre y cuando sea aplicable para el Banco.

5.5 DESCRIPCIÓN DE LAS FASES QUE INTEGRAN LA GESTIÓN DE LOS RIESGOS DE FRAUDE Y LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA METODOLOGÍA

Figura 17: Controles

5.5.1 Estructura de control del riesgo de fraude: Comprende en forma general la filosofía, tono de la Gerencia, políticas y procedimientos, código de conducta, entre otros, establecidos y utilizados en el Banco para una adecuada estrategia en cuanto a la gestión de los riesgos de fraude.

Es la base sobre la cual se desarrolla la metodología. Comprende, entre otros:

- La declaración de la Visión del Banco en cuanto a la gestión eficiente de los riesgos de fraude.
- El conjunto de políticas y procedimientos establecidos por la Gerencia para el manejo de los riesgos de fraude
- El establecimiento de un marco de control y de comportamiento:
    - ✓ Código de conducta (ética)
    - ✓ Sistema de control interno
- Tono de la Gerencia

El cumplimiento de esta fase debería estar reflejado en la existencia de lo siguiente:

- ✓ Políticas y procedimientos escritos para la gestión de los riesgos de fraude
- ✓ Incorporación de criterios de prevención de fraude en los procesos administrativos, operativos y de negocios existentes en el Banco
- ✓ Manual de procesos para la gestión de los riesgos de fraude
- ✓ Existencia de roles y responsabilidades formalmente establecidos para la gestión de los riesgos de fraude
- ✓ Declaración de la Visión y Misión de el Banco en cuanto al tratamiento de los riesgos de fraude
- ✓ Existencia de la función de auditoría interna
- ✓ Creación de una Cultura de prevención del fraude
- ✓ Criterios para el logro y mantenimiento de un sistema de control interno saludable
- ✓ Programas de capacitación y orientación del personal en temas de control interno, seguridad, ética y prevención del fraude
- ✓ Otras medidas dispuestas por la Alta Dirección del Banco

5.5.2 Prevención: **Políticas y procedimientos establecidos por el Banco para prevenir en forma razonable la ocurrencia de fraudes.**

La metodología enfatiza en la conveniencia de contar con una adecuada estructura de controles preventivos (manuales, automáticos o una combinación de ambos).

La naturaleza, complejidad y alcance de los controles preventivos dependerá en gran medida del resultado de los análisis costo-beneficio (ej: resultaría poco conveniente desarrollar e implementar un control de US$10M para mitigar un riesgo de fraude de baja probabilidad de ocurrencia y con impacto estimado en US$10) y del tipo de escenario relacionado a un producto y servicio en particular.

Una relación (no excluyente) de controles preventivos a considerar en el Banco comprende lo siguiente:

- ✓ Código de ética
- ✓ Procedimientos para el reclutamiento seguro de personal
- ✓ Programas de entrenamiento y de difusión de cultura ética
- ✓ Estructura organizacional apropiada
- ✓ Procedimientos para asegurar el cumplimiento de políticas de rotación de puestos y goce anual de vacaciones
- ✓ Segregación de funciones
- ✓ Salvaguarda de activos
- ✓ Existencia de niveles de autonomía y mecanismos de control para asegurar su cumplimiento en toda el Banco
- ✓ Adecuado soporte documental para todas las operaciones

- ✓ Supervisión de las operaciones
- ✓ Controles de acceso a las instalaciones del Banco
- ✓ Controles de acceso a los sistemas computarizados y datos
- ✓ Adecuadas políticas de seguridad y administración de los recursos de tecnología
- ✓ Documentación de los sistemas y procesos
- ✓ Descripciones de puestos de trabajo
- ✓ Restricciones de seguridad para retirar información del Banco vía documentos físicos o canales electrónicos (email, internet, blackberry, USB's, etc.)
- ✓ Monitoreo del personal (ej: niveles de endeudamiento severos; estrés; agresividad, resentimiento hacia el Banco, etc.)
- ✓ Auditorías
- ✓ Evaluaciones periódicas de los riesgos de operación-Mapas de riesgo
- ✓ Consultorías

5.5.3 Detección: **Políticas y procedimientos establecidos por el Banco para permitir la identificación oportuna de fraudes.**

Los mecanismos que permitirán la detección oportuna de fraudes pueden ser algunos o combinaciones de los siguientes:

- ✓ Monitoreo del personal (ej: cambios en estilo de vida ; enriquecimiento no justificado)
- ✓ Procedimientos rutinarios para revisar variaciones en cuentas de ingresos y gastos
- ✓ Análisis de variaciones en el número, importe y antigüedad de cuentas transitorias, y monitoreo de los procedimientos de depuración
- ✓ Incorporación de reportes para el control de excepciones: i) tasas y comisiones distintas a las establecidas; ii) movimientos en cuentas

dormidas; iii) cuentas contables con saldos y movimientos ajenos a su naturaleza; iv)facturas pagadas sin orden de compra correspondiente; v)accesos a datos y programas en horario fuera de oficina o por usuarios no identificables (genéricos)

- ✓ Revisión de archivos de seguridad (log´s) del sistema
- ✓ Programa de arqueos de valores y de efectivo, aleatorios y sorpresivos
- ✓ Auditorias
- ✓ Revisiones especiales orientadas a la identificación de riesgos de fraudes
- ✓ Información proporcionada por colaboradores o clientes

🔔 **Importante**: La detección de hechos de fraude debería ser consecuencia directa de la eficacia de los controles implementados por el Banco y consistente con sus políticas de apetito y tolerancia al riesgo.

5.5.4 Investigación: **Comprende todas las actividades y criterios a seguir por el Banco, con la finalidad de esclarecer la naturaleza, características, responsabilidades, causa(s) e impacto. Esta fase es indispensable para poder activar la fase de recuperación del fraude.**

- **Factores que activan un proceso de investigación de fraude**:

  Un proceso de investigación puede ser activado si la ocurrencia de un fraude:

  - ✓ Ha sido determinada

- ✓ Se presume (existen indicios)
- ✓ Ha sido informada por una fuente: interna o externa; anónima o identificada

- **Consideraciones a tomar en cuenta**:

Será necesario tener claramente establecidas las responsabilidades y roles de las áreas e instancias establecidas por el Banco para la realización de las tareas de investigación de un fraude y que correspondan al factor que activó esta fase de investigación. Se debería considerar también:

- ✓ Agentes que podrán participar en un proceso de investigación de fraude: Dependiendo de la naturaleza, magnitud e información disponible respecto al evento de fraude, podrían participar: Auditoría (Interna / Externa); Seguridad; Recursos Humanos; Legal; Sistemas; Operaciones y otros que la Dirección de el Banco (o responsable de las tareas de gestión de los riesgos de fraude) decida.

- ✓ Técnicas de investigación: entrevistas; revisión del proceso, producto o servicio afectado, incluyendo la documentación y controles existentes (se recomienda utilizar la información recogida en la Hoja de Trabajo HT-04 o su equivalente)[2]; revisión documentaria de la operación y/o transacciones involucradas; revisión de reportes de control y archivos de seguridad; inspección de cintas de video de seguridad; aplicación de técnicas de análisis forense (fuera del alcance de esta metodología). Se

[2] Se recomienda coordinar con la División Riesgo Operativo para simplificar esfuerzos y aprovechar sinergias.

sugiere contratación de personal experto de una consultora o firma de auditoría para su aplicación; auditoría de datos; análisis de código fuente de programas; aplicación de cuestionarios; entre otros que el Banco pueda considerar pertinentes y enmarcados en las leyes del país.

- ✓ Oportunidad y duración de las investigaciones: todo proceso de investigación deberá ser realizado en un plazo de tiempo que el Banco estime razonable y conveniente según sea la naturaleza y materialidad del fraude.

- ✓ Protocolo de inicio y término de una investigación: tanto el inicio como el término / cancelación / paralización de un proceso investigatorio deberían contar con protocolos preestablecidos en las políticas de gestión de fraudes del Banco, a fin de facilitar su mejor desarrollo y comunicación a las áreas y agentes externos que pudieran formar parte de las tareas de investigación.

- ✓ Presentación de resultados: Debería considerarse los siguientes aspectos: i) Niveles de reporte (destinatarios); ii) Forma de reporte (informe, presentación, memorando, email, etc.); iii) Tiempo máximo para: a) generar reporte; b) presentar reporte (interna y externamente al Banco).

- ✓ Archivo y custodia de los papeles de trabajo: Es conveniente que el Banco tenga políticas precisas para el archivo y custodia de los papeles de trabajo relacionados a la investigación de un fraude. Dichas políticas también deberían comprender las restricciones de seguridad y confidencialidad de los mismos.

