ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROPUESTA DE GESTIÓN DE LAS TIC'S PARA UN SITE ALTERNO DE ENTIDADES BANCARIAS, BASADO EN LAS MEJORES PRÁCTICAS

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MAGISTER (MSc.)

EN GESTIÓN DE LA COMUNICACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

MARIA SOLEDAD PICO MANTILLA

solepico@hotmail.com

PAULINA ELIZABETH PICO MANTILLA

paulina_pico@hotmail.com

DIRECTOR: MSc. GUSTAVO SAMANIEGO

gustavo.samaniego@epn.edu.ec

Quito, Enero 2012

DECLARACIÓN

Nosotros, Pico Mantilla María Soledad y Pico Mantilla Paulina Elizabeth, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Pico Mantilla María Soledad

Pico Mantilla Paulina Elizabeth

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por María Soledad Pico Mantilla y Paulina Elizabeth Pico Mantilla, bajo mi supervisión.

MSc. Gustavo Samaniego

DIRECTOR DE TESIS

CONTENIDO

ÍNDICE DE TABLAS:

ÍNDICE DE FIGURAS:

RESUMEN

Las Entidades Bancarias en el Ecuador se encuentran reguladas por la Superintendencia de Bancos las mismas que para mantener niveles de servicio óptimo en casos de desastres cuentan con alternativas de recuperación que deberán suplir parte o la totalidad de los procesos críticos. La presente propuesta de gestión pretende brindar un marco de referencia para la gestión adecuada de TIC's.

En el capítulo 1 se realiza un análisis de la situación actual de la Entidades Bancarias en el Ecuador, se determina los riesgos a los que están expuestos, así como las características que debe cumplir un Site Alterno para alcanzar los objetivos de la Entidad.

En el capítulo 2 se describen las consideraciones a tomarse en cuenta al momento de seleccionar un Site Alterno. También se determinan las mejores prácticas a ser utilizadas en la gestión de TIC´s en Sites Alternos.

En el capítulo 3 se desarrolla la propuesta de gestión de las TIC´s para un Site Alterno utilizando los cuatro dominios de COBIT y mapeados con ITIL, ISO/IEC y NIST. Como resultado se obtiene la matriz de gestión del Site Alterno.

En el capítulo 4 se realiza la evaluación de la aplicabilidad de la propuesta en Pacificard considerando los aspectos técnico, operacional, legal y económico. A continuación se aplica la matriz de evaluación propuesta en Pacificard.

Finalmente, en el capítulo 5 se exponen las conclusiones y recomendaciones.

CAPÍTULO 1

SITUACIÓN ACTUAL DE LAS ENTIDADES FINANCIERAS EN EL ECUADOR

1.1 INTRODUCCIÓN

En el Ecuador las Entidades bancarias son supervisadas por la Superintendencia de Bancos, y para asegurar las inversiones y dinero de los depositantes se hacen auditorías periódicas a diferentes áreas de la organización. Se revisan los balances contables, las áreas de análisis de riesgo, sistemas, servicio al cliente, estabilidad, contingencias, madurez de los procesos, entre otras. Se asegura la continuidad de la operación de la organización mediante la obtención de altos niveles de integridad, confidencialidad y disponibilidad de la información.

La falta de control estricto a las Entidades Financieras años atrás permitió que en el Ecuador en el año 1999 exista un feriado bancario, en el cual miles de clientes de diferentes Entidades perdieron su dinero. El Estado asumió un determinado valor para devolverlo, sin embargo hubo dinero que no se ha recuperado aún. Se debe tener una revisión adecuada que garantice que estas Entidades realicen sus operaciones de forma apropiada, sin afectar a la sociedad ecuatoriana y garantizando que un evento como este no vuelva a ocurrir.

El atentado del 11 de Septiembre de 2001 a las torres gemelas fue un detonante que prácticamente obligó a Entidades bancarias y empresas de toda índole a poder garantizar que en caso de un atentado, siniestro, accidente, etc.; se pueda continuar con sus operaciones, ocasionando el menor impacto posible a clientes, empleados, accionistas y la sociedad, que podría solventarse con la existencia de un Site Alterno. Con este atentado muchas empresas cerraron definitivamente sus puertas, además se perdió información vital de clientes, facturas, cuentas por cobrar lo que hizo imposible que dichas empresas puedan reabrir sus puertas.

Las Entidades bancarias poseen una infraestructura tecnológica que les permite brindar los servicios, centrados en un centro de cómputo principal o Site principal, de donde se monitorean procesos, se brindan los recursos para que los empleados entreguen servicios a los clientes con procesos óptimos y adecuados.

En el caso de que este Site principal por razones adversas no pueda funcionar, ya sea por falta de recursos tecnológicos, humanos, físicos u otros factores externos; debe existir otro Site, al que por razones de identificación se denominará Alterno que garantice todas las operaciones principales, o las que se consideran vitales en el Plan de Continuidad del Negocio para esta Entidad.

La identificación y evaluación de riesgos debe ser considerada al momento de evaluar la capacidad del Site Alterno, además de definir escenarios estratégicos sobre los cuales se va a trabajar. Las empresas están en la obligación de difundir y entrenar a su personal, para que se mantenga alineado con el plan estratégico de la empresa, y en caso de desastre definir planes que permitan recuperar lo que más valor tenga el negocio.

Es importante garantizar el éxito de este proyecto al momento de una posible implementación, por este motivo se dispondrá de prácticas adecuadas que ayuden al negocio y permitan que el área de Tecnología (TIC´s) ofrezca alta disponibilidad con un nivel de servicio definido, determinando el impacto que cada uno de los diferentes riesgos puede ocasionar en la organización.

Al realizar la presente tesis se está considerando para Entidades Bancarias la legislación ecuatoriana y las regulaciones establecidas por la Superintendencia de Bancos, sin descartar que otro tipo de negocios puedan tomarlo como guía y lo puedan personalizar de acuerdo a sus necesidades.

1.2 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LAS ENTIDADES FINANCIERAS EN EL PAÍS

En el Ecuador el Sistema Financiero Nacional se compone por Bancos Privados, Cooperativas, Mutualistas, Sociedades Financieras y Banca Pública (Ver Anexo 3). Desde el 2005 la tendencia es positiva tanto para Cooperativas, Banca Privada y Banca Pública; los usuarios aumentan, se utilizan los servicios financieros en cuentas corrientes, de ahorros y depósitos a plazo.

El mayor número de depositantes se tiene en cuentas de Ahorro, y el menor número en cuentas a Plazo como se indica en la Tabla 1.1:

SUBSISTEMA	CUENTA	30-jun-10
BANCOS PRIVADOS	**CORRIENTE**	**735801**
	AHORRO	**4397975**
	PLAZO	**103931**
	OTROS	**36342**
TOTAL BANCOS PRIVADOS		**5274049**
COOPERATIVAS	**CORRIENTE**	**-**
	AHORRO	**2485060**
	PLAZO	**101782**
	OTROS	**607673**
TOTAL COOPERATIVAS		**3194515**
MUTUALISTAS	**CORRIENTE**	**-**
	AHORRO	**288541**
	PLAZO	**12086**
	OTROS	**16102**
TOTAL MUTUALISTAS		**316729**
SOCIEDADES FINANCIERAS	**CORRIENTE**	**-**
	AHORRO	**-**
	PLAZO	**20736**
	OTROS	**16**
TOTAL SOCIEDADES FINANCIERAS		**20752**
BANCA PÚBLICA	**CORRIENTE**	**16080**
	AHORRO	**751587**
	PLAZO	**3572**
	OTROS	**10480**
TOTAL BANCA PÚBLICA		**781719**
SISTEMA FINANCIERO NACIONAL	**CORRIENTE**	**751881**
	AHORRO	**7923163**
	PLAZO	**242107**
	OTROS	**670613**
TOTAL SISTEMA FINANCIERO NACIONAL		**9587764**

Tabla 1.1 Número de depositantes por subsistema y tipo de cuenta con corte a junio de 2010 en Ecuador[1].

[1] Fuente: Superintendencia de Bancos y Seguros. Dirección Nacional de Estudios. Subdirección de Estadística, Elaboración: Superintendencia de Bancos y Seguros. Dirección Nacional de Estudios. Subdirección de Estudios

El Ecuador consta de 24 provincias y específicamente en las Provincias de Pichincha y Guayas se puede evidenciar mayores captaciones, así como mayor número de clientes, como se indica en la Tabla 1.2. Lo contrario sucede con la Provincia de Galápagos, la misma que a pesar de tener un alto nivel turístico tiene la menor cantidad de captaciones y saldos de depósitos.

TOTALES POR Provincias	TOTAL DE NÚMERO DE CLIENTES	CUOTA	TÓTAL SALDOS DE DEPÓSITOS	CUOTA
DE BOLIVAR	**106471**	**1,11%**	**76639**	**0,42%**
DE CAÑAR	**163482**	**1,71%**	**233592**	**1,27%**
DE COTOPAXI	**227244**	**2,37%**	**214086**	**1,17%**
DE EL ORO	**372342**	**3,88%**	**436579**	**2,38%**
DE ESMERALDAS	**158683**	**1,66%**	**116666**	**0,64%**
DE GALÁPAGOS	**18828**	**0,20%**	**21330**	**0,12%**
DE IMBABURA	**282771**	**2,95%**	**301206**	**1,64%**
DE LOJA	**345075**	**3,60%**	**386541**	**2,11%**
DE LOS RIOS	**265768**	**2,77%**	**234459**	**1,28%**
DE MANABÍ	**686002**	**7,15%**	**466056**	**2,54%**
DE MORONA SANTIAGO	**97821**	**1,02%**	**68440**	**0,37%**
DE NAPO	**62260**	**0,65%**	**34701**	**0,19%**
DE ORELLANA	**62530**	**0,65%**	**48642**	**0,27%**
DE PASTAZA	**94129**	**0,98%**	**52606**	**0,29%**
DE PICHINCHA	**2483379**	**25,90%**	**8803406**	**48,00%**
DE SANTA ELENA	**90594**	**0,94%**	**58642**	**0,32%**
DE SANTO DOMINGO DE TSÁCHILAS	**213867**	**2,23%**	**214938**	**1,17%**
DE SUCUMBIOS	**92546**	**0,97%**	**63048**	**0,34%**
DE ZAMORA CHINCHIPE	**37035**	**0,39%**	**24896**	**0,14%**
DEL AZUAY	**687585**	**7,17%**	**1430561**	**7,80%**
DEL CARCHI	**153704**	**1,60%**	**96946**	**0,53%**
DEL CHIMBORAZO	**251367**	**2,62%**	**323634**	**1,76%**
DEL GUAYAS	**2176409**	**22,70%**	**4023582**	**21,94%**
DEL TUNGURAHUA	**457872**	**4,78%**	**609023**	**3.32%**
Total General	**9587764**	**100,00%**	**18340219**	**96,69%**

Tabla 1.2 Sistema financiero nacional captaciones por provincia con corte a junio de 2010. En dólares y porcentajes [2]

[2] Fuente: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estadística.
Elaboración: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estudios.

La Superintendencia de Bancos utiliza tanto el indicador de bancarización como el indicador de profundización para los análisis del Sistema Financiero Nacional.

1. El indicador de Bancarización del Sistema Financiero Nacional SFN relaciona el número de depositantes frente a la población total[3]. A continuación en la

SUBSISTEMA	dic-05	dic-06	dic-07	dic-08	dic-09	dic-10
Bancos	**24,98%**	**26,52%**	**27,61%**	**32,58%**	**36,03%**	**37,14%**
Cooperativas	**10,64%**	**10,51%**	**16,85%**	**18,59%**	**20,50%**	**22,50%**
Mutualistas	**1,87%**	**0,95%**	**2,64%**	**2,07%**	**2,18%**	**2,23%**
Soc. Financieras	**0,08%**	**0,09%**	**0,12%**	**0,09%**	**0,13%**	**0,15%**
Banca Pública	**1,34%**	**1,36%**	**2,44%**	**3,78%**	**6,66%**	**5,51%**
Sistema Financiero Nacional	**38,91%**	**39,43%**	**49,66%**	**57,11%**	**65,50%**	**67,53%**

Tabla 1.3 Bancarización del sistema financiero nacional[4]. Indicadores obtenidos en los últimos años por cada Subsistema del Sistema Financiero Nacional.