> **Importante**: Todos los aspectos antes mencionados deben estar enmarcados en prácticas y estándares de Debido Cuidado Profesional. Considerar también la creación y/o actualización de una base de datos de pérdidas por fraude[3].

5.5.5 Recuperación: **Lineamientos y acciones definidos por el Banco para restablecer el normal y correcto funcionamiento de un proceso, producto o servicio (en el sentido más amplio), así como para revertir el impacto de un fraude y gestionar acciones de naturaleza laboral y legal.**

Es recomendable tomar en consideración lo siguiente:

- Asignación de la responsabilidad y procedimientos para:
  - ✓ Recuperación / resarcimiento de fondos/activos sustraídos
  - ✓ Recuperación de imagen
  - ✓ Recuperación del proceso/producto/servicio afectado (incorporación de controles). Se sugiere actualizar la Hoja de Trabajo HT-04 o su equivalente.
- Resolución de vínculos laborales o contractuales, según corresponda
- Denuncia policial y seguimiento
- Retroalimentar la función de monitoreo

> **Importante**: La metodología descrita en este documento, no debe representar en forma alguna, limitación o exclusión de otros enfoques y marcos de control

[3] Disponible en el sistema administrado por la División de Riesgo Operativo

5.6 Evaluación de Riesgos

5.6.1 Grabación de tarjetas

Seguridad Física

- El área de grabación de las tarjetas debe estar distribuida de manera que las actividades de ingreso de tarjetas nuevas, así como la entrega de tarjetas grabadas, no deben interrumpir ni tener acceso a las actividades propias de la grabación de tarjetas.
- Las actividades del personal que realiza la entrega, grabación y salida de tarjetas deben estar monitoreadas constantemente, a través del uso de cámaras de seguridad que puedan capturar las actividades pero no los valores ingresados a los procesadores y/o máquinas embosadoras.
- Todo acceso de tarjetas en blanco y salida de tarjetas grabadas debe ser registrado en una bitácora que se encuentre en el área de grabación.
- El área de grabación de tarjetas debe ubicarse siempre en un área restringida, por lo que no debe contar con paredes, ventanas o puertas que colinden con la parte externa del edificio del Banco.
- El acceso a esta área debe estar debidamente autorizada. Los operadores del equipo, asistentes y jefe del área deberán contar con una identificación de acceso que debe ser portada de manera constante. Así mismo, deberán usar un método automático de verificación de identidad, como una tarjeta de proximidad o controles biométricos.
- El acceso de personas ajenas al área de grabación deberá ser solicitado de manera escrita y justificada por un Gerente de Departamento, Gerente General o Jefe de órgano de control, y sólo podrá ser autorizado por el Jefe del área de grabación, bajo la opinión de la División Seguridad de Información.
- Todo acceso de personal ajeno al área de grabación, debidamente autorizado, deberá ser registrado y acompañado en todo momento por personal propia

del área, verificando que los visitantes no tengan acceso a información confidencial.

- Se deben contar con alarmas de movimiento, para evitar la intrusión de personas ajenas al área mientras ésta se encuentre vacía.
- Las cámaras de monitoreo debe estar siempre activas y almacenar la información de por lo menos sesenta (60) días de anterioridad.
- El sistema de cámaras y las alarmas deberán contar con mantenimiento preventivo y su funcionamiento deberá ser sometido a pruebas de manera periódica.
- Todas las tarjetas en blanco que sean entregadas al área de grabación, deben almacenarse en una caja fuerte o bóveda interna. Se debe contar con una cámara que monitoree las actividades de ingreso y salida a dicha caja fuerte o bóveda, pero no deberán registrar el ingreso de la clave secreta de apertura.
- El acceso a la caja fuerte o bóveda debe realizarse bajo control dual. La clave de acceso y la llave física deben ser administradas por personas diferentes que pertenezcan al área de grabación.
- La clave de la caja fuerte y bóveda debe ser cambiada cada treinta (30) días o cada vez que el custodio de la clave sea reemplazado.

Seguridad lógica

- El acceso a las máquinas de grabación de tarjetas debe ser mediante clave de acceso que cumpla con los siguientes controles:
  - Identificador único en la red
  - Identificador único en la aplicación de grabación de tarjetas
  - La contraseña no debe ser menor de 8 dígitos
  - La contraseña debe ser forzada a cambiarse como máximo cada 30 días.
  - La contraseña deberá constar de por lo menos 2 de los siguientes grupos de caracteres: letras minúsculas, letras mayúsculas, números, caracteres especiales.

- La contraseña no podrá repetirse hasta por lo menos haber realizado 6 cambios de la misma.
- En caso de olvido de la contraseña, esta deberá ser restaurada a través del sistema de administración de contraseñas del Banco. De generarse una contraseña por defecto o que sea conocida por el administrador de la red, ésta deberá ser cambiada automáticamente por el operador.

Riesgos mitigados: 7.1.2

- Toda actividad realizada dentro de la aplicación, debe ser registrada por un log de auditoría, donde se especifique la hora, fecha y actividad realizada con un identificador de usuario. Los intentos fallidos de acceso también deberán ser registrados en el log.

  Riesgos mitigados: 7.1.2

Procesamiento

- El archivo que contiene la información de los tarjetahabientes, cuentas y llaves de seguridad, que es enviada desde el computador central hacia las máquinas de grabación de tarjetas, debe viajar por la red de manera encriptada bajo una llave ZPK.
- Se debe verificar de manera dual que el número de tarjetas a grabar sea igual al número de tarjetas solicitadas por el computador central. No se deben grabar tarjetas que no hayan sido solicitadas.
- Al finalizar el proceso, dos personas deben contar el número de tarjetas grabadas y sin grabar, para comprarlo con el número de tarjetas retiradas de la caja fuerte o bóveda, y concordarlo con la orden de trabajo. Si existe alguna diferencia, debe revisarse si hay informe de tarjetas dañadas.
- En caso que una tarjeta resulte dañada por el proceso, ésta deberá ser almacenada en la caja fuerte o bóveda, hasta que se indique el momento de destrucción de dicha tarjeta.
- La destrucción de las tarjetas debe realizarse de manera segura, que no permita reconstruir la información que en ella pudo almacenarse.

- La destrucción de tarjetas dañadas deberá realizarse semanalmente y en presencia de un representante de Auditoría o Legal, y de Seguridad de Información (dos como mínimo), y deberá contar con un Acta de Destrucción donde se constate la presencia de los veedores y el número de tarjetas a destruir. El modelo de Acta de Destrucción se muestra en la figura 5.6:

ACTA DE DESTRUCCIÓN DE TARJETAS
Fecha: ___de_____del 200___

Participantes	
Número de Tarjeta	
Motivo de destrucción	

Firman en señal de conformidad, a las ____ horas:

_____	_____
Seguridad de Información	Auditoría Interna/ Asesoría Legal

Figura 18: Acta de Destruccion de Tarjeta

5.6.2 De la operación

Procesamiento de la información .

- Los PINs no aparecerán nunca almacenados en texto claro en ninguna base de datos, archivo o sistema. Su almacenamiento deberá ser exclusivamente en valor encriptado.

Transacciones en ATMs

Transacciones On-US – Rol Emisor

1. La información ingresada en el cajero es encriptada bajo la llave
2. En el switch central se desencripta la información
3. Se resuelve la transacción en el computador central y devuelve la respuesta al ATM.