2. El índice de Profundización Financiera mide la relación tanto de las captaciones como de la cartera frente al Producto Interno Bruto PIB[5], existe profundización financiera de depósitos como se muestra en la Figura 1.1 y de cartera como se muestra en la Figura 1.2.

[3] www.superban.gob.ec

[4] Fuente: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estadística.
Elaboración: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estudios.

[5] www.superban.gob.ec

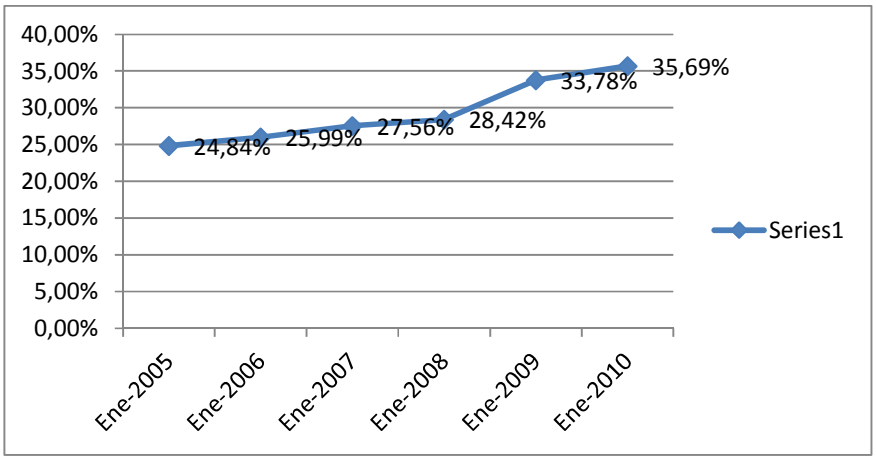


Figura 1.1 Profundización financiera de depósitos Ene. 2005 - Ene. 2010[6]

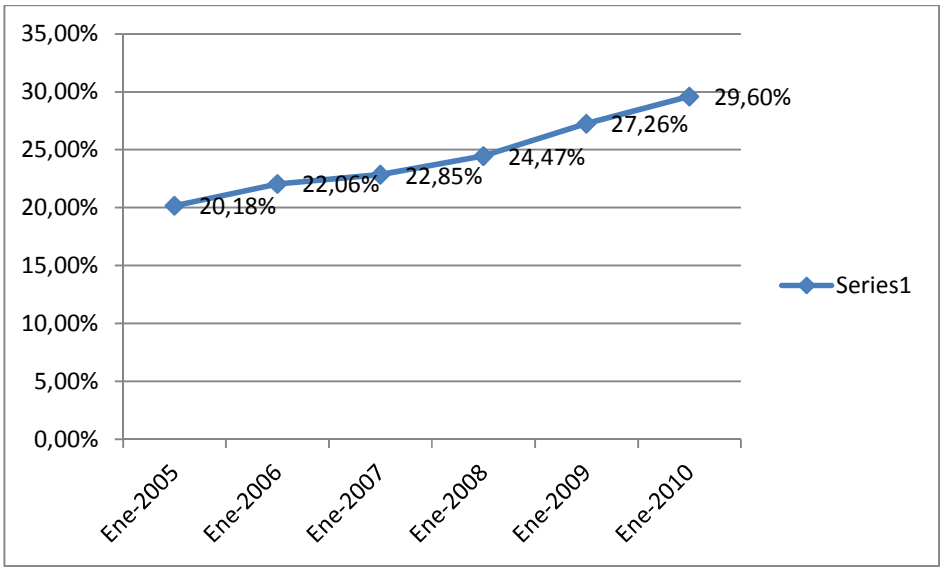


Figura 1.2 Profundización financiera de cartera de créditos Ene. 2005 - Ene. 2010[7]

Las figuras 1.1 y figura 1.2 permiten identificar que hubo un incremento en los procesos de Bancarización y Profundización Financiera en los últimos años.

[6]Fuente: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estadística.
Elaboración: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estudios

[7] Fuente: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estadística.
Elaboración: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estudios

1.2.1 OBLIGACIONES DE LAS ENTIDADES BANCARIAS

Para asegurar el estado financiero de una Entidad, es indispensable tener información real de la situación financiera de la misma, por eso las empresas reguladoras basan sus operaciones en una serie de controles que garanticen que los datos obtenidos son reales. Para ello las Entidades financieras deben cumplir con las recomendaciones de Basilea y SOX (Ver Anexos 1 y 2).

Se va a considerar estas exigencias al momento de la implantación del Site alterno.

1.2.2 TIPOS DE INFORMACION QUE SE GENERA

Al momento las Entidades generan información de diferente índole y con varios niveles de confidencialidad por citar algunos ejemplos:

1. Impresa.- Todo documento tangible generado con ayuda de un equipo de computación, de impresión o una máquina de escribir. Por ejemplo: reportes, documentos firmados, documentos sellados, contratos etc.
2. Escrita.- Toda documentación que se encuentra en un archivo físico por un tiempo determinado por la superintendencia de bancos, generado de manera manual. Ejemplo: Sumillas, firmas, disposiciones, cartas, calificaciones de riesgo.
3. Electrónica.- Toda información que se ha generado de manera digital. Ejemplo: información personal de clientes, transacciones, obligaciones de cada empleado, disposiciones, bases de datos. Generadas en medios como tape backup, CDs, diskettes, DVDs, discos externos, etc.
4. Correos electrónicos.- Algunas transacciones y procesos de cada área, empiezan con una solicitud que se envió mediante un correo electrónico,

además hay información que se comunica a los involucrados por esta vía. En determinados casos puede servir como evidencia de un determinado proceso.

5. Enviada por correo electrónico.- En el correo electrónico es posible adjuntar archivos que contienen información del negocio, como por ejemplo: archivos con extensiones (doc, docx, xls, xlsx, ppt, pptx, pdf, jpeg, etc.).
6. Películas y Grabaciones.- Toda información de la empresa que con apoyo de medios como filmadoras, cámaras, micrófonos, son de vital importancia para la empresa y generan fuente de conocimiento.
7. Conversaciones y Conferencias.- Actualmente las empresas cuentan ya con salas de video conferencias y toda información que se genere en las mismas debe respaldarse.

1.3 BUENAS PRÁCTICAS DE ENTIDADES BANCARIAS EN ECUADOR

A continuación se va a describir algunas de las buenas prácticas reconocidas llevadas a cabo en algunas Entidades bancarias del país.

Para seleccionar los bancos, de los cuales se toman las mejores prácticas, se consideran los siguientes aspectos:

- ✓ Información publicada en Internet y de fácil acceso para poderla investigar y analizar sus mejores prácticas. (Banco de Guayaquil, Banco Bolivariano)
- ✓ Bancos o Entidades financieras que tienen varias oficinas a nivel nacional y son de fácil reconocimiento para el público en general. (Banco de Guayaquil, Banco del Pichincha, Pacificard)
- ✓ Banco del cual dependen otros bancos para realizar sus transacciones. (Banco Central del Ecuador)

- ✓ Entidad financiera que tiene un Site Alterno, para poder evaluar la propuesta desarrollada en el siguiente plan. (Pacificard)

Luego de la evaluación de los siguientes puntos se escogió a los siguientes bancos y Entidades bancarias para la revisión de sus mejores prácticas.

- Banco de Guayaquil
- Banco del Pichincha
- Banco Central del Ecuador
- Banco Bolivariano
- Pacificard

1.3.1 BANCO DE GUAYAQUIL

El Banco de Guayaquil es una Entidad bancaria que realiza sus gestiones en el Ecuador y se rige a las normas establecidas por la Superintendencia de Bancos, a continuación se va a detallar un poco sobre el funcionamiento de esta Entidad y como esta Entidad contribuye a la prevención de fraudes y robos informáticos, mostrando de esta manera su contribución de buenas prácticas para esta Entidad y sus clientes en general.

Gobierno Corporativo.- El banco de Guayaquil al igual que otras empresas modernas fortalece su administración a través de un gobierno corporativo dinámico y eficiente, estableciendo sólidas prácticas apoyadas en el marco de las políticas el Comité de Basilea

Para contribuir a cumplir las metas del Banco de Guayaquil, se tienen varios comités, entre los cuales se destacan el comité de auditoría, comité integral de

administración de riesgo y comité de sistemas, que contribuyen a desarrollar mejores prácticas de TI para esta Entidad y ayudar con planes de continuidad del negocio.

1.3.1.1 Estructura Organizacional del Banco de Guayaquil

La estructura está conformada por el Directorio, los Comités Normativos, los Comités Gerenciales y Estructura Administrativa.

A continuación se detalla los objetivos de cada ente del gobierno corporativo:

El Directorio del Banco es responsable principalmente de:

1. Definir la Política financiera y crediticia, y de controlar su ejecución;
2. Analizar y pronunciarse sobre los informes de riesgos crediticios y de la proporcionalidad y vigencia de las garantías otorgadas.
3. Conocer y aprobar los resultados financieros y el informe de auditoría interna.
4. Conocer y resolver sobre el aumento de capital suscrito y pagado del Banco.
5. Elegir a los representantes legales del Banco.
6. Autorizar y aprobar el presupuesto del Banco; y además atribuciones constantes en el Estatuto Social del Banco y la Ley General de Instituciones del Sistema Financiero.

1.3.1.2 Mejores Prácticas Utilizadas por el Banco de Guayaquil

De acuerdo al boletín publicado en mayo 2011[8], el Banco de Guayaquil tiene en operación su Banca Virtual, el mismo que ingresa con su usuario y contraseña, la comunicación con el cliente es mediante una capa de conexión segura.

Para activar esta seguridad, el cliente se acerca al banco y solicita la tarjeta de coordenadas, una vez recibida ingresa al portal Web del banco y debe seguir varias instrucciones.

Finalmente para la activación debe ingresar las coordenadas aleatorias que el banco le solicite.

El Banco de Guayaquil tiene la siguiente política de seguridad:

En el Banco de Guayaquil contamos con la más alta tecnología para mantener las seguridades adecuadas y salvaguardar los intereses de nuestros clientes, contamos además con personal idóneo que trabaja permanentemente para que el manejo de la información financiera de nuestros clientes sea confidencial e íntegro.

Realiza un constante monitoreo transaccional, para contrarrestar las diferentes modalidades de fraude, con sofisticadas herramientas de análisis de transacciones que permiten identificar operaciones inusuales y prevenir posibles fraudes.

Cumple con el “Sigilo” y “Reserva Bancaria”, exigido por la Superintendencia de Bancos para guardar reserva y discreción sobre los datos de sus clientes.