Transacciones Domésticas – Rol Adquirente

1. La información ingresada en el cajero es encriptada bajo la llave
2. En el switch central se desencripta la información y se determina que es una transacción doméstica.
3. Firma la información con la llave pública de Visanet Perú y la envía a Visanet Perú.
4. Visanet Perú desencripta la información con su llave privada con el Banco.
5. Determina a la entidad doméstica A a la cual pertenece la transacción.
6. Firma la transacción con la llave pública de la entidad A y se la envía.
7. La entidad A desencripta la información con su llave privada y resuelve la transacción.
8. Envía la respuesta encriptada con la llave pública a Visanet Perú.
9. Visanet Perú desencripta la información con su llave privada con la entidad A.
10. Determina al Banco como adquirente de la transacción.
11. Firma la transacción con la llave pública del Banco y se la envía.
12. El Banco desencripta la información con su llave privada y responde al ATM encriptando la información

Transacciones Internacionales – Rol Adquirente

1. La información ingresada en el cajero es encriptada bajo la llave
2. En el switch central se desencripta la información y se determina que es una transacción internacional.
3. Firma la información con la llave pública de Visa y se la envía.
4. Visa desencripta la información con su llave privada con el Banco

5. Determina al emisor E a la cual pertenece la transacción.
6. Firma la transacción con la llave pública del emisor E y se la envía.
7. El emisor E desencripta la información con su llave privada y resuelve la transacción.
8. Envía la respuesta encriptada con la llave pública a Visa.
9. Visa desencripta la información con su llave privada con el emisor E.
10. Determina al Banco como adquirente de la transacción.
11. Firma la transacción con la llave pública del Banco y se la envía.
12. El Banco desencripta la información con su llave privada y responde al ATM encriptando la información

Transacciones en ATMs de otros bancos

Transacciones Domésticas – Rol Emisor

1. La información ingresada en el cajero de otro banco X es encriptada bajo la llave TPK.
2. En el switch central se desencripta la información con la y se determina que es una transacción doméstica.
3. Firma la información con la llave pública de Visanet Perú y la envía a Visanet Perú.
4. Visanet Perú desencripta la información con su llave privada con el banco X.
5. Determina que la entidad emisora es el Banco.
6. Firma la transacción con la llave pública del Banco y se la envía.
7. El Banco desencripta la información con su llave privada y resuelve la transacción.
8. Envía la respuesta encriptada con la llave pública a Visanet Perú.
9. Visanet Perú desencripta la información con su llave privada con el Banco.

10. Determina al Banco X como adquirente de la transacción.
11. Firma la transacción con la llave pública del Banco X y se la envía.
12. El Banco X desencripta la información con su llave privada y responde al ATM encriptando la información bajo la

Transacciones Internacionales – Rol Emisor

1. La información ingresada en el cajero del Banco Y es encriptada bajo la llave.
2. En el switch central se desencripta la información y se determina que es una transacción internacional.
3. Firma la información con la llave pública de Visa y se la envía.
4. Visa desencripta la información con su llave privada con el Banco Y.
5. Determina que la entidad emisora es el Banco.
6. Firma la transacción con la llave pública del Banco y se la envía.
7. El Banco desencripta la información con su llave privada y resuelve la transacción.
8. Envía la respuesta encriptada con la llave pública a Visa.
9. Visa desencripta la información con su llave privada con el Banco.
10. Determina al Banco Y como adquirente de la transacción.
11. Firma la transacción con la llave pública del Banco Y y se la envía.
12. El Banco Y desencripta la información con su llave privada y responde al ATM encriptando la información

Flujo de aceptación de operaciones de una tarjeta chip en un ATM

Paso 1: Comenzar una transacción

Para comenzar una transacción, la tarjeta chip es insertada dentro del ATM. El chip en la tarjeta se conecta con los contactos en el ATM para que puedan comunicarse uno con el otro. La tarjeta debe permanecer en éste hasta que la transacción esté completada.

Paso 2: Selección de la aplicación

El ATM determina cuales aplicaciones son soportadas tanto por él como por la tarjeta. Si la tarjeta y el ATM no tienen aplicaciones en común, la transacción es terminada. Si la tarjeta y el ATM tienen una aplicación en común, esa aplicación es usada. Si la tarjeta y el ATM tienen más de una aplicación en común, el ATM muestra una lista de aplicaciones para la selección del tarjetahabiente. Una vez que la aplicación es seleccionada, la tarjeta envía información al ATM para ser usada durante la transacción.

Paso 3: Verificación del tarjetahabiente

La tarjeta y el ATM trabajan conjuntamente para determinar el método de verificación apropiado para la transacción (tanto la firma, PIN en línea, verificación del tarjetahabiente). Si el método de verificación del tarjetahabiente es PIN fuera de línea, el terminal solicita al tarjetahabiente el ingreso de su PIN. El PIN ingresado del tarjetahabiente es comparado con el PIN almacenado en el chip por el emisor durante el proceso de personalización de la tarjeta. Los métodos de verificación en línea son implementados de manera similar a la banda magnética.

El Banco debe implementar todas las modalidades disponibles en sus cajeros automáticos. La verificación del PIN fuera de línea debe realizar como primera

medida antes de enviar los datos de la transacción al switch central. En casos de contingencia, esta verificación debe realizarse cuando exista conexión con el computador central pero no exista respuesta del Switch Stratus o del HSM.

Paso 4: Transacciones en línea

Cuando la tarjeta y el ATM deciden enviar una transacción en línea y la tarjeta soporta la facilidad de autenticación de tarjeta en línea, el chip genera un criptograma ARQC resultado de la encripción de los datos de la tarjeta, el ATM, y la transacción bajo la TPK. El criptograma es único por cada transacción. El chip de la tarjeta envía el criptograma y los datos al terminal.

El terminal envía el criptograma, y los elementos de datos originales usados por el chip para crear el criptograma, al adquirente. El adquirente formatea estos datos en el mensaje de autorización y los envía al emisor a través de la red en línea.

Paso 5: Procesamiento del emisor

El emisor valida el criptograma y usa los resultados de la autenticación de la tarjeta en línea en su decisión de autorización. El emisor puede también usar los resultados de la administración de riesgos fuera de línea, como el PIN fuera de línea y la autenticación de datos fuera de línea, para determinar la respuesta de autorización.

Paso 6: Respuesta del emisor

Para proteger la respuesta de autorización del emisor y asegurar que la respuesta venga de un emisor válido, el emisor tiene la habilidad de enviar un criptograma para la autenticación del emisor en línea en la respuesta. Este criptograma es llamado Criptograma de Respuesta de Autorización.

El emisor también tiene la opción de enviar actualizaciones post emisión para la tarjeta en la respuesta. Estas actualizaciones permiten al emisor cambiar información en la tarjeta después de que ésta ha sido emitida. Antes de aplicar las actualizaciones Post emisión, la tarjeta asegura que se está comunicando con un emisor válido.

Cuando la tarjeta recibe la respuesta, ésta aplica la actualización post emisión (si está presente) después de asegurar de que las actualizaciones provienen del emisor correcto. El código de respuesta de autorización es usado para determinar si la transacción es aprobada o declinada.

Paso 7: Compensación y Pago

Ya sea para transacciones aprobadas en línea o fuera de línea, la tarjeta genera un criptograma final llamado Certificado de Transacción. Este criptograma y sus elementos de datos soportados representan una pista de auditoría. Las pistas de auditoría proveen evidencia de las actividades realizadas por la tarjeta y el terminal de punto de la transacción. Esta información es incluida con el mensaje de compensación y pueden ser usados durante un proceso de disputa.

Beneficios

- Disminución del costo de inicialización de los cajeros automáticos.
- Reducción del riesgo de compromiso por conocimiento de los componentes de las claves.
- Minimizar el uso de personal para labores de operación con claves.
- Protección de las claves simétricas secretas.

Capítulo 6: Glosario de Términos

- Acceso remoto: Acceso a redes informáticas desde una ubicación remota, en general localizada fuera de la red. Las redes VPN constituyen un ejemplo de tecnologías de acceso remoto.
- Administrador de base de datos: También denominado “DBA”. Persona responsable de gestionar y administrar una base de datos.
- Adquiriente: También denominado “banco adquirente” o “institución financiera adquiriente”.
- Entidad que inicia y mantiene relación con comerciantes y permite que estos últimos acepten tarjetas de pago.
- Adware: Tipo de software malicioso cuya instalación hace que el equipo muestre o descargue publicidad de manera automática.
- Algoritmo de cifrado: Secuencia de instrucciones matemáticas usadas para transformar textos o datos no cifrados en textos o datos cifrados y viceversa.
- Amenaza: Condición o actividad capaz de ocasionar que la información o recursos para el procesamiento de la información se pierdan, modifiquen o vuelvan inaccesible; o bien queden expuestos o afectados de algún otro modo en detrimento de la organización.
- Análisis de seguridad de red: Proceso mediante el cual se comprueba de manera remota la vulnerabilidad de las entidades de un sistema. Este proceso se realiza por medio de herramientas manuales o automáticas. Análisis de seguridad que incluyen la evaluación de sistemas internos y externos y la elaboración de informes acerca de servicios expuestos a la red. Los análisis pueden identificar vulnerabilidades de los servicios, dispositivos y sistemas operativos que individuos malintencionados pueden utilizar a su favor.
- Antivirus: Programa o software capaz de detectar y eliminar los diferentes tipos de programas maliciosos (también conocidos como "malware"), incluidos virus, troyanos, gusanos, spyware, adware y rootkits, y de proteger su computadora contra estos.

- Aplicación: Todos los programas o grupos de programas de software comprados o personalizados, incluidas las aplicaciones internas y externas (por ejemplo, aplicaciones web).
- Área confidencial: Todo centro de datos, sala de servidores o cualquier área que aloje sistemas que almacenen procesos o transmitan datos de titulares de tarjetas. No se incluyen las áreas en las que solo haya terminales de punto de venta, como el área de cajas en un comercio.
- Autenticación: Proceso de identificación de la identidad de un individuo, dispositivo o proceso.
- Autenticación de dos factores: Método de autenticación de un usuario mediante la comprobación de dos o más factores. Los factores incluyen algo que el usuario posee (como un token de hardware o software), algo que sabe (como una contraseña, frase de seguridad o PIN) o algo que el usuario es o hace (como las huellas dactilares y otros elementos biométricos).
- Autorización: Otorgamiento de derechos de acceso u otros derechos similares a un usuario, programa o proceso. En cuanto a las redes, la autorización define lo que un individuo o programa está autorizado a realizar después de un proceso de autenticación correcto.
- En cuanto a las transacciones realizadas mediante tarjetas de pago, se refiere al momento en el cual el comerciante recibe notificación de que una tarjeta de pago está autorizada para una determinada transacción.
- Base de datos: Formato estructurado que permite organizar y mantener información de fácil recuperación. Algunos ejemplos simples de base de datos son las tablas y las hojas de cálculo.
- Bluetooth: Protocolo inalámbrico que utiliza tecnología de comunicación de corto alcance y permite la transmisión de datos entre dos dispositivos ubicados a poca distancia.
- Cifrado: Proceso que consiste en transformar la apariencia de los datos para volverlos ininteligibles para todos aquellos que no posean una clave criptográfica especifica. El cifrado evita que la información cifrada y descifrada (proceso contrario al cifrado) sea revelada a personas no autorizadas.

- Cifrado de base de datos por columna: Técnica o tecnología (software o hardware) utilizada para cifrar el contenido de una columna especifica en una base de datos, en lugar de toda la base de datos. Como alternativa, consulte Cifrado de disco o Cifrado por archivo.
- Cifrado de disco: Técnica o tecnología de software o hardware que se utiliza para cifrar todos los datos almacenados en un dispositivo (por ejemplo, un disco duro o una unidad flash). Además, los contenidos de archivos o columnas específicas pueden cifrarse mediante el cifrado por archivo o el cifrado de base de datos por columna.
- Cifrado por archivo: Técnica o tecnología de software o hardware que se utiliza para cifrar todo el contenido de archivos específicos. Como alternativa, consulte Cifrado de disco o Cifrado de base de datos por columna.
- Clave: En criptografía, la clave es un valor que determina el resultado de un algoritmo de cifrado al transformar texto simple en texto cifrado. En general, la extensión de una clave determina la dificultad para descifrar el texto de un determinado mensaje. Consulte Criptografía solida.
- Código de servicio: Código de valor de tres o cuatro dígitos en la banda magnética junto a la fecha de vencimiento de la tarjeta de pago presente en la pista de datos. Se utiliza para definir atributos del servicio, diferenciar entre intercambios nacionales e internacionales e identificar restricciones de uso.
- Código o valor de verificación de la tarjeta: Se refiere a: (1) Datos de banda magnética o (2) funciones de seguridad impresas.
- Elementos de datos en la banda magnética de una tarjeta que utiliza procesos criptográficos para proteger la integridad de datos de la banda y evidencia cualquier alteración o falsificación. Conocida como CAV, CVC, CVV o CSC, según la marca de la tarjeta de pago. La siguiente lista especifica los términos según la marca de tarjeta:

  CAV: Card Authentication Value (valor de autenticación de la tarjeta) (tarjetas de pago JCB)

  CVC: Card Validation Code (código de validación de la tarjeta) (tarjetas de pago MasterCard)

CVV: Card Verification Value (valor de verificación de la tarjeta) (tarjetas de pago Visa y Discover)

CSC: Card Security Code (código de seguridad de la tarjeta) (tarjetas de pago American Express)

En el caso de las tarjetas de pago Discover, JCB, MasterCard y Visa, el segundo tipo de valor o código de validación de la tarjeta es el valor de tres dígitos impreso que se encuentra más a la derecha de la zona del panel de firma, en el reverso de la tarjeta. En el caso de las tarjetas

American Express, el código es un número de cuatro dígitos no grabado en relieve, sino impreso encima del PAN, en el anverso de todas las tarjetas de pago. El código se asocia en forma exclusiva con cada plástico individual y vincula el número de cuenta de la tarjeta al plástico.

A continuación, se ofrece una descripción general:

CID: Card Identification Number (numero de identificación de la tarjeta) (tarjetas de pago American Express y Discover)

CAV2: Card Authentication Value 2 (valor de autenticación de la tarjeta 2) (tarjetas de pago JCB)

CVC2: Card Validation Code 2 (código de validación de la tarjeta 2) (tarjetas de pago MasterCard)

CAV2: Card Verification Value 2 (valor de verificación de la tarjeta 2) (tarjetas de pago Visa)

- Comerciante: En lo que concierne a la industria PCI DSS, la definición de comerciante incluye toda entidad que acepte tarjeta de pago con el logotipo de cualquiera de los cinco miembros del PCI SSC (American Express, Discover, JCB, MasterCard o Visa) como forma de pago por mercancías y servicios. Tenga en cuenta que un comerciante que acepta tarjetas de pago por mercaderías y servicios puede ser también un proveedor de servicios, si los servicios comerciados conllevan al almacenamiento, procesamiento o a la transmisión de los datos del titular de la tarjeta en beneficios de otros comerciantes o proveedores de servicios. Por ejemplo, puede que un ISP sea un comerciante que acepte tarjetas pago por facturaciones mensuales, pero que, si los clientes para

los que actúa como host son comerciantes, sea al mismo tiempo proveedor de servicios.

- Componentes de red: Los componentes de la red incluyen, a modo de ejemplo, firewalls, conmutadores, routers, puntos de acceso inalámbricos, aplicaciones de red y otras aplicaciones de seguridad.
- Componentes del sistema: Todo componente de red, servidor o aplicación que se incluye en el entorno de datos del titular de la tarjeta o está conectado a él.
- Conocimiento parcial: Condición en la cual dos o más entidades separadas poseen componentes de una clave, pero que, de forma individual, no pueden descifrar la clave criptográfica resultante.
- Consola: Pantalla o teclado que permite obtener acceso al servidor o equipo de mainframe y controlarlo dentro de un entorno de red.
- Consumidor Persona compradora de bienes, servicios o ambos.
- Contraseña o Frase de seguridad: Una serie de caracteres que autentican la identidad del usuario.
- Contraseñas predeterminadas: Contraseña perteneciente a la administración de un sistema o a las distintas cuentas de servicio predefinidas en un sistema, dispositivo o aplicación. Generalmente, esta contraseña está relacionada con una cuenta predeterminada. Las contraseñas y cuentas predeterminadas son de dominio público y, en consecuencia, es fácil averiguarlas.
- Control de acceso: Mecanismo que limita la disposición de información, o de los recursos necesarios para su procesamiento, solo a personas o aplicaciones autorizadas.
- Control dual: Proceso que consiste en utilizar dos o más entidades distintas (por lo general, personas) de manera coordinada para proteger funciones o información confidenciales. Ambas entidades son igualmente responsables de la protección física de los materiales que intervienen en transacciones vulnerables. Una sola persona es incapaz de obtener acceso o utilizar estos materiales (por ejemplo, la clave criptográfica). Para generar, transferir, cargar, almacenar y recuperar manualmente una clave, el proceso de control dual requiere que esta

clave se divida entre dos o más participantes. (Consulte también División del conocimiento).

- Controles de compensación: Los controles de compensación pueden tenerse en cuenta cuando una entidad no puede cumplir con un requisito explícitamente establecido debido a limites comerciales legítimos, técnicos o documentados, pero pudo mitigar el riesgo asociado con el requisito de forma suficiente, mediante la implementación de otros controles. Los controles de compensación deben:

  Cumplir con el propósito y el rigor del requisito original de las PCI DSS.

  Proporcionar un nivel similar de defensa, como el requisito original de las PCI DSS.

  Superar ampliamente los requisitos de otras PCI DSS (no solamente en cumplimiento de otras PCI DSS).

  Ser cuidadoso con el riesgo adicional que impone la no adhesión al requisito de las PCI DSS.

  Para obtener información acerca del uso de los controles de compensación, consulte los Anexos B y C de los Controles de compensación que se encuentran en los Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad.

- Copia de seguridad: Copia duplicada de datos que se realiza con el fin de archivarla o protegerla de daños o perdidas.