También se dan políticas de cómo proteger el computador de los clientes que acceden vía Internet a la página del Banco. Se dan recomendaciones sobre el uso de:

Antivirus, Antipharming, Antimalware, Antyspyware, Parches del sistema operativo, Firewall, Protección de la red WI-Fi

[8] http://www.portal.banred.fin.ec/images/stories/Boletin/2011/boletinmayo2011.pdf

Se muestra también consejos de seguridad en canales como:

- ✓ Seguridades en el Manejo de Chequeras
- ✓ Seguridades con las Tarjetas de Crédito
- ✓ Seguridades con las Tarjetas de Débito
- ✓ Seguridades en claves y Tarjetas Bancontrol
- ✓ Seguridad en Internet
- ✓ Seguridades con los cajeros automáticos
- ✓ Seguridades en oficinas y/o Ventanillas

Se detallan algunos fraudes con tarjetas y en oficinas:

- ✓ Cambiazo
- ✓ Clonación de Tarjetas
- ✓ Cajeros Gemelo
- ✓ Suplantación de idEntidad
- ✓ Sacapintas
- ✓ Suplantación de empleados

Se detallan algunos fraudes en Internet como:

- ✓ Troyano Bancario
- ✓ Robo de clave
- ✓ Espía en la red
- ✓ Clickjacking
- ✓ Robo de identidad
- ✓ Reenvío de correos en cadena
- ✓ Ingeniería Social

- ✓ Cross-Site Scripting
- ✓ Phishing
- ✓ Pharming
- ✓ Intruso Virtual

1.3.2 BANCO DEL PICHINCHA

Banco del Pichincha es un banco ecuatoriano que cuenta con la mayor cantidad de clientes en nuestro país, basando este en la cantidad de agencias y sucursales que tiene a lo largo de todo el territorio ecuatoriano.

El Banco del Pichincha actualmente, es uno de los bancos más grandes del país por lo cual ha sufrido muchos ataques que han afectado a varios de sus clientes y por lo tanto a su imagen, esto ha servido como premisa para que el banco implemente un sistema biométrico que brinde mayor seguridad a sus cliente mientras realizan sus transacciones por Internet.

De acuerdo al boletín de mayo 2011[9], las Entidades financieras deben fortalecer su imagen frente a sus clientes mejorando sus niveles de seguridad y entre una de las mejores prácticas del Banco del Pichincha está el sistema biométrico que esta Entidad brinda a sus clientes.

1.3.2.1 Sistema Biométrico

Se aclara que un sistema biométrico, debe ser mediante el reconocimiento de huellas digitales o pupila del ojo, pero en este caso se va a hacer mediante claves usadas desde un computador o celular.

[9] http://www.portal.banred.fin.ec/images/stories/Boletin/2011/boletinmayo2011.pdf

El cliente ingresa a la página del Banco del Pichincha, solicita su clave biométrica, para lo cual el banco pide datos del cliente, cómo cedula y clave de su tarjeta Xperta, y se aceptan las condiciones del contrato para el uso del sistema biométrico, el cliente debe ingresar su información correo electrónico y celular, un sistema similar a otras Entidades bancarias, luego el sistema pide recordar preferencias personales de los clientes y un nombre de usuario.

1.3.3 BANCO CENTRAL DEL ECUADOR

A partir del 30 de junio de 1998, mediante la expedición del Decreto Ejecutivo # 1564, el Banco Central del Ecuador puso en vigencia su nueva estructura organizacional basada en procesos.

El Banco Central del Ecuador tiene un estatuto que debe cumplir, el cual deben acatar las diferentes Entidades bancarias ecuatorianas, por lo tanto la adopción de buenas prácticas de esta Entidad, sirve de ejemplo para otras Entidades bancarias del país.

Actualmente se ha adoptado la estructura organizacional por procesos, para lo cual utilizaron la siguiente metodología:

a) Se identificaron los clientes externos de la banca central, que justifican la existencia de la institución.

b) Se determinaron los productos Por producto se entiende los bienes o servicios que genera la institución.

Asociados a dichos clientes, que son inherentes a la misión o naturaleza del instituto emisor y que dan valor agregado a sus responsabilidades.

c) Se establecieron y delimitaron los procesos que generan dichos productos institucionales.

d) El conjunto de actividades que producen un bien o servicio que se integra o complementa a otro producto de mayor valor agregado se definió como subproceso.

e) Por su diferente forma de contribuir a la institución, se establecieron cuatro clases de procesos:

Procesos Gobernadores, los encaminados a aprobar políticas, normas, procedimientos, a planificar y dirigir la organización.

Procesos Creadores de Valor, los encargados de generar aquellos productos esenciales a la misión del Banco Central del Ecuador.

Procesos Habilitantes, los orientados a producir los bienes y servicios requeridos por los procesos gobernadores, creadores de valor y para sí mismos.

Procesos Especiales, los que tienen a su cargo la ejecución de las políticas cultural y social de la institución.

Esta estructura propuesta permite ver a la organización como una sola red tecnológica-administrativa geográficamente integrada y no como el conjunto de unidades funcionales aisladas.

Los procesos corresponden a una estructura de banca central moderna, con características de versatilidad que responde a las necesidades del presente y desafíos del futuro.[10]

1.3.4 BANCO BOLIVARIANO

CAF-banco de desarrollo de América Latina- y el Banco Bolivariano (BB), firmaron una cooperación técnica no reembolsable para establecer principios y lineamientos que permitan la adopción e implementación de buenas prácticas de Gobierno Corporativo en la institución bancaria.

[10] http://www.bce.fin.ec/contenido.php?CNT=ARB0000869

Esta es la primera intervención específica de CAF en la implementación de prácticas de Gobierno Corporativo en una institución financiera en el Ecuador con la finalidad de generar un importante efecto demostrativo para el sector financiero del país.

El Programa de Gobierno Corporativo busca contribuir, a través de la promoción de buenas prácticas, a la competitividad responsable, tanto a nivel de las empresas como a nivel sectorial y macroeconómico.

La adopción de prácticas de Gobierno Corporativo trae consigo importantes beneficios para las empresas que las aplican, tales como la reducción del riesgo para los inversionistas y los acreedores, y elevan su valor a favor de los accionistas.

El trabajo desde CAF para la promoción de buenas prácticas de Gobierno Corporativo inició desde el año 2004, con la elaboración, redacción y difusión de los Lineamientos para un Código Andino de Gobierno Corporativo, aplicable a los cinco países de la Comunidad Andina de Naciones.

Banco Bolivariano nació el 13 de marzo del año 1980 y bajo el manejo de una administración eficiente, logró colocarse como una de las Entidades sólidas del mercado ecuatoriano. Mantiene elevados niveles de calidad de activos, rentabilidad y liquidez comparados con el sistema financiero ecuatoriano.

CAF -banco de desarrollo de América Latina- tiene como misión impulsar el desarrollo sostenible y la integración regional, mediante el financiamiento de proyectos de los sectores público y privado, la provisión de cooperación técnica y otros servicios especializados. [11]

[11] http://www.elciudadano.gov.ec/index.php?option=com_content&view=article&id=18742:caf-y-el-banco-bolivariano-impulsan-___practicas-de-buen-gobierno-corporativo-en-sector-financiero.

1.3.5 PACIFICARD

Pacificard S.A.[12] es una empresa emisora y administradora de tarjetas de Crédito-Pago servicios del tarjetahabiente y procesamiento Operativo a Terceros.

Hace 30 años varios inversionistas junto con el Banco del Pacífico, constituyeron la primera empresa emisora y administradora de tarjetas de crédito del Ecuador, misma que nació con el nombre de Unicredit. Luego de 14 años de exitoso desempeño, su razón social cambió a MasterCard del Ecuador. En el 2003 y fruto de los deseos de seguir desarrollando el mercado de medios de pago en el Ecuador, se da su última transformación a PacifiCard S.A., incorporando la administración de la marca Visa.

Actualmente Pacificard tiene la certificación ISO 9001:2008, para cumplir la misma todos los procesos fueron documentados y estandarizados, incluyendo al área de sistemas.

Entre las mejores prácticas de Pacificard, se destaca asegurar la seguridad de sus clientes, un ejemplo es a la adopción de tarjetas con Chip, para combatir a mafias mundiales que se dedican a la clonación de tarjetas[13].

Para asegurar la seguridad de sus clientes en transacciones realizadas por Internet, Pacificard utiliza Verified by Visa y Mastercard Secure Code, los cuales solicitan una clave adicional al cliente.

En la página Web de Pacificard se da a los clientes consejos de seguridad que deben adoptar para evitar sufrir fraudes con sus tarjetas.

Pacificard cuenta con un área de Prevención de fraudes, adoptando así una buena práctica que garantice la seguridad de sus clientes.

[12] https://www.pacificard.com.ec/quienes-somos.aspx
[13] http://www.hoy.com.ec/noticias-ecuador/pacificard-implementa-chip-de-seguridad-286999-286999.html

Entre las buenas prácticas de Pacificard es muy notoria su preocupación adoptando políticas en su portal Web, que previenen ingresos no autorizados.

1.4 DETERMINACIÓN DE LOS PRINCIPALES RIESGOS PARA LAS ENTIDADES BANCARIAS

A continuación se va a definir para las Entidades Bancarias los riesgos bancarios y los riesgos informáticos.

1.4.1 RIESGOS BANCARIOS

En el Ecuador las Entidades Calificadoras de Riesgo que tienen facultad de extender una calificación, previo análisis son:

- HUMPHREYS S. A.
- MICROFINANZAS SRL
- BANK WATCH RATINGS
- PCR PACIFIC S.A

Las calificaciones que se pueden otorgar son las siguientes:

AAA	La situación de la institución financiera es muy fuerte y tiene una sobresaliente trayectoria de rentabilidad, lo cual se refleja en una excelente reputación en el medio, muy buen acceso a sus mercados naturales de dinero y claras perspectivas de estabilidad. Si existe debilidad o vulnerabilidad en algún aspecto de las actividades de la institución, ésta se mitiga enteramente con las fortalezas de la organización;
AA	La institución es muy sólida financieramente, tiene buenos antecedentes de desempeño y no parece tener aspectos débiles que se destaquen. Su perfil general de riesgo, aunque bajo, no es tan favorable como el de las instituciones que se encuentran en la categoría más alta de calificación;
A	La institución es fuerte, tiene un sólido récord financiero y es bien recibida en sus mercados naturales de dinero. Es posible que existan algunos aspectos débiles, pero es de esperarse que cualquier desviación con respecto a los niveles históricos de desempeño de la Entidad sea limitada y que se superará rápidamente. La probabilidad de que se presenten problemas significativos es muy baja, aunque de todos modos ligeramente más alta que en el caso de las instituciones con mayor calificación;
BBB	Se considera que claramente esta institución tiene buen crédito. Aunque son evidentes algunos obstáculos menores, éstos no son serios y/o son perfectamente manejables a corto plazo;
BB	La institución goza de un buen crédito en el mercado, sin deficiencias serias, aunque las cifras financieras revelan por lo menos un área fundamental de preocupación que le impide obtener una calificación mayor. Es posible que la Entidad haya experimentado un período de dificultades recientemente, pero no se espera que esas presiones perduren a largo plazo. La capacidad de la institución para afrontar imprevistos, sin embargo, es menor que la de organizaciones con mejores antecedentes operativos:
B	Aunque esta escala todavía se considera como crédito aceptable, la institución tiene algunas deficiencias significativas. Su capacidad para manejar un mayor deterioro está por debajo de las instituciones con mejor calificación;
C	Las cifras financieras de la institución sugieren obvias deficiencias, muy probablemente relacionadas con la calidad de los activos y/o de una mala estructuración del balance. Hacia el futuro existe un considerable nivel de incertidumbre. Es dudosa su capacidad para soportar problemas inesperados adicionales;
D	La institución tiene considerables deficiencias que probablemente incluyen dificultades de fondeo o de liquidez. Existe un alto nivel de incertidumbre sobre si esta institución podrá afrontar problemas adicionales;
E	la institución afronta problemas muy serios y por lo tanto existe duda sobre si podrá continuar siendo viable sin alguna forma de ayuda externa, o de otra naturaleza.
	A las categorías descritas se pueden asignar los signos (+) o (-) para indicar su posición relativa dentro de la respectiva categoría.

Tabla 1.4 Profundización financiera de cartera de créditos[14].
Fuente: Superintendencia de Bancos y Seguros

[15] Fuente: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Suddirección de EstadísticaElaboración: Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Suddirección de Estudios

Entre los riesgos bancarios que existen se pueden considerar los siguientes: fraudes, robo de dinero, seguridades físicas y lógicas vulnerables, lavado de dinero, falta de liquidez, información no real proporcionada por accionistas o clientes de la Entidad bancaria, utilización de testaferros, malas inversiones por parte de los accionistas, incendios.