- Criptografía: Disciplina de las matemáticas y la informática que se ocupa de la seguridad de la información, en especial de los procesos de cifrado y autenticación. En relación a la seguridad de redes y aplicaciones, es una herramienta que permite controlar el acceso a la información, y su confidencialidad e integridad.

- Criptografía solida: Criptografía basada en algoritmos probados y aceptados por la industria. Extensiones de clave solidas y prácticas adecuadas de administración de claves. La criptografía es un método de protección de datos e incluye el cifrado, reversible, y la refundición, no reversible o de un solo uso. SHA-1 es un ejemplo de un algoritmo de refundición probado y aceptado por la

industria. Algunos ejemplos de algoritmos de refundición probados y aceptados por la industria incluyen: AES (128 bits y superior), TDES (claves mínimas de doble extensión), RSA (1024 bits y superior), ECC (160 bits y superior) y El Gamal (1024 bits y superior). Para obtener más información, consulte la publicación especial de NIST 800- 57 (http://csrc.nist.gov/publications/).

- Cuentas predeterminadas: Cuenta de inicio de sesión que se encuentra predefinida en un sistema, dispositivo o aplicación y permite obtener acceso por primera vez al momento en que el sistema comienza a funcionar.
- Datos confidenciales de autenticación: Información de seguridad (códigos o valores de validación de tarjetas, datos completos de banda magnética, PINs y bloqueos de PIN) utilizada en la autenticación de titulares de tarjetas que aparezcan en texto simple u otra forma desprotegida.
- Datos de banda magnética: También denominados “datos de pistas”. Datos codificados en una banda magnética o un chip que se utilizan para obtener autorización y proceder a una transacción de pago. Puede ser la imagen que aparece en la banda magnética o los datos de la pista 1 y/o pista 2 de la banda magnética. Las entidades no deben retener todos los datos de una banda magnética después de obtener autorización para proceder con la transacción.
- Datos de transacción: Datos relacionados a las transacciones con tarjetas de pago electrónico.
- Datos del titular de la tarjeta: Los datos del titular de la tarjeta contienen, como mínimo, el PAN completo.
- Es posible que los datos del titular de la tarjeta incluyan el PAN completo mas alguno de los siguientes datos:

  Nombre del titular de la tarjeta

  Fecha de vencimiento

  Código de servicio

  Consulte Datos confidenciales de autenticación para obtener más información sobre elementos de datos que pueden transmitirse o procesarse como parte de una transacción de pago.

- Desinfección: Proceso mediante el que se eliminan datos confidenciales de un archivo, dispositivo o sistema. La definición también incluye la modificación de datos para que sean inservibles si se accede a ellos en un ataque.
- Destrucción magnética: También denominada “destrucción magnética de disco”. Proceso o técnica mediante el cual se desmagnetiza un disco para destruir permanentemente toda la información almacenada en el.
- Dirección IP: También denominada “dirección de protocolo de Internet”. Código numérico que identifica exclusivamente un equipo en Internet.
- Dirección MAC: Abreviatura de “media access control address” (dirección de control de acceso a medios). Valor único de identificación que el fabricante asigna a los adaptadores de red y a las tarjetas de interfaz de red.
- Emisor: También denominado “banco emisor” o “instituciones financieras emisoras”. Entidad que emite tarjetas de pago directamente a consumidores y no consumidores.
- Ensambladores: En la criptografía, el ensamblador de un solo uso es un algoritmo de cifrado con texto que se combina con una clave aleatoria o "ensamblador". Presenta una extensión igual a la del texto simple y puede utilizarse solo una vez. Asimismo, si la clave es en verdad aleatoria, secreta y de un solo uso, no será posible descifrar el ensamblador.
- Entorno de los datos del titular de la tarjeta: Área del sistema de redes que posee datos acerca del titular de la tarjeta o datos confidenciales de autenticación e información referida a los sistemas y segmentos que colaboran o asisten directamente en el procesamiento, almacenamiento o transferencia del titular de dicha tarjeta. Es probable que una segmentación adecuada de red, que aísle los sistemas que almacenan, procesan o transfieren datos del titular de la tarjeta de los sistemas que no realizan estas operaciones, reduzca el alcance del entorno de datos del titular de la tarjeta y, por ende, el alcance de la evaluación PCI DSS. Un entorno de datos del titular de la tarjeta está formado por componentes de sistemas. Consulte Componentes de sistemas.
- Evaluación o análisis de riesgos: Proceso que identifica los recursos valiosos de un sistema y sus amenazas; cuantifica la exposición a riesgos (es decir, el

potencial de perdida) según frecuencias estimadas y costos derivados por siniestros; y, opcionalmente, recomienda el modo de asignar recursos como medidas preventivas que minimicen el índice general de exposición.

- Falsificación de dirección IP: Técnica de ataque que utiliza una persona malintencionada para obtener acceso no autorizado a equipos. La persona malintencionada envía mensajes engañosos a otros equipos. Los mensajes tienen una dirección IP que indica que el mensaje proviene de un host de confianza.
- Filtrado de ingreso: Método que permite filtrar el tráfico que ingresa en una red interna mediante un router para verificar que los paquetes entrantes realmente provengan de las redes de las que parecen venir.
- Filtrado de salida: Método que permite filtrar el tráfico que egresa de una red interna mediante un router, de modo que el tráfico no autorizado no pueda salir de la red interna.
- Filtrado dinámico de paquetes: Consulte Inspección completa.
- Herramientas forenses: También denominadas "herramientas forenses electrónicas". Con respecto a la seguridad de la información, es la aplicación de herramientas de investigación y técnicas de análisis para reunir evidencia a partir de diferentes recursos informáticos que determinan el origen de riesgos de datos.
- Host: Hardware del equipo principal en el que está instalado el software informático.
- Informe de cumplimiento: También denominado "ROC". Informe que describe detalles relacionados al estado de cumplimiento de las normas PCI DSS por parte de una entidad.
- Informe de validación También denominado "ROV". Informe que describe detalles relacionados al cumplimiento de una aplicación de pago de las normas PCI DSS.
- Inspección estática: También denominada "filtro de paquete dinámico", es un firewall que, al seguir la ruta de los paquetes de comunicación, proporciona una seguridad mejorada. Tan solo los paquetes entrantes con respuestas adecuadas ("conexiones establecidas") pueden atravesar el firewall.

- Inyección SQL: Tipo de ataque a sitios web basados en bases de datos. Un individuo malintencionado ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a los equipos de host de una organización mediante el equipo que funciona como servidor de la base de datos.
- Limpieza segura: También denominada "eliminación segura", es una aplicación utilizada para eliminar archivos específicos de un sistema informático de manera permanente.
- Mainframe: Computadoras diseñadas para trabajar con grandes volúmenes de entrada y salida de datos y para enfatizar el rendimiento informático. Los sistemas mainframe pueden ejecutar varios sistemas operativos, por lo que parece que estuvieran operando múltiples computadoras. Muchos sistemas heredados presentan un diseño de mainframe.
- Medios electrónicos extraíbles: Medios capaces de almacenar datos fáciles de extraer y transportar de un sistema informático a otro. Algunos ejemplos incluyen CD-ROM, DVD-ROM, unidades flash USB y discos rígidos extraíbles.
- Monitorización: Utilización de sistemas o procesos que supervisan de manera constante los recursos informáticos o de red para alertar al personal en caso de fallas, alarmas u otros eventos definidos con anterioridad.
- Monitorización de integridad de archivos: Técnica o tecnología mediante la cual se supervisan determinados archivos o registros para detectar si sufrieron modificaciones. En caso de que se modifiquen archivos o registros críticos, debe alertarse al personal de seguridad indicado.
- Número de cuenta: Consulte Número de cuenta principal (PAN).
- Ocultamiento: Método mediante el cual se oculta un segmento de los datos mostrados. El ocultamiento se utiliza cuando no existen requisitos comerciales que demanden mostrar el PAN completo.
- Parche: Actualización de un software existente para agregarle funcionalidad o corregir un defecto.

- Política: Normas vigentes para toda la organización que reglamentan el uso aceptable de los recursos informáticos, las practicas de seguridad y el desarrollo guiado de procedimientos operacionales. Política de seguridad Conjunto de leyes, reglamentos y prácticas que regulan el modo en una empresa administra, protege y distribuye información confidencial.
- Procedimiento: Narración descriptiva de una política. El procedimiento equivale a los pasos de una política y describe como debe implementarse una determinada política.
- Productos estándar: Descripción de productos listos para usar comercializados como mercaderías no personalizadas o específicamente diseñadas para un cliente o usuario.
- Protocolo: Método acordado de comunicación utilizado en las redes. Son las especificaciones que describen las reglas y procedimientos que deben seguir los diferentes productos informáticos para realizar actividades en la red.
- Protocolo, servicio o puerto inseguro: Un protocolo, servicio o puerto que produce preocupación en cuanto a la seguridad debido a la falta de controles de confidencialidad y/o integridad. Estas preocupaciones relacionadas con la seguridad afectan a los servicios, protocolos o puertos que transmiten datos y credenciales de autenticación (como contraseñas o frases de seguridad de texto simple en Internet), o son simples de explotar si se los configura incorrectamente o de forma predeterminada. El protocolo FTP constituye un ejemplo de un protocolo, servicio o puerto inseguro.
- Proveedor de host: Ofrece diferentes servicios a comerciantes y otros proveedores de servicios. Los servicios abarcan desde lo simple a lo complejo: desde un espacio compartido en un servidor hasta una completa gama de opciones para el "carrito de compras"; desde aplicaciones de pago, pasando por hosting dedicados exclusivamente a un cliente, hasta conexiones con pasarelas y procesadores de pago. Es posible que el proveedor de hosting sea un proveedor de hosting compartido, encargado de prestar servicio a diferentes entidades en un solo servidor.

- Proveedor de servicios: Entidad comercial diferente de una marca de pago que está directamente relacionada al procesamiento, almacenamiento o a la transmisión de los datos del titular de la tarjeta. Se incluyen también empresas que proveen servicios que controlan o pueden tener injerencia en la seguridad de los datos del titular de la tarjeta. Algunos ejemplos incluyen proveedores de servicios administrados que proveen firewalls gestionados, IDS y otros servicios; proveedores de hosting y otras entidades. Quedan excluidas las empresas de
- Telecomunicaciones que solo proveen enlaces de comunicaciones sin acceso a la capa de aplicaciones de este enlace.
- Prueba de penetración: Las pruebas de penetración tienen como objetivo explotar vulnerabilidades a fin de determinar la posibilidad de accesos no autorizados al sistema u otras actividades malintencionadas. Las pruebas de penetración incluyen pruebas de aplicaciones y redes y controles y procesos de redes y aplicaciones. Se realizan tanto desde el exterior de la red hacia el interior (pruebas externas) como en el sentido contrario.
- Punto de acceso inalámbrico: También denominado "AP". Dispositivo que permite a los mecanismos de comunicación inalámbrica conectarse a una red inalámbrica. Usualmente conectado a una red con cable, es capaz de transferir por medio de la red datos entre dispositivos inalámbricos y con cable.
- Red: Dos o más computadoras interconectadas para compartir recursos.
- Red de confianza: Red de una organización que la empresa es capaz de controlar y administrar.
- Red no confiable: Red que se encuentra afuera de las redes de una organización y que, por ende, la empresa no puede controlar o administrar.
- Red privada: Red establecida por una organización un espacio de dirección IP privado.
- Generalmente, a las redes privadas se las denomina redes de área local. El acceso a redes privadas desde redes públicas debe estar protegido adecuadamente mediante firewalls y routers.

- Red pública: Red específicamente implementada y operada por un proveedor de telecomunicaciones con el propósito de ofrecer al público servicios de transmisión de datos. Los datos que se transfieren por medio de redes públicas pueden ser interceptados, modificados y/o redirigidos. Algunos de los ejemplos de redes públicas para las que rigen las normas PCI DSS son Internet y las tecnologías móviles e inalámbricas.
- Redes inalámbricas: Red que conecta equipos sin necesidad de una conexión física de cables.
- Re digitación de clave: Proceso que consiste en el cambio de las claves criptográficas para limitar la cantidad de datos que pueden cifrarse con una misma clave.
- Refundición: Proceso que convierte los datos del titular de la tarjeta en una serie de algoritmos criptográficos de longitud fija, y los vuelve ilegibles, mediante la Criptografía solida.
- Registro de auditoría: También denominado "pista de auditoría". Registro cronológico de las actividades del sistema. Esta herramienta proporciona una pista que permite la reconstrucción, revisión y evaluación de los entornos y actividades que rodean o conducen las operaciones, los procedimientos o eventos relacionados a una transacción desde que comienza hasta que finaliza.
- Riesgo: También denominado "riesgo de datos" o "violación de datos". Intrusión en un sistema de computadoras en la cual se sospecha una divulgación, un robo, una modificación o la destrucción no autorizada de datos del titular de la tarjeta.
- Rootkit: Tipo de software malicioso que, al instalarse sin autorización, es capaz de pasar desapercibido y tomar el control administrativo de un sistema informático.
- Router: Hardware o software que conecta dos o más redes. Clasifica e interpreta la información mediante la comprobación de direcciones y transmisión de bits de datos a los destinos correctos. Algunas veces se denomina puerta de enlace al software de un router.
- Segmentación de red: Medios de reducir el alcance de una evaluación de las PCI DSS por medio de la reducción del tamaño del entorno de datos del titular de la

tarjeta. Para lograrlo, es necesario que los sistemas que almacenan, procesan o transfieren datos del titular de la tarjeta estén aislados de aquellos sistemas que almacenan, procesan o transfieren estos datos mediante controles de red. Consulte la sección Segmentación de red en Requisitos de las DSS PCI y procedimientos de evaluación de seguridad para obtener información acerca del uso de segmentación de red.

- Seguridad de la información: Protección de la información que garantiza la confidencialidad, integridad y disponibilidad.
- Separación de funciones: Práctica que consiste en dividir los pasos de una función entre varias personas para evitar que un solo individuo pueda arruinar todo el proceso.
- Servidor: Equipo que presta servicios a otros equipos, como el procesamiento de comunicaciones, almacenamiento de archivos y acceso a impresoras.
- Algunos servidores incluyen entre otros: web, autenticación, DNS, correo, proxy, base de datos, aplicaciones y protocolos NTP.
- Servidor web: Equipo con un programa capaz de aceptar pedidos HTTP de clientes web y brindar respuestas HTTP (en general, páginas web).
- Sistema de información: Conjunto especifico de recursos de datos estructurados organizados para recolectar, procesar, mantener, usar, compartir, diseminar o disponer de la información.
- Sistema operativo o SO: Software del equipo a cargo de compartir recursos informáticos y administrar y coordinar todas las actividades informáticas. Algunos ejemplos incluyen
- Microsoft Windows, Mac OS, Linux y Unix.
- Software malicioso o malware: Software desarrollado para infiltrarse en un equipo informático o dañarlo sin que el propietario se entere o exprese su consentimiento. Por lo general, esta clase de software se infiltra en una red en el transcurso de distintas actividades comerciales aprobadas y explota las vulnerabilidades del sistema. Alguno ejemplos son los virus, gusanos, troyanos (o caballos de Troya), rootkits y programas del tipo spyware y adware.

- Spyware: Clase de software malicioso cuya instalación intercepta o toma control parcial del equipo del usuario sin que el consentimiento de este ultimo.
- SysAdmin: Abreviatura de “system administrator” (administrador de sistemas). Persona con alto nivel de privilegios responsable de administrar un sistema informático o red.
- Tarjeta inteligente: También denominada “tarjeta con chip” o “tarjeta IC (tarjeta de circuito integrado)”. Un tipo de tarjeta de pago que tiene circuitos integrados insertos en su interior. Estos circuitos, también llamados el “chip”, contienen datos de la tarjeta de pago entre los cuales se cuentan los datos equivalentes a los datos de banda magnética.
- Tarjetas de pago: En lo que concierne a las normas PCI DSS, toda tarjeta de pago o dispositivo que lleve el logotipo de los miembros fundadores del PCI SSC: American Express, Discover Financial Services, JCB International, MasterCard Worldwide o Visa Inc.
- Titular de la tarjeta: Cliente consumidor o no consumidor para el que se emite la tarjeta de pago, o todo individuo autorizado para su utilización.
- Token: Hardware o software encargado de realizar autenticaciones dinámicas o dos factores.
- Token de índice: Token criptográfico que, basado en un índice dado para un valor imprevisible, reemplaza el PAN.
- Troyano: También denominado “caballo de Troya”. Una clase de software malicioso cuya instalación permite al usuario ejecutar funciones normalmente, mientras los troyanos ejecutan funciones maliciosas sin que él lo sepa.
- Truncamiento: Método mediante el cual se elimina definitivamente un segmento de datos del PAN, con lo cual todo el PAN se vuelve ilegible.
- Usuarios no consumidores: Todas las personas, con excepción de los titulares de tarjetas, que tengan acceso a los componentes de sistema, entre los cuales se incluyen empleados, administradores y terceros.
- Vulnerabilidad: Debilidades de un sistema que permiten a un individuo malintencionado explotarlo y violar su integridad.