Se consideran también a los desastres naturales como por ejemplo inundaciones, terremotos, deslaves, eventos en la zona como la corriente fría del niño.

Existen los riesgos informáticos tales como robo de información, falta de actualización tecnológica, falta de control de acceso lógico, información desactualizada, falta de políticas de respaldos, problemas de concurrencia, problemas de red, falta de procedimientos de rollback.

Entre los riesgos operativos bancarios ya sean voluntarios e involuntarios se tienen falta de procedimientos y controles, falta de ética profesional por parte de las personas que trabajan en la institución, falta de liderazgo, falta de buenas prácticas, falta de difusión de seguridades y cuidados que deben tener hacia los clientes.

Entre los riesgos gubernamentales y legales que afectan a las Entidades bancarias se tienen: Leyes de Gestión Tributaria, Paquetazos económicos, Incumplimiento o Desconocimiento de las leyes como por ejemplo la Ley del Comercio Electrónico.

1.4.2 RIESGOS INFORMÁTICOS

Con el apoyo de una metodología es posible obtener un reporte de análisis de riesgos, cada paso describe la información de entrada de entrada y de salida.

1.4.2.1 Metodología

En la actualidad existen una gama de metodologías con las cuales las Entidades Bancarias pueden cumplir los objetivos propuestos y proteger uno de los principales activos que tienen que es la información.

La metodología que se utilizará es la publicada por NIST SP 800-30 que es la Guía de Gestión de Riesgos para Sistemas de Tecnología de Información, con la finalidad de identificar las amenazas y los riesgos asociados.

Para una mejor comprensión es necesario manejar algunos conceptos:

Riesgo: Evento que pueda impedir alcanzar un objetivo.

Vulnerabilidad: Alguna debilidad que podría ser explotada

Amenaza: Existencia de peligro de que ocurra algo.

La Administración de Riesgos para Sistemas Tecnología de Información, será utilizada para identificar los riesgos que afectan a las Entidades de Emisión de Tarjetas de crédito[15].

1. *Caracterización de los sistemas*

Se establece el alcance de la evaluación del riesgo, en este caso se realizó una evaluación de riesgos al Site Principal, que conlleva a la necesidad de mantener un Site Alterno, para este caso se considera hardware, software, comunicaciones, datos, información, usuarios del sistema, políticas de seguridad, arquitectura, seguridad ambiental, mandos de funcionamiento, controles técnicos, etc.

2. *Identificación de amenazas*

[15] Special Publication Nist 800-30, Gary Stoneburner, Alice Goguen, and Alexis Feringa

Identificar las amenazas de la posibilidad de ejercer una determinada vulnerabilidad.

Problemas eléctricos

Problemas de telecomunicaciones

Problemas de hardware y software

Las amenazas naturales como inundaciones, terremotos, tornados, deslizamientos, avalanchas, tormentas eléctricas y otros eventos.

Las amenazas operativas, son aquellas que pueden ser causadas por seres humanos.

Las amenazas ambientales, contaminación, productos químicos, etc.

Amenazas informáticas, como actos intencionales, entrada inadvertida de datos, o acciones deliberadas red los ataques basados en, cargar software malicioso, sin autorización acceso a información confidencial.

Configuración física

3. Identificación de vulnerabilidades

Las vulnerabilidades son las debilidades, las mismas deben ser identificadas y listadas para ser gestionadas adecuadamente.

4. Análisis de Controles

Analizar los controles existentes o que están por implementarse para minimizar la probabilidad de ocurrencia.

Vulnerabilidad	**Fuente de Amenaza**	**Acción para la amenaza**
Problemas eléctricos	Racionamiento de energía, corto circuito, incendios, etc.	Planta eléctrica
Problemas informáticos	Virus, spam, ataques, software malicioso, gusanos, etc	Parches y actualizaciones
Problemas en Configuración física	Cambios sin de controles de cambios adecuados	Mantener una gestión adecuada de configuración
Problemas de telecomunicaciones	Caída de los enlaces	Notificar al personal involucrado para que proceda a levantarlo.
Problemas de Hardware	Equipos sensibles a variación de voltaje Daños de fábrica	Reposición de piezas o mantenimiento adecuado, compra.
Problemas de Software	Daño en las aplicaciones	Restaurar las aplicaciones con los respaldos

Tabla 1.5 Vulnerabilidades y amenazas para un Site Alterno
Fuente: NIST SP 800-30

5. Determinación de la Probabilidad

En este paso se debe determinar la probabilidad de que alguna vulnerabilidad se lleve a cabo.

Nivel	Descripción
Alto	Las amenazas es latente y los controles no logran mitigarlas adecuadamente
Medio	Las amenazas son latentes pero es posible, aplacarlas con los controles que se tienen
Bajo	La amenaza es baja, sin embargo en caso de que se llevará a cabo los controles son suficientes.

Tabla 1.6 Descripción de los niveles de amenazas
Fuente: NIST SP 800-30

6. Análisis de Impacto

Determinar el nivel de afectación en caso de que un riesgo llegara a concretarse.

Magnitud de Impacto	Definición
Alto	Alta vulnerabilidad, puede resultar un alto costo en pérdida de bienes materiales o recursos, puede causar daños irreparables.
Medio	Media vulnerabilidad, puede resultar una pérdida costosa de materiales o recursos, puede ocasionar daños evidentes.
Bajo	Baja vulnerabilidad, puede resultar la pérdida de materiales o recursos, que podrían recuperarse.

Tabla 1.7 Descripción de la Magnitud de Impacto
Fuente: NIST SP 800-30

7. Determinación de riesgos

Se trabaja con una matriz de riesgo para determinar los niveles de riesgo.

	Bajo Impacto	Medio Impacto	Alto Impacto
Amenaza Alta	Bajo	Medio	Alto
Amenaza Media	Bajo	Medio	Medio
Amenaza Baja	Bajo	Bajo	Bajo

Tabla 1.8 Matriz de niveles de riesgo
Fuente: NIST SP 800-30

8. Recomendaciones de Control

Se proponen controles que mitiguen el riesgo y que estén dentro de las operaciones que Pacificard debe realizar.

9. Documentar resultados

Luego de una adecuada y rigurosa evaluación de riesgos, se debe documentar y entregar un reporte para ser usado por Pacificard. En estos resultados es importante definir la eficacia de acciones definidas, el cumplimiento de las leyes, la política de la organización, el impacto operacional, la Seguridad y fiabilidad.

1.4.2.2 Resultados – Reporte de Evaluación de Riesgos

El propósito de la Evaluación de riesgos para Entidades Bancarias, determina varios riesgos que pueden impedir entregar servicios de calidad, considerando que dependen de la infraestructura.

Por lo tanto se hace una lista de posibles riesgos que podría ocasionar que el Site Principal deje de funcionar, en estos casos debe empezar a funcionar el Site Alterno y debe presentar las garantías para proveer los servicios que se determinaron debe brindar en los tiempos propuestos y estimados.

Considerando que se necesita restaurar servicios y ayudar a la continuidad del negocio se incluyeron las siguientes áreas:

Seguridad de la Información

Operadores

Infraestructura

Telemática

Manejo de servidores de Iseries

1.4.2.3 Enfoque de la Evaluación de Riesgos

Para la evaluación de riesgos se tomó en cuenta riesgos considerados por la Superintendentencia de Bancos y personal de Pacificard encargado de garantizar la continuidad del negocio.

Se va a trabajar con una matriz donde en la parte superior se va a poner si el impacto es alto, medio o bajo y en lado izquierdo la calificación de la amenaza, si es alta, media o baja.
A continuación las puntuaciones que determinan si la calificación de amenaza e impacto son alta, media o baja, dependiendo de cada riesgo.

PROBABILIDAD DE AMENAZA	IMPACTO		
	BAJO (10)	MEDIO (50)	ALTO (100)
ALTA (1.0)	Bajo 10x1.0=10	Medio 50x1.0=50	Alto 100x1.0=100
MEDIA (0.5)	Bajo 10x0.5=5	Medio 50x0.5=25	Medio 100x0.5=50
BAJA (0.1)	Bajo 10x0.1=1	Bajo 50x0.1=5	Bajo 100x0.1=10

Tabla 1.9 Matriz de nivel de riesgo
Fuente: NIST SP 800-30

La probabilidad de Amenaza se determina como alta, media o baja considerando:

Alta: Fuente de amenaza altamente motivada, con controles de prevención que pueden ser inefectivos.

Media: La fuente de amenaza es posible pero los controles considerados pueden funcionar de manera adecuada.

Baja: La amenaza es poco probable, y con los controles considerados pueden responder efectivamente a estas amenazas.

Las definiciones de Magnitud de Impacto son alta, media y baja, se explican de la siguiente manera:

Alta: Alta pérdida de principales activos tangibles y recursos, violación daño o dificultad de la misión de la empresa y puede resultar en muerte humana o lesión seria.

Media: Pérdida de activos tangibles, dificultad de la misión de la empresa, puede resultar en una lesión humana.

Baja: Pérdida de algunos activos, puede afectar notablemente a la reputación e interés de la organización. [16]

[16] Special Publication Nist 800-30, Gary Stoneburner, Alice Goguen, and Alexis Feringa,

Paso 1 Caracterización del sistema

Se va a describir la importancia del Site Principal y del Site Alterno para el desempeño normal de Pacificard.

Criticidad del Sistema	Categoría de sensibilidad
Confidencialidad	Alta
Integridad	Alta
Disponibilidad	Alta

Tabla 1.10 Criticidad y sensibilidad del Site Principal
Fuente: NIST SP 800-30

Criticidad del Sistema	Categoría de sensibilidad
Confidencialidad	Media
Integridad	Media
Disponibilidad	Media

Tabla 1.11 Criticidad y sensibilidad del Site Alterno
Fuente: NIST SP 800-30

Cabe indicar que los datos del Site Altero, son estos mientras siga siendo un Site de Respaldo, el momento de una contingencia esta pasaría a tener los valores del Site Principal.

Paso 2 Identificación de Amenazas

A continuación se va a detallar Fuentes de amenaza potenciales y las principales consecuencias que cada una de ellas conlleva.

A continuación se describen amenazas

No	Amenaza	Acciones de la Amenaza
1	• Terremoto	• Destrucción infraestructura y construcción • Personal afectado.
2	• Temblor	• Destrucción parcial de infraestructura
3	• Tormenta Eléctrica	• Suspensión del servicio de energía eléctrica. • Equipos quemados por variación de voltaje
4	• Incendio en el sector	• Pérdida de suministro eléctrico • Bloqueo de movilización para entrar y salir de las instalaciones • Falta de servicio
5	• Incendio en el edificio	• Pérdida de suministro eléctrico, y su contingencia que es el generador del banco. • Destrucción de infraestructura tecnológica • Destrucción de infraestructura física • Bloqueo de puertas • Equipos quemados • Personal afectado • Pérdidas de información. • Falta de disponibilidad de servicios • Pérdida de configuraciones
6	• Humedad/Sobrecalentamiento/Inundaciones	• Daño de equipos. • Enfermedades • Mantenimiento se incrementa • Disminuye el tiempo de vida útil de equipos
7	• Animales/ Plagas	• Daños en equipos. • Enfermedades

No	Amenaza	Acciones de la Amenaza
8	• Cambios continuos del personal	• Costos de capacitación, reorganización y nuevas asignaciones de responsabilidades y actividades.
9	• Ingresos no autorizados al sistemas por personal externo	• Controles inadecuados
10	• Daños causados por personal interno	• Ingreso de virus por el uso de memorias USB con virus. • Divulgación de información de manera indebida • Pérdida de confidencialidad e integridad de los datos: entrada de datos falsificados, corrompidos. • Venta/intercambio de información personal. • Fallas del sistema. • Intrusión al sistema. • Sabotaje al sistema. • Acceso no autorizado al sistema.
11	• Administración indebida	• Fallas en el sistema. • Accesos no autorizados. • Pérdida de confidencialidad.
12	• Robo	• Costos para reposición de equipos. • Falta de disponibilidad. • Pérdida de confidencialidad.
13	• Phishing	• Obtienen información confidencial a través del correo electrónico. • Obtienen información al sustituir páginas por otras muy parecidas.
14	• Pharming	• Obtienen claves a través de redireccionar al usuario a páginas muy similares a las de bancos.
15	• Malware, troyanos, keyloggers	• Captar y grabar las teclas y combinaciones de teclas usadas para ingresar en una página web
16	• Skimming	• Grabar la información de una tarjeta al pasar por un aparato llamado skimmer para luego colocarla en una clonada
17	• Estafa piramidal, hoax, carta nigeriana	• A través de una red social se trata de convencer de invertir o entregar claves
18	• Caída de los Sistemas	• Impide la atención a Usuarios • Posibles daños en las Aplicaciones

Tabla 1.12 Fuentes de Amenaza
Fuente: www.sbs.gob.ec[17]
Elaborado por: autores

[17] www.sbs.gob.ec, 27 de diciembre de 2011

Pasos 3 y 4 Identificación de Vulnerabilidades y Análisis de Controles

No	Amenaza	Vulnerabilidad	Controles para mitigar
1	• Terremoto	• Ubicación en área volcánica	• Contacto con Entidades como el INAHMI
2	• Temblor	• Ubicación en área volcánica	• Contacto con Entidades como el INAHMI
3	• Tormenta Eléctrica	• Se dispone de equipos como antenas que están expuestas a rayos	• Pararayos
4	• Incendio en el sector	• Algunos de las casas cercanas no cuentan con extinguidores y seguridades contra incendios	• Sensores de incendios
5	• Incendio en el edificio	• Al existir una gran cantidad de equipos se está expuesto a corto circuitos	• Sensores de incendios
6	• Humedad/Sobrecalentamiento Inundaciones	• El clima es variable	• Sensores de agua y control de temperatura
7	• Animales/ Plagas	• Infiltración de plagas	• Fumigaciones periódicas
8	• Cambios continuos del personal	• Controles inadecuados de salida	• Procedimientos de entrada y salida de personal
9	• Ingresos no autorizados al sistemas por personal externo	• Controles inadecuados de seguridad	• Procedimientos de entrada y salida de personal
10	• Daños causados por personal interno	• Falta de conocimiento • Falta de capacitación	• Cámaras
11	• Administración indebida	• Falta de destreza en administración	• Auditoría
12	• Robo	• Al ser una Entidad emisora de tarjetas de crédito es punto blanco de robo	• Contratar Seguridad
13	• Phishing	• Acceso a Internet	• Actualización de parches y antivirus • Firewall
14	• Pharming	• Acceso a Internet	• Actualización de

No	Amenaza	Vulnerabilidad	Controles para mitigar
			• parches y antivirus • Firewall
15	• Malware, troyanos, keyloggers	• Acceso a Internet Correo electrónico • Dispositivos infectados	• Actualización de parches y antivirus • Firewall
16	• Skimming	• Clonación en cajeros o al momento de pagar	• Actualización de parches y antivirus • Firewall
17	• Estafa piramidal, hoax, carta nigeriana	• Acceso a Internet • Correo electrónico	• Actualización de parches y antivirus • Firewall
18	• Caída de los sistemas	• Falla en las aplicaciones • Problemas de concurrencia • Problemas de comunicaciones	• Site Alterno

Tabla 1.13 Pasos 3 y 4: Identificación de Vulnerabilidades y Análisis de Controles
Fuente: www.sbs.gob.ec[18]
Elaborado por: autores

[18] www.sbs.gob.ec, último acceso 27 de diciembre de 2011

Pasos 5, 6 y 7 Definición de probabilidades, impacto y valoración de riesgo

No	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Valoración del riesgo
1	• Terremoto	• Ubicación en área volcánica	Bajo	Alto	Bajo
2	• Temblor	• Ubicación en área volcánica	Medio	Medio	Medio
3	• Tormenta Eléctrica	• Se dispone de equipos como antenas que están expuestas a rayos	Alto	Bajo	Bajo
4	• Incendio en el sector	• Algunos de las casas cercanas no cuentan con extinguidores y seguridades contra incendios	Bajo	Medio	Bajo
5	• Incendio en el edificio	• Al existir una gran cantidad de equipos se está expuesto a corto circuitos	Bajo	Alto	Bajo
6	• Humedad/Sobrecalentamiento	• El clima es variable	Bajo	Medio	Bajo
7	• Animales/ Plagas	• Infiltración de plagas	Bajo	Bajo	Bajo
8	• Cambios continuos del personal	• Controles inadecuados de salida	Alto	Bajo	Bajo
9	• Ingresos no autorizados al sistemas por personal externo	• Controles inadecuados de seguridad	Medio	Medio	Medio
10	• Daños causados por personal interno	• Falta de conocimiento • Falta de capacitación	Medio	Medio	Medio
11	• Administración indebida	• Falta de destreza en administración	Bajo	Alto	Bajo
12	• Robo	• Al ser una Entidad emisora de tarjetas de crédito es punto	Medio	Alto	Medio

No	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Valoración del riesgo
		blanco de robo			
13	• Phishing	• Acceso a Internet	Medio	Alto	Medio
14	• Pharming	• Acceso a Internet	Medio	Alto	Medio
15	• Malware, troyanos, keyloggers	• Acceso a Internet • Correo electrónico • Dispositivos infectados	Medio	Alto	Medio
16	• Skimming	• Clonación en cajeros o al momento de pagar	Medio	Alto	Medio
17	• Estafa piramidal, hoax, carta nigeriana	• Acceso a Internet • Correo electrónico	Medio	Alto	Medio
18	• Caída de los Sistemas	• Falla en las aplicaciones • Problemas de concurrencia • Problemas de comunicaciones	**Medio**	Alto	Medio

Tabla 1.14 Pasos 5, 6 y 7 Definición de probabilidades, impacto y valoración de riesgo

Fuente: www.sbs.gob.ec[19]

Elaborado por: autores

[19] www.sbs.gob.ec, 27 de diciembre de 2011

Paso 8 Controles y Recomendaciones

Se deben incluir soluciones preventivas y correctivas, NIST 800-30 brinda una arquitectura modelo que puede mitigar los riesgos considerablemente, lo ideal es que ello se mantenga en el Site Principal y en el Alterno, como se muestra en la Figura 1.3.

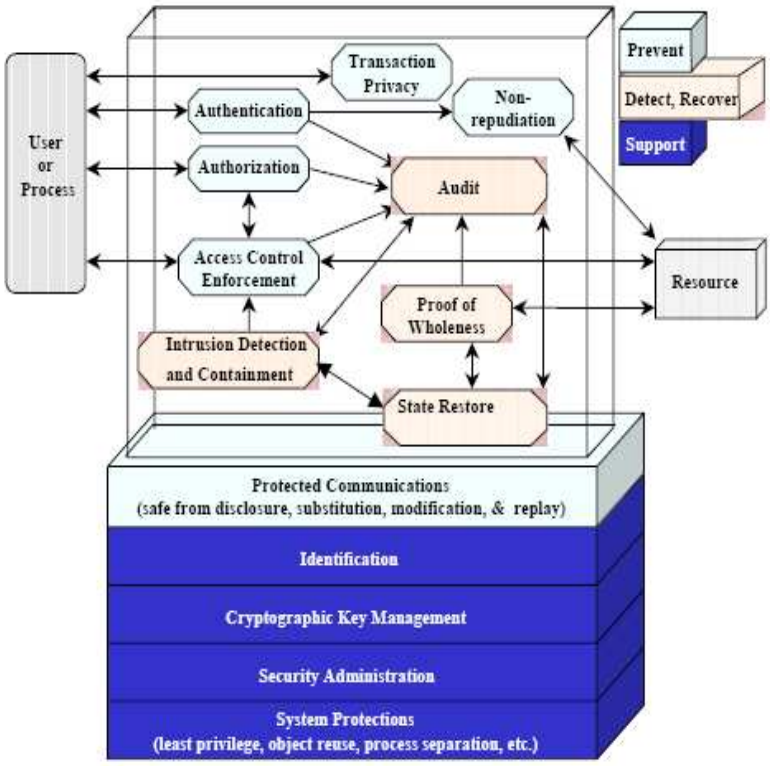


Figura 1.3 Controles Técnicos de Seguridad [20]

[20] Special Publication Nist 800-30, Gary Stoneburner, Alice Goguen, and Alexis Feringa, pág. 33

Paso 9 Documentar Resultados

Como se pudo observar existen muchos riesgos que afectan a las Entidades Bancarias, sin embargo varios de ellos se solventan con el Site Alterno, especialmente aquellos más críticos de total destrucción donde se marcaría la diferencia entre la supervivencia o la extinción, sin embargo para obtener el efecto esperado este Site debe complementarse con una adecuada gestión.

Los riesgos de phishing, pharming, malware, troyanos, keyloggers, skimming, deben ser mitigados por la Entidad Emisora de Tarjetas de Crédito puesto que en el casos de problemas los Usuarios empezarían a poner quejas, podrían dejar de usar este servicio o lo que es peor la cerrarían definitivamente.

El robo es otro de los riesgos que es necesario mitigar puesto que pone en riesgo la información, bienes materiales y humanos, la Entidad Emisora de Tarjetas de Crédito al igual que las otras Entidades Bancarias son el blanco que con más frecuencia utilizan los delincuentes.

Los cortes de energía eléctrica es otro de los problemas que se da con frecuencia y al ser un riesgo que impide el funcionamiento de la infraestructura tecnológica y es solucionado con la planta de energía.

1.5 CARACTERÍSTICAS QUE DEBE CUMPLIR UN SITE ALTERNO

Un Site Alterno debe cumplir todas las funciones que realiza el Site Principal, debe tener la capacidad de funcionar como backup instantáneo si ocurriera algún evento que afecte de forma temporal o definitiva el Site Principal. Entre las características que debe cumplir se mencionan las siguientes:

- Doble acometida eléctrica.
- Muelle de carga y descarga.
- Montacargas y puertas anchas.
- Altura suficiente de las plantas.
- Medidas de seguridad en caso de incendio o inundación: drenajes, extintores, vías de evacuación, puertas ignífugas, etc.
- Aire acondicionado, teniendo en cuenta que se usará para la refrigeración de equipamiento informático.
- Almacenes
- Pisos y techos falsos.
- Cableado de red y teléfono.
- Doble cableado eléctrico.
- Generadores y tableros de distribución eléctrica.
- Sistema de ventilación para evitar calentamiento de equipos.
- Instalación de alarmas, control de temperatura y humedad con avisos SNMP o SMTP.
- Cerraduras electromagnéticas.
- Torniquetes.
- Cámaras de seguridad.
- Detectores de movimiento.
- Tarjetas de identificación.
- Creación de zonas desmilitarizadas (DMZ).
- Segmentación de redes locales y creación de redes virtuales (VLAN).