- AAA: Acrónimo de "authentication, authorization, and accounting" (autenticación, autorización y contabilidad). Protocolo utilizado para la autenticación del usuario basado en su identidad verificable, para otorgarle autorizaciones de acuerdo a los derechos de usuario que posea y para dar cuenta del uso de los recursos de red.
- AES: Abreviatura de "Advanced Encryption Standard" (norma de cifrado avanzado). Método de cifrado por bloques utilizado en la criptografía de clave simétrica que el NIST adopto en noviembre de 2001 como U.S. FIPS PUB 197 (o "FIPS 197"). Consulte Criptografía solida.
- ANSI: Acrónimo de "American National Standards Institute" (Instituto Estadounidense de Normas). Organización privada y sin fines de lucro que administra y coordina el sistema de evaluación de conformidad y la estandarización voluntaria en los Estados Unidos.
- ASV: Acrónimo de "Approved Scanning Vendor" (proveedor aprobado de escaneo). Empresa aprobada por la industria PCI SSC para prestar servicios de análisis de vulnerabilidad externa.
- CIS: Acrónimo de "Center for Internet Security" (centro de seguridad en Internet). Empresa sin fines de lucro cuya misión es ayudar a las organizaciones a reducir el riesgo de interrupciones en su negocio y en el comercio electrónico provocados por controles y técnicas de seguridad inadecuados.
- CIS: Acrónimo de "Center for Internet Security" (centro de seguridad en Internet). Empresa sin fines de lucro cuya misión es ayudar a las organizaciones a reducir el riesgo de interrupciones en su negocio y en el comercio electrónico provocados por controles y técnicas de seguridad inadecuados.
- FIPS: Acrónimo de "Federal Information Processing Standards" (normas de procesamiento de información federal de los EE. UU). Normas aceptadas públicamente por el gobierno federal de los EE. UU., a disposición también de agencias no gubernamentales y contratistas.
- Firewall: Tecnología de hardware y/o software que protege los recursos de red contra el acceso no autorizado. Un firewall autoriza o bloquea el tránsito de

datos entre redes con distintos tipos de niveles de seguridad, basándose en un conjunto de normas y otros criterios.

- FTP: Acrónimo de "file transfer protocol" (protocolo de transferencia de archivos). Protocolo de red que se utiliza para transferir datos de un equipo a otro mediante un red pública, como Internet. En general, se considera que FTP es un protocolo inseguro, porque permite enviar contenidos de archivos y contraseñas desprotegidos y con texto simple. El protocolo FTP puede implementarse con seguridad mediante Secure Shell (SSH) u otra tecnología.
- GPRS: Acrónimo de "General Packet Radio Service" (servicio de radio paquete general). Servicio de datos portátil disponible para los usuarios de teléfonos móviles GSM. Reconocido por el uso eficaz de capacidades de ancho de banda limitadas. Ideales para enviar y recibir pequeños paquetes de datos, como correos electrónicos, y para navegar en Internet.
- GSM: Acrónimo de "Global System for Mobile Communications" (sistema global de comunicaciones móviles). Norma ampliamente difundida para teléfonos móviles y redes. La ubicuidad de la norma GSM convierte el acceso de llamada itinerante o "roaming" a nivel internacional en algo muy común entre los operadores telefónicos, lo que permite a los suscriptores utilizar sus teléfonos en distintos lugares del mundo.
- HTTP: Acrónimo de "hypertext transfer protocol" (protocolo de transferencia de hipertexto). Protocolo abierto de Internet, utilizado para transferir o transmitir información en la Web.
- HTTPS: Acrónimo de "hypertext transfer protocol over secure socket layer" (protocolo de transferencia de hipertexto mediante una capa de conexión segura). Conexión HTTP segura que proporciona funciones de autenticación y comunicación cifrada en Internet. Está diseñada para comunicaciones que demandan condiciones muy seguras, como inicios de sesion basados en web.
- ID: Identificación de un usuario o una aplicación especifica.
- IDS: Acrónimo de "intrusion detection system" (sistema de detección de intrusiones). Software o hardware utilizado para identificar o alertar acerca de intentos de intrusión en redes o sistemas. Conformado por sensores que generan

eventos de seguridad; una consola que supervisa eventos y alertas y controla los sensores; y un motor central que registra en la base de datos los eventos denotados por los sensores. Utiliza un sistema de reglas que generan alertas en respuesta a cualquier evento de seguridad.

- IETF: Acrónimo de "Internet Engineering Task Force" (grupo de trabajo de ingeniería en Internet). Comunidad internacional abierta y extensa de diseñadores de redes, operadores, proveedores e investigadores que trabajan en el desarrollo de la arquitectura de Internet y se ocupan de su correcto funcionamiento. El IETF no exige la acreditación de membrecías y está abierto a cualquier persona interesada.
- IP: Acrónimo de "internet protocol" (protocolo de Internet). Protocolo de capas de red que contiene información sobre direcciones y algunos datos de control, y permite el ruteo de paquetes. IP es el protocolo primario de capas de red en la suite de protocolos de Internet.
- IPS: Acrónimo de "intrusion prevention system" (sistema de prevención de intrusiones). El IPS va un paso más allá que el IDS y bloquea el intento de intrusión.
- IPSEC: Abreviatura de "Internet Protocol Security" (protocolo de seguridad de Internet). Protocolo estándar que se utiliza para asegurar las comunicaciones IP mediante el cifrado y/o la autenticación de todos los paquetes IP. IPSEC brinda seguridad en la capa de red.
- ISO: Acrónimo de "International Organization for Standardization" (Organización Internacional de Normalización). Organización no gubernamental formada por una red de institutos nacionales de normalización pertenecientes a más de 150 países, con un miembro representante por país. La secretaria central, encargada de coordinar el sistema, se encuentra en Ginebra, Suiza.
- LAN: Acrónimo de "local area network" (red de área local) Red cuya cobertura se limita a un área reducida; en general, un edificio o grupo de edificios.
- LDAP: Acrónimo de "lightweight direct access protocol" (protocolo ligero de acceso directo). Repositorio de datos para la autenticacion y autorizacion

destinado a las consultas y modificaciones relativas a permisos de usuario y al otorgamiento de derechos de acceso a recursos protegidos.

- LPAR: Abreviatura de “logical partition” (partición lógica). Sistema de subdivisión o partición de todos los recursos de un equipo (procesadores, memoria y almacenamiento) en unidades más pequeñas, capaces de ejecutarse con una copia propia distinta del sistema operativo y de las aplicaciones. En general, la partición lógica se utiliza para posibilitar el uso de varios sistemas operativos y aplicaciones en un solo dispositivo. Es posible, aunque no obligatorio, configurar las particiones para que se comuniquen entre si o compartan recursos del servidor, como las interfaces de red.
- MAC: Acrónimo de “message authentication code” (código de autenticación de mensajes). En criptografía, información breve que se utiliza para autenticar un mensaje. Consulte Criptografía solida.
- MPLS: Acrónimo de “multi protocol label switching” (conmutación de etiquetas para protocolos varios). Mecanismo de red o de telecomunicaciones diseñado para conectar un grupo de redes basadas en la conmutación de paquetes.
- NAT: Acrónimo de “network address translation” (traducción de direcciones de red). Llamada simulación de red o simulación IP. Cambio de la dirección IP de una red por una dirección IP distinta conocida dentro de otra red.
- NIST: Acrónimo de “National Institute of Standards and Technology” (Instituto Nacional de Estándares y Tecnología). Agencia federal no regulatoria dependiente de la Administración Tecnológica del Departamento de Comercio de los Estados Unidos. Su misión es promover la innovación estadounidense y la competitividad industrial mediante la promoción de medidas de ciencia, normas y tecnologías que mejoren la estabilidad económica y la calidad de vida.
- NMAP: Software para el análisis de riesgos de seguridad encargado de delinear redes e identificar puertos abiertos en los recursos de red.
- NTP: Acrónimo de “network time protocol” (Protocolo de tiempo de red). Protocolo usado para sincronizar los relojes de sistemas informáticos con redes de datos basadas en la conmutación de paquetes de latencia variable.