- Despliegue y configuración de la electrónica de red: pasarelas, encaminadores, conmutadores, etc.
- Creación de los entornos de explotación, pre-explotación, desarrollo de aplicaciones y gestión en red.
- Creación de la red de almacenamiento.
- Instalación y configuración de los servidores y periféricos.
- Políticas y Procedimientos de Seguridad del Hardware
- Políticas y Procedimientos de Seguridad del Software
- Políticas y Procedimientos de Seguridad para el Control de Acceso a los Sistemas de Información

El Site Alterno si no cumple todas las funciones del Site Principal por lo menos debe realizar todas aquellas que se establecieron en el Plan de Continuidad del Negocio, o las que la empresa determino vitales para su subsistencia.[21]

Un Site Alterno debe garantizar la protección de:

1. Sistemas de Aplicación
2. Tecnología
3. Instalaciones
4. Información

Dicha información debe cumplir con las siguientes características:

- Efectividad
- Eficiencia
- Confidencialidad

[21] http://es.wikipedia.org/wiki/Centro_de_procesamiento_de_datos

- Integridad
- Disponibilidad
- Cumplimiento
- Confiabilidad

1.5.1 CARACTERISTICAS QUE DEBE TENER UN SITE ALTERNO: APLICADO A UN CASO DE ESTUDIO "EMISORA DE TARJETAS DE CRÉDITO"

Para definir las características que debe cumplir un Site Alterno en una Emisora de Tarjetas de Crédito es importante considerar los siguientes aspectos:

Un desastre informático es una interrupción prolongada, no planificada, que afecta procesos críticos de una organización y que necesita de un sitio de cómputo alterno para su recuperación.

Se debe establecer un plan a seguir que reúna los procedimientos y acciones que le permitirán a la Entidad emisora de Tarjetas de Crédito, restablecer los servicios.

Una parte importante es la evaluación de riesgos potenciales que pueden ocurrir, es necesario analizar todos los posibles incidentes y el impacto que pueden tener en la organización y en la continuidad de operaciones normales.

Entre los riesgos potenciales que se han identificado para Entidades emisoras de tarjetas de crédito constan los siguientes: Caída de energía eléctrica, piratas informáticos, virus, spams, incendios, entre otros.

Se debe definir las responsabilidades, estrategias y actividades para operar aplicaciones críticas considerando infraestructura, telecomunicaciones, etc.

Se debe determinar niveles de emergencia, los cuales pueden ser:

Total

Se tiene un tiempo máximo aceptable para restablecer todas o algunas de las prestaciones del Centro de Cómputo, es total cuando no se va a poder usar las instalaciones físicas por un período superior al máximo permitido definido.

Parcial

Cuando los equipos han sufrido daños menores y pueden tener un funcionamiento parcial.

Normal

En el caso de que los desperfectos se solucionan mediante la reinstalación y reconfiguración de equipos, por lo que no es necesaria la acción de un externo.

Se requiere desarrollar un Plan de Recuperación de Desastres, debe contar con estrategias generales de recuperación como esquemas de alta disponibilidad, esquema de procesamiento alterno, esquema de conectividad, métodos de respaldo. Para la activación del plan de contingencia se debe contar con tiempos de recuperación, personal involucrado, hardware y software.

Además se debe mantener actualizado el plan y entrenar al personal involucrado, debe contar con redundancia eléctrica, redundancia de comunicaciones, seguridad física, seguridad lógica, control de acceso, pisos y techos falsos, cableado de red y teléfono, doble cableado eléctrico, generadores y tableros de distribución eléctrica, sistemas y sensores de ventilación para evitar calentamiento de equipos,

Instalación de alarmas, control de temperatura y humedad con avisos SNMP o SMTP, entre otros.

1.5.1.1 Personal involucrado

Gerente de recuperación: Encargado de asegurar que se cumplan los objetivos y metas establecidos, asume la responsabilidad total en caso de desastres, incluye presupuestos y gastos para este fin, verifica los resultados de las pruebas y simulacros, toma decisiones, tiene disponibilidad 24/7, coordina las mejoras, etc.

Administrador del Plan de Recuperación: Conoce a detalle todo el procedimiento que debe llevarse a cabo, debe realizar las actualizaciones en base a los cambios que hayan surgido, coordina las acciones con todo el equipo de recuperación de desastres, sugiere mejoras en los procedimientos, tiene disponibilidad 24/7.

Establecedor de Daños: Determina el impacto de los daños causados.

Oficial de seguridad lógica: Configura y controla las medidas de seguridad en la red, computadoras y aplicaciones.

Administrador de instalación y logística: Soporte legal y logístico incluyendo adquisiciones y transporte de material, suministros, equipos, servicios a terceros y personal.

Jefe de Producción: Instalar, configurar y revisar, el computador de respaldo, el sistema operativo, software de seguridad, software de administración de base de datos y utilitarios, los cuales serán usados en los procesos de reconstrucción y actualización.

Jefe de Infraestructura: Configura las instalaciones de voz y datos en el servidor alterno, instalar módulos y software de comunicaciones, restablece el control de la red de usuarios/sistemas.

Gerente de Desarrollo: Analizar y determinar el punto de partida desde el cual debe comenzar el proceso de construcción y actualización de aplicaciones, configuración y pruebas, declarar las aplicaciones técnicamente listas para iniciar su operación, monitorear el desempeño de las aplicaciones y la integridad de la base de datos.

Soporte técnico: Establecer las instalaciones y configuraciones de los sistemas de información, incluyendo preparación de equipos de hardware, software, accesorios, suministros, cronogramas y turnos.

Gerentes de Usuarios finales: Revisar y analizar datos transaccionales, fluidez en los procesos críticos.

1.5.1.2 Aplicaciones críticas y software

A pesar de que todas las aplicaciones tienen importancia, se debe establecer prioridades de recuperación a fin de que el levantamiento sea ordenado en función de los procesos o servicios más relevantes.

Aplicación para Tarjetas de Crédito: que contienen módulos para: análisis de crédito, emisión de tarjetas, establecimientos, riesgos, autorizaciones, seguridad, caja, cobranzas, legal, servicio a clientes, inversiones, afiliación para establecimientos, logística, etc.

Aplicaciones BAT (Business Advantage Technology): Contiene los módulos: cuentas por pagar, contabilidad, conciliaciones, administración de aplicaciones y acceso a usuarios, sistema de roles, etc.

Aplicación para la Intranet: Las aplicaciones disponibles para los colaboradores de la Emisora de Tarjetas de Crédito como directorio telefónico, solicitudes de talento humano, proveeduría, etc.

Aplicación para el Call center: Permite gestionar adecuadamente los requerimientos telefónicos de clientes y establecimientos, para un adecuado seguimiento y un servicio de calidad.

SMS (Sistema de Mensajería): Las aplicaciones celular que permiten notificar promociones, saldos, recargas, etc.

Además es importante considerar que se deben definir perfiles de usuarios para: usuarios de caja, usuarios de servicio al cliente, usuarios del centro de atención telefónica, usuarios de ventas, usuarios de servicio de inversiones, usuarios de crédito, usuarios de mercadeo, usuarios de operaciones, etc.

1.5.1.3 Hardware y Networking

Un sistema en red se base en la operación fluida de sus servidores importantes para levantar aplicaciones críticas. Para lo cual se debe considerar:

Configuración de servidores: Para lo cual se debe considerar las características

Configuración para telecomunicaciones y networking: equipos para la red de comunicaciones, acceso a Internet de equipos y usuarios

Otros equipos: como impresoras, escáneres, etc.

Configuración de los discos y dispositivos de backup/restore

Detalle de las direcciones PC por usuarios

1.5.1.4 Logística de las copias de respaldo y restauración

Los respaldos deben garantizar la recuperación total de las operaciones

Controles internos del Centro de Cómputo

Se refiere a las normas que se aplican en los procesos de respaldo y restauración de la información, se debe definir la responsabilidad del encargado de respaldo tanto en la emisión como en la entrega, debe establecerse horarios de respaldos automáticos, los mismos que después deberán ser entregados al responsable para que sean enviados a una caja de seguridad externa o las que se hayan definido, debe realizarse pruebas continuas de restauración para asegurarse de

que los respaldos están en perfectas condiciones, debe llevarse un registro de todos los movimientos que se realicen con respaldos y restauraciones.

Detalle de los respaldos y restauraciones

Se deben realizar backups de aplicaciones, backups de BDD, backups de librerías, backups de desarrollo, backups de configuraciones, etc.

1.5.1.5 Entrenamiento, pruebas, mantenimiento y actualización

Se deben realizar programas de concientización, riesgos, probabilidad de ocurrencia, simulacros, talleres de seguridad industrial, etc.

Si bien es cierto existen documentos que contienen procedimientos a seguir, es muy importante que los mismos sean actualizados constantemente en base a la experiencia y eventos ocurridos.

Pruebas y validación del plan

Las pruebas deben planificarse según la disponibilidad de recursos y la criticidad de aplicaciones:

Fase implementación de la contingencia

Son las pruebas iniciales y verifican la funcionalidad del software, se usan para determinar fallos en la implementación, calidad o uso de las aplicaciones.

Fase pruebas de la contingencia

Son las pruebas funcionales que se llevan a cabo con usuarios e instituciones seleccionadas, estas pruebas deben considerar la mayor cantidad de escenarios esperados.

Fase producción de la contingencia

Son las Pruebas de integración que verifican todos los componentes comprometidos.

1.5.1.6 Procedimiento de respuesta ante contingencias

Caída de energía eléctrica

Si el corte es pequeño podrá ser suplido por la energía que proporcionan los UPSs, si es más largo se ve la necesidad de activar una planta generadora de energía a la misma que deberán conectarse los equipos que se determinó deben permanecer encendidos durante la contingencia.

Ataques de Hackers y Virus

Para este caso deberán recibir asesoramiento de personal especializado en seguridad de la información para contar con procedimientos en caso de intento masivo de usuarios no autorizados, en casos de infección por virus a sistemas, aplicaciones y programas, denegación de servicios, detección de intrusos, etc.

Incendio del Centro de cómputo

Partiendo desde que deben existir alarmas contra incendios, en el caso de que se activen es el punto más crucial en el cual se verá la necesidad de elevar el Site Alterno para continuar brindando los servicios. Eso no descarta que a los equipos de mayor criticidad, brindando mayor seguridad para sobrevivir al evento.

1.5.1.7 Detalles y esquemas técnicos de recuperación

El personal involucrado puede ser interno o externo:

Personal Interno

Funcionarios y empleados: Son ejecutivos, funcionarios, empleados. Personal con el cual la compañía cuenta para la recuperación

Propietarios de las aplicaciones: Propietarios de módulos o aplicaciones se incluye los especialistas encargados del mantenimiento de las aplicaciones y de los usuarios claves de las mismas, se debe incluir funcionarios y empleados claves, que sin ser programadores ni usuarios finales principales podrían ser requeridos a nivel de orientación o soporte en determinado momento.

Personal Externo

Proveedores de Hardware y Software:

Hardware

Se debe incluir los datos relevantes de funcionarios y empleados claves de proveedores de Hardware, como por ejemplo: Cableado estructurado, mantenimiento de impresoras, mantenimiento de servidores, venta de Hardware, venta y mantenimiento de UPSs.

Software

Mantenimiento de aplicaciones, se debe incluir los datos relevantes de funcionarios y empleados claves de proveedores de Software, proveedores de antivirus, proveedores de mensajes de texto, aplicaciones contables, aplicaciones de SAC, sistemas para Cobranzas, sistema de riesgos, VPNs seguras.

Proveedores de BDD

Proveedor de BDD convencional, proveedor de BDD documental, proveedor se Sistemas de Backup, proveedor de restauración, Datawarehouse, Datamining, etc.

Proveedores de comunicaciones

Proveedor de enlace principal, backup para enlace principal, proveedor de enlaces entre agencias, proveedor de enlaces por tipo de tarjeta, proveedor de enlaces datafast, proveedor de telefonía convencional, proveedor de telefonía celular, proveedores de enlaces para servicios dedicados.

Proveedores de servicios asociados a ambiente de producción

Está relacionado a los trabajos que se pueden realizar en la Entidad de tarjeta de crédito: mantenimiento general a nivel físico de servidores, mantenimiento general de UPSs, cableado estructurado, soporte y administración de Call Canter, intranet, sistemas contables, instalación y mantenimiento de antispam y antivirus, desarrollo y soporte web, servidor de transacciones.

CAPÍTULO 2

DETERMINACIÓN DE LAS MEJORES PRÁCTICAS PARA LA GESTIÓN DE TIC'S EN UN SITE ALTERNO

Las empresas en la actualidad, incluidas las Entidades bancarias, requieren utilizar estándares en cada proceso que realizan, con el apoyo de las buenas prácticas es posible identificar lo que se debería hacer, cómo hacerlo y por qué se importante hacerlo.

Un Site Alterno podría hacer la diferencia entre el éxito y el fracaso de una empresa al atravesar situación difícil, de aquí parte la necesidad de gestionarlo de manera adecuada para obtener el mayor beneficio de él, solventar los problemas que puedan presentarse y minimizar los efectos dañinos.

A continuación la definición de Site Alterno y los tipos que existen con su respectiva descripción.

2.1 SITE ALTERNO[22]

Un Site Alterno es un lugar donde una organización puede fácilmente trasladarse después de un desastre, como incendios, inundaciones, amenazas terroristas u otros eventos destructivos, es un sitio de recuperación del área de trabajo. Es parte del plan de recuperación de desastres y del plan de continuidad de negocio de una organización.

Un Site Alterno puede estar operando fuera de la organización, o puede ser contratado a través de una empresa especializada en servicios de recuperación de desastres. En algunos casos, una organización puede tener un convenio con otra organización para operar un Site Alterno conjunto.

[22] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457

A continuación las alternativas de recuperación que son utilizadas una vez que el Site Principal no esté disponible que permite utilizar instalaciones alternas para mantener los procesos en funcionamiento: .Cold Site, Sitio Móvil, Warm Site, Acuerdo recíproco, Hot Site, Sitio Duplicado y Acuerdo Recíproco. La diferencia entre cada opción está determinadas por los costos, tiempo y el esfuerzo necesarios para implementarlos.

2.1.1 COLD SITE[23]

Un Cold Site se define como una instalación que cuenta con un espacio apropiado, dispone de infraestructura básica, no incluye los equipos de TI de comunicaciones, tampoco dispone de programas, datos y soporte de oficina.

Cuando se activa el plan y se dispone de un Cold Site, en dicho documento deben constar las disposiciones para adquirir e instalar, hardware, software y equipos de oficina.

Este Site es el más económico, sólo está asignado el sitio físico, como antes se mencionó en él no se incluyen copias de respaldos de datos e información del Site Principal de la organización, tampoco hardware ya configurado, lo que contribuye a un mínimo costo para su funcionamiento, sin embargo requiere tiempo para que la organización vuelva a funcionar del modo que operaba antes del desastre.

[23] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457

2.1.2 SITE MÓVIL[24]

Un Site Móvil se define como una instalación empacada y modular, que se aloja sobre vehículos de transporte y está listo para la entrega e instalación en la ubicación asignada el momento en el que se activa el plan.

Cuando se activa un plan y se dispone de un Site Móvil debe especificar las ubicaciones de los sitios que podrían ser utilizados, se debe proporcionar el derecho al acceso al Site seleccionado por el Proveedor y la Compañía, se debe proporcionar la infraestructura necesaria para soporte al Site como vías de acceso, agua, eliminación de desperdicios, energía eléctrica y comunicaciones.

2.1.3 WARM SITE[25]

Un Warm Site se define como una instalación con espacio e infraestructura básica y algunos o todos los equipos requeridos de TI y comunicaciones instalados.

Los equipos pueden ser de menor capacidad que el Site Principal, sin embargo adecuados para sustentar las aplicaciones críticas. El personal sería transferido a este sitio y las versiones y programas actuales y datos se cargarían antes de iniciar las actividades.

[24] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457
[25] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457

2.1.4 HOT SITE[26]

Un Hot Site se define como una instalación con el espacio e infraestructura básica y los todos equipos de TI y comunicaciones para respaldar aplicaciones críticas así como mobiliario y equipos de oficina para uso del personal.

Se tienen instaladas versiones de los programas requeridos para aplicaciones críticas, las copias de respaldo más recientes deben ser cargadas antes de reanudar las aplicaciones críticas. A pesar de existir personal asignado para respaldar las operaciones, los empleados se transfieren al Hot Site para respaldar las operaciones al momento de la activación.

Este Site es el más costoso, es un duplicado del Site Principal de la organización, contiene sistemas informáticos, respaldos de datos de los clientes y usuarios. La sincronización en tiempo real entre los dos Sites se utiliza para reflejar por completo el entorno de datos del sitio original hacia el alterno para lo que cuenta con enlaces y software especializado. Después de una interrupción en el Site Principal, la organización se puede reubicar con pérdidas mínimas. Un Hot Site será instalado y estará funcionando en cuestión de horas o menos. La capacidad puede o no coincidir con la capacidad del Site Principal en función de las necesidades de la organización. Son muy populares entre las organizaciones que operan los procesos en tiempo real tales como instituciones bancarias, proveedores de comercio electrónico, entre otras.

2.1.5 SITE DUPLICADO[27]

Un Site Duplicado se define como aquel completamente redundante con replicación de datos en tiempo real desde el Site Principal. Estos sitios cuentan

[26] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457
[27] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457

con todos los equipos y personal, pueden asumir procesamientos críticos sin interrupciones, de tal manera que sea transparente para el usuario.

2.1.6 ACUERDO RECÍPROCO ENTRE COMPAÑÍAS[28]

Un Acuerdo Recíproco se define como un convenio entre compañías independientes pero con características similares para compartir instalaciones de TI en un tiempo limitado cuando una de las compañías pierda su capacidad de procesamiento.

No se consideran una opción adecuada debido al esfuerzo requerido para mantener la compatibilidad entre hardware y software, pueden surgir inconvenientes en seguridad y privacidad durante aplicaciones compartidas y la dificultad de ejecutar el plan si surge alguna discrepancia.

2.1.7 ACUERDO RECÍPROCO CON OTRAS ORGANIZACIONES[29]

Un Acuerdo recíproco se define como un acuerdo entre dos o más organizaciones con equipos o aplicaciones únicas, bajo estas condiciones los participantes se comprometen a proporcionar asistencia en caso de que surja una emergencia, es una alternativa de recuperación poco usada.

[28] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457
[29] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457

2.2 CONSIDERACIONES A TOMAR EN CUENTA AL MOMENTO DE ESCOGER UN SITE ALTERNO

El seleccionar una estrategia de recuperación adecuada depende de la criticidad del proceso del negocio, las aplicaciones que respaldan esos procesos, los costos, los tiempos requeridos para recuperación así como la seguridad.

El sitio alterno debe estar fuera del área afectada, debe establecerse comunicaciones con el sitio alterno, se debe proporcionar soluciones redundantes para que posterior a la interrupción puedan estar en contacto.

Las alternativas de recuperación pueden ser suministradas por Proveedores externos o por la misma Entidad, cuando la instalación es de la Entidad es más fácil resolver el problema, sin embargo cuando las instalaciones pertenecen a un Proveedor externo es importante que estén claramente definidos los procesos contractuales así como garantizar el acceso sin demoras luego del desastre.

El proporcionar una recuperación más rápida implica costos más altos y recursos dedicados. Para seleccionar una alternativa de recuperación apropiada se debe comparar los costos de negocio asociados a la interrupción de procesos críticos (desarrollados en el BIA[30]) con el costo de opciones de procesamiento alternativo, la dirección de la Entidad debe encontrar el RTO[31] y el RPO[32], a continuación se definirá cada uno de ellos.

2.2.1 ANÁLISIS DE IMPACTO DEL NEGOCIO BIA[33]

El BIA es un paso crítico en el desarrollo de la estrategia de continuidad del negocio, se utiliza para evaluar procesos críticos así como tiempo, prioridades,

[30] BIA: Análisis de Impacto del Negocio
[31] RTO: Objetivo de Tiempo de Recuperación
[32] RPO: Objetivo de Punto de Recuperación
[33] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457

recursos, interdependencias y riesgos. En el BIA es importante se incluyan todos los tipos de recursos y no solo los tradicionales incluso los componentes ocultos.

Para evaluar el tiempo que no es productivo se desarrollan las bandas de impacto que a quienes se le podría calificar como alto, medio y bajo, y para cada proceso se debe estimar el tiempo en horas, días, semanas. Con un enfoque similar se puede estimar el impacto de la pérdida de datos y de ser necesario incluso asignar un valor financiero.

Para establecer un BIA es necesario conocer cuáles son los diferentes procesos del negocio críticos y no críticos, posteriormente se identifican los procesos críticos así como el período de tiempo de recuperación crítico para recursos de información en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas.

2.2.2 OBJETIVO DE PUNTO DE RECUPERACIÓN RPO[34]

Afecta a las soluciones de protección de datos, se determina tomando como base la pérdida de datos aceptables en el caso de interrupción de las operaciones, indica el tiempo mínimo posible en el que se pueden recuperar los datos, incluso se menciona los datos de alcance que son aquellos que deben ingresarse luego de colocado el último respaldo.

Cuantifica la cantidad permitida de pérdida de datos en caso de desastres.

2.2.3 OBJETIVO DE TIEMPO DE RECUPERACIÓN RTO[35]

El RTO generalmente afecta al tipo de instalación que se ha seleccionado como por ejemplo: warm, hot, cold, se determina basándose en el tiempo improductivo

[34] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457
[35] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457

aceptable en caso de una interrupción de operaciones, indica el punto más próximo en el que se deben retomar las operaciones luego del desastre.

2.2.4 POLITICA DE CONTINUIDAD DEL NEGOCIO[36]

Es un documento aprobado por la alta dirección de la Entidad donde se define la magnitud y el alcance del esfuerzo de continuidad del negocio, se divide en dos partes:

- Interna, que es un mensaje para las partes interesadas de la organización
- Pública, es un mensaje para las partes interesadas externas.

El ciclo de vida de la planificación de la continuidad del negocio cuenta con una planificación del proyecto, evaluación y análisis de riesgos, análisis de impacto del negocio, estrategia de desarrollo, ejecución de estrategia, plan de desarrollo, desarrollo del plan, pruebas del plan, monitoreo, mantenimiento y actualización del plan.

2.3 MEJORES PRÁCTICAS

Los negocios están mejorando la administración de la calidad y confiabilidad de TI, con la adopción de mejores prácticas para responder a requerimientos normativos y contractuales, que el mundo globalizado exige.

Existe peligro de que las mejores prácticas, potencialmente útiles, sean costosas y desenfocadas, por lo que las mejores prácticas deben ser aplicadas en el contexto del negocio y enfocadas en brindar mayor beneficio a la organización.

[36] Manual de Preparación Examen CISA 2010, capítulo 6, Continuidad del Negocio y Recuperación en caso de desastre pág. 421-457

Se necesita que la alta dirección, los gerentes, los auditores, oficiales de cumplimiento y directores de TI trabajen en armonía para asegurar que las mejores prácticas conduzcan a servicios económicos y bien controlados.

Las mejores prácticas de TI deben estar alineadas con las metas del negocio, ayudando a que el negocio pueda cumplir sus metas de una forma organizada y optimizando recursos.

Algunas de las ventajas de utilizar las mejores prácticas serán detalladas a continuación:

- Es posible mejorar la gestión de TI.
- Permite tener un marco de referencia eficaz que gestiona políticas, controles internos y prácticas definidas, lo que ayuda a que cada persona tenga conocimiento de las funciones que debe realizar y el procedimiento para ejecutarlas.
- Menor dependencia de expertos.
- Menor cantidad de errores.
- Eleva la confianza de socios, clientes y entes reguladores.

La actual tesis se enfocará en las mejores prácticas propuestas por los marcos de referencia que se describen a continuación:

ITIL: Publicado por OGC (Office of Government Commerce) del gobierno británico para la gestión de servicios de TI.