- OWASP: Acrónimo de “Open Web Application Security Project” (Guía para proyectos de seguridad de aplicaciones web abiertas). Fundada en 2004, es una organización sin fines de lucro especializada en mejorar la seguridad del software de aplicación. OWASP publico OWASP Top Ten, una lista con las diez vulnerabilidades mas criticas de las aplicaciones web. (Consulte http://www.owasp.org).
- PAN: Acrónimo de “primary account number” (número de cuenta principal), también denominado “número de cuenta”. Numero exclusivo de una tarjeta de pago (en general, de tarjetas de crédito o debito) que identifica al emisor y la cuenta especifica del titular de la tarjeta.
- PA-QSA: Acrónimo de “Payment Application Qualified Security Assessor” (Asesor de seguridad certificado para las aplicaciones de pago), una empresa calificada por el PCI SSC para realizar evaluaciones de aplicaciones de pago de acuerdo con las PA-DSS.
- PAT: Acrónimo de “port address translation” (traducción de dirección de puertos) o “traducción de dirección de puertos de red”. Tipo de NAT que además traduce números de puertos.
- PCI: Industria de tarjetas de pago.
- PDA: Acrónimo de “personal data assistant” (asistente de datos personal) o “personal digital assistant” (asistente digital personal). Dispositivo portátiles manuales que funcionan como teléfonos móviles, redactores de correos electrónicos y navegadores web.
- PIN: Acrónimo de “personal identification number” (número de identificación personal). Contraseña numérica secreta que conocen solo el usuario y un sistema. Este ultimo utiliza el PIN para autenticar al usuario. El usuario tan solo obtiene acceso si su PIN coincide con el PIN del sistema. Los PINs más comunes se utilizan en las operaciones de préstamo de efectivo y las ATM. Otro tipo de PIN es el que utilizan las tarjetas con chip de tipo EMV, en las que el PIN reemplaza la firma del titular de la tarjeta.
- PVV: Acrónimo de “PIN verification value” (valor de verificación de PIN). Valor discrecional codificado en la banda magnética de una tarjeta de pago.

- POS: Acrónimo de “point of sale” (punto de venta). Hardware y/o software que se utiliza para procesar transacciones con tarjetas de pago en la ubicación del comerciante.
- QSA: Acrónimo de “Qualified Security Assessor” (evaluador de seguridad certificado), empresa autorizada por el PCI SSC para realizar evaluaciones in situ del cumplimiento de las normas PCI DSS.
- RADIUS: Abreviatura de “remote authentication and dial-in user service” (autenticación remota y servicio dial-in del usuario). Sistema de autenticación y cuentas. Comprueba que la información transferida al servidor RADIUS, como el nombre de usuario y la contraseña, sea correcta, para autorizar luego el acceso al sistema.
- RBAC: Acrónimo de “role-based access control” (control del acceso basado en funciones). Controles que usuarios específicos autorizados utilizan para restringir el acceso según el grado de responsabilidad del cargo.
- RSA: Algoritmo para criptografía asimétrica descripto en 1977 por Ron Rivest, Adi Shamir y Len Adleman en el MIT (Massachusetts Institute of Technology). Las letras RSA corresponden a las iniciales de sus nombres.
- SANS: Acrónimo de “SysAdmin, Audit, Networking and Security” (Administracion de sistemas, auditorias, redes y seguridad), un instituto especialista en capacitación en seguridad informática y certificación profesional. (Consulte www.sans.org).
- SAQ: Acrónimo de “Self-Assessment Questionnaire” (Cuestionario de autoevaluación). Herramienta utilizada por una entidad para validad su cumplimiento con las normas PCI DSS.
- SDLC: Acrónimo de “system development life cycle” (ciclo de vida de desarrollo del sistema). Etapas del desarrollo de un software o sistema informático que incluye el planeamiento, análisis, diseño, la evaluación e implementación.
- SHA-1/SHA-2: Acrónimo de “Secure Hash Algorithm” (Algoritmo de refundición seguro). Una familia o conjunto de funciones criptográficas de

ordenamiento relacionadas, que incluye SHA-1 y SHA-2. Consulte Criptografía solida.

- SNMP: Acrónimo de "Simple Network Management Protocol" (Protocolo simple de administración de red). Admite la supervisión de dispositivos conectados a una red dada cualquier condición que justifique atención administrativa.
- SQL: Acrónimo de "Structured Query Language" (Lenguaje de consulta estructurado). Lenguaje informático utilizado para crear, modificar y recuperar datos de sistemas de administración de bases de datos relacionales.
- SSH: Abreviatura de "secure Shell". Conjunto de protocolos que proporcionan cifrado de servicios de red, como inicio de sesión remoto o transferencia remota de archivos.
- SSL: Acrónimo de " secure sockets layer" (capa de conexión segura). Estándar industrial establecido que cifra el canal entre un navegador web y un servidor web para garantizar la privacidad y confiabilidad de los datos transferidos por este canal.
- TACACS: Acrónimo de "terminal access controller access control system" (sistema de control de acceso del controlador de acceso a terminales). Protocolo de autenticación remoto que se utiliza generalmente en redes que se comunican entre un servidor de acceso remoto y un servidor de autenticación para determinar los derechos de acceso del usuario a la red.
- TCP: Acrónimo de "Transmission Control Protocol" (Protocolo de control de transmisión). Lenguaje comunicativo o protocolo básico de Internet.
- TDES: Acrónimo de "Triple Data Encryption Standard" (Estándar de cifrado de datos triple), también denominado "3DES" o "Triple DES". Cifrado por bloques formado por un cifrado DES repetido tres veces. Consulte Criptografía Solida.
- TELNET: Abreviatura de "telephone network protocol" (Protocolo de redes telefónicas). En general, se lo utiliza para proporcionar sesiones de inicio con líneas comandos orientadas al usuario para dispositivos de red. Las credenciales del usuario se transmiten en texto simple.

- TLS: Acrónimo de “transport layer security” (seguridad de capa de transporte). Desarrollado para brindar integridad y confidencialidad de datos en la comunicación entre dos aplicaciones. TLS es el sucesor de SSL.
- VLAN: Abreviatura de “virtual LAN” (LAN virtual) o “virtual local área network” (red de área local virtual). Red de área local lógica que se extiende más allá de una sola red física de área local.
- VPN: Acrónimo de “virtual private network” (red privada virtual) Una red informática donde algunas conexiones son circuitos virtuales dentro de redes más extensas, como Internet, en lugar de conexiones directas por medio de cables físicos. Cuando este es caso, los puntos finales de una red virtual se transmiten a través de una red mayor. Al contrario de una aplicación común, formada por comunicaciones seguras en la red pública, una red VPN puede presentar o no funciones de seguridad, como la autenticación y el cifrado de contenidos.
- WAN: Acrónimo de “wide area network” (red de área amplia). Red informática que abarca un área amplia, a menudo parte de un sistema con cobertura en toda una región o empresa.
- WEP: Acrónimo de “wired equivalent privacy” (privacidad equivalente por cable). Algoritmo débil utilizado en el cifrado de redes inalámbricas. Expertos en el tema han informado que la conexion WEP presenta varias debilidades tan serias que puede descifrársela en minutos utilizando herramientas de software comunes. Consulte WPA.
- WLAN: Acrónimo de “wireless local area network” (red de área local inalámbrica). Red de área local que se conecta a dos o más equipos o dispositivos sin cables.
- WPA/WPA2: Acrónimo de “WiFi Protected Access” (acceso protegido WiFi). Protocolo de seguridad creado para asegurar las redes inalámbricas. WPA es la tecnología sucesora de WEP y se la considera más segura que WEP. También se lanzo WPA2, tecnología sucesora de WPA.

CAPITULO 7. REFERENCIAS BIBLIOGRÁFICAS

- http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
- http://www.upc.edu.pe/2/modulos/JER/JER_Interna.aspx?ARE=2&PFL=2&JER=3749
- IT Governance Institute. All rights reserved. www.itgi.org
- http://www.worldlingo.com/ma/enwiki/es/PCI_DSS
- ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems - Requirements
- ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management
- ISO/IEC 27006:2007 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (anterior ISO/IEC 17799:2005)
- ISO 9001:2000, Quality management systems — Requirements
- ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management
- ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security
- ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards
- ISO 14001:2004, Environmental management systems — Requirements with guidance for use

- ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management
- ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing

CAPITULO 8. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La realización de este trabajo consistió en revisar los estándares, normas y marcos teóricos que ha sido importante para el alineamiento.
- El tener información de una entidad financiera y conocer de cerca el proceso de Tarjeta de Crédito, me ha permitido asegurar los controles de seguridad de la entidad financiera.
- Para de crear una metodología para la gestión de prevención del riesgo se necesita un estudio y análisis del método antes presentado.

RECOMENDACIONES

- Se recomienda el uso de los Marcos Teóricos y el mapeo de estos marcos teóricos para ejercer las buenas practicas en la empresa, en este caso financiera.
- Se debe difundir el cumplimiento de la Norma PCI y en el proceso de maduración el organismo de Control Gubernamental (SBS) debería hacerlo mandatario para protección del Tarjetahabiente.