COBIT: Publicado por ITGI para control y gobierno de TI

ISO/IEC: Publicado por ISO (International Organization for Standardization) y por IEC (International Electrotechnical Commission) para gestión de seguridad de la información.

NIST: National Institute of Standards, agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos para promover la

innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

La implementación de mejores prácticas debe ser consistente con el marco de control y gestión de riesgos de la empresa ajustada a las necesidades de la empresa e integrada con otras metodologías que ya se estén utilizando.

La implementación debe ser adaptada al negocio, priorizada y planificada para lograr su uso eficaz.

El objetivo de esta tesis es explicar el valor de las mejores prácticas y el mecanismo para armonizarlas, implementarlas e integrarlas.

Entre los desafíos actuales que se pretende alcanzar con ayuda de las mejores prácticas se menciona:

Creación de conciencia del propósito del negocio.

Las mejores prácticas normalmente son conocidas por profesionales, gerentes y asesores de TI, quienes pueden adaptarlos y utilizarlos pero no tienen un enfoque de negocio (alta dirección) o no cuentan con la ayuda del cliente. Si se desea alcanzar el máximo valor de las mejores prácticas se necesita involucrar a los clientes y a los proveedores.

El uso de TI es crítica para el éxito empresarial, ofrece una ventaja competitiva y medios para incrementar la productividad, incluso influirá en la supervivencia del negocio.

Las mejores prácticas ayudan a mejorar el desempeño, transparencia y control de actividades de TI.

Las mejores prácticas representan un enfoque común para un buen control de TI, que trata de unificar el lenguaje para las personas involucradas.

Las mejores prácticas también ayudan a gestionar adecuadamente los riesgos de TI evitando: proyectos fallidos, inversiones perdidas, brechas de seguridad, fallas

de los sistemas y fallas de proveedores para entender y satisfacer los requerimientos de los clientes.

Para implantar las mejores prácticas necesitan un marco de referencia de gestión eficaz que permita un enfoque integral consistente y que asegure resultados exitosos.

El utilizar mejores prácticas traza un camino desde una situación caótica hacia procesos definidos y gestionados de TI.

Las mejores prácticas estarán mejor alineadas con los requerimientos de gobierno y del negocio antes que a los requisitos técnicos.

El gobierno de TI se ocupa de lo siguiente:

- El alineamiento estratégico
- La entrega de valor
- La gestión de riesgos
- La gestión de recursos
- La medición del desempeño

Se requiere definir los derechos para la decisión y rendición de cuentas, el logro de ellos en la teoría (la organización está claramente definida) y la práctica (todos saben lo que hay que hacer y cómo hacerlo) requiere una cultura correcta, políticas, controles internos y prácticas definidas, algunas incluso ayudan a identificar roles y responsabilidades para un gobierno de TI efectivo.

Las mejoras prácticas contribuyen con la empresa de la siguiente manera:

- Mejorando la calidad, la respuesta y la fiabilidad de las soluciones y servicios de TI.

- Mejorando la viabilidad, previsibilidad, y repetitividad de resultados de negocio exitoso.
- Ganando la confianza y el creciente involucramiento de usuarios y patrocinadores del negocio.
- Reduciendo riesgos, incidentes y fallas en los procesos.
- Mejorando la habilidad del negocio para gestionar y supervisar la realización de beneficios de TI.
- Evitando la reinvención de prácticas probadas.
- Reduciendo la dependencia de expertos
- Incrementando el potencial del Staff, menos experto pero correctamente enterado.
- Superando silos verticales y comportamientos no deseados
- Incrementando la estandarización que conduzca a la reducción de costos
- Haciéndolo más fácil para aprovechar la ayuda externa a través del uso de procesos estandarizados.
- Logrando el cumplimiento y la aplicación de controles internos
- Demostrando adherirse a buenas prácticas aceptadas y probadas por la industria
- Mejorando la confianza y la seguridad de la dirección y los socios
- Generando respeto de los entes reguladores y supervisores externos.

A continuación se determinará las mejores prácticas propuestas por COBIT, ITIL, ISO/IEC y NIST a ser utilizadas en la gestión de TIC’s en Sites Alternos.

2.3.1 COBIT[37]

Es un marco de referencia aceptado a nivel mundial que se basa en estándares de la industria y mejores prácticas. La dirección ejecutiva necesita tener la suficiente seguridad en los sistemas de información y en la información que producen los sistemas, y de este modo alcanzar un retorno positivo de inversiones. Con COBIT es más fácil que los ejecutivos conozcan procedimientos, métodos y estándares de cómo dirigir y gestionar el uso de TI en el negocio, con las herramientas que se les proporciona las que permiten supervisar todas las actividades relacionadas con TI, incluso los servicios que proporcionan los proveedores. Cuando COBIT es implementado los ejecutivos pueden asegurarse de que las TI se ajustan eficazmente a los objetivos del negocio y así obtener ventajas comerciales.

COBIT brinda un lenguaje común, de este modo es más fácil comunicar las metas, objetivos y resultados a las personas involucradas. Además brinda herramientas para el monitoreo y la gestión de las actividades de TI. Las TI son una inversión importante que debe ser gestionada, COBIT permite comprender y gestionar las inversiones de TI durante el ciclo de vida e incluso evaluar si los servicios y las nuevas iniciativas de TI satisfacen los requerimientos empresariales así como las probabilidades de entregar los beneficios esperados.

Hay una clara diferencia entre las personas que realizan una buena gestión de TI y las que no lo hacen. COBIT permite el desarrollo de políticas y mejores prácticas para la administración de TI, el marco ayuda a incrementar el valor obtenido de TI, a gestionar los riesgos relacionados con TI, a asegurar el cumplimiento, la continuidad, seguridad y privacidad.

Como COBIT es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, una vez implementado es una muestra de buena gestión en la organización. Ayuda a los profesionales y usuarios a demostrar su competencia profesional a la alta dirección, en procesos del negocio genéricos, existen

[37] COBIT 4.1-2007. IT Governance Institute.

estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI, COBIT se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas.

Los ejecutivos ganan confianza en que la utilización de las TI puede ser gestionada de forma eficaz, toda vez que se ha implementado los principios claves de COBIT en una empresa.

Una vez que las empresas adoptan COBIT las empresas esperan:

- El personal de TI puede trabajar en conjunto ya que tiene claro el funcionamiento del negocio y puede brindar buenas iniciativas para TI.
- Los costos del ciclo de vida de TI serán más fáciles de presupuestar y aprobar.
- La información otorgada por TI será entregada en el momento indicado y de calidad.
- Los proyectos de TI que se cumplan en su totalidad aumentarán, y entregarán mayores resultados.
- TI en la empresa en general tendrá claros los requisitos de seguridad y privacidad que ellos como TI deben cumplir, mejorando el monitoreo.
- Una vez que se han identificado los riesgos de TI, es establecerá la gestión adecuada. En la elaboración de auditorías se tendrán buenos resultados y exitosas implementaciones para la mejora continua de la empresa.
- Que TI cumpla los requisitos dados por entes externos será una práctica normal para la empresa.

Las versiones de COBIT incluyen lo siguiente:

- Marcos de Trabajo: En COBIT se indica cómo organizar la gestión de gobierno de TI, los objetivos de control, los procesos y dominios de TI y los relaciona con las necesidades del negocio. El marco contiene 34 objetivos

de control, uno para cada proceso de TI y los agrupa en 4 dominios: Planificar y Organizar, Adquirir e implementar, Entregar y dar soporte, Monitorear y evaluar.

- Los procesos cubren las áreas de responsabilidad de la empresa y de TI desde el principio hasta el final.
- Los objetivos de control contienen objetivos de gestión para los procesos de TI.
- Se ofrecen herramientas para asignar responsabilidades y medir el desempeño.
- Además proporciona perfiles de procesos de TI que describen estados actuales y futuros respecto al modelo de madurez.

COBIT ha sido desarrollado para entrega de valor del gobierno de TI[38].

En la figura 2.1 se encuentra el cubo de componentes de COBIT, donde se puede visualizar los procesos de TI, los recursos de TI y los requerimientos del negocio.

[38] Alineando COBIT 4.1 ITIL v3 e ISO/IEC 27002 en beneficio del negocio, Governance Institute, OGC Office of Government Commerce, 2008, pág. 6 - 14

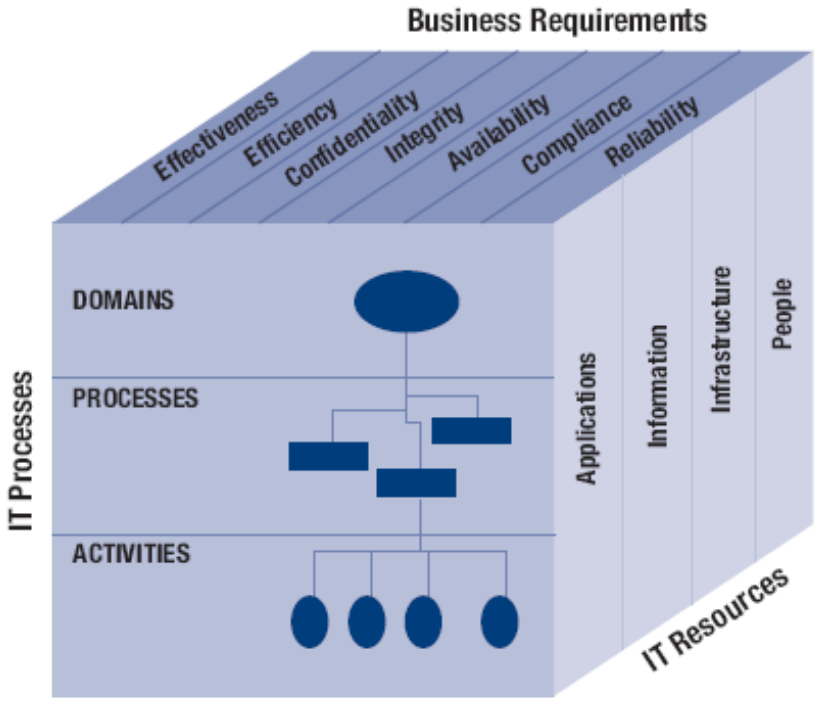


Figura 2. 1 Cubo Componentes COBIT
Fuente: COBIT 4.1-2007. IT Governance Institute. Página 25

Requerimientos del Negocio

Los requerimientos del negocio son:

1. Efectividad
2. Eficiencia
3. Confidencialidad
4. Integridad
5. Disponibilidad
6. Cumplimiento
7. Confiabilidad

- Recursos de TI

1. Aplicaciones
2. Información
3. Infraestructura
4. Personas

- Dominios

1. Planear y Organizar
2. Adquirir e Implementar
3. Entregar y dar soporte
4. Monitorear y Evaluar

Cada uno con sus respectivos procesos y actividades.

COBIT fue establecido en 1998 con la finalidad de evolucionar el pensamiento y definir estándares internacionales con respecto a la dirección y control total de la tecnología de información para las empresas. En la figura 2.2 se ilustra de que manera con COBIT se alinean los procesos de TI al negocio, es decir, el negocio define sus objetivos así como las estrategias que utilizará para conseguirlos y la tecnología se alinea de la mejor manera para conseguirlos.

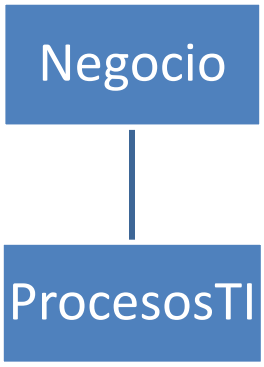


Figura 2. 2 Alineamiento
Fuente: Curso COBIT –CEC-Instructor: Ing. Mark Jaramillo, Página 4

COBIT contiene dominios, los mismos que a su vez contienen procesos, que permiten que la tecnología se enfoque en los principales requerimientos de la Entidad de tal modo que estén alineados como lo muestra la figura 2.3.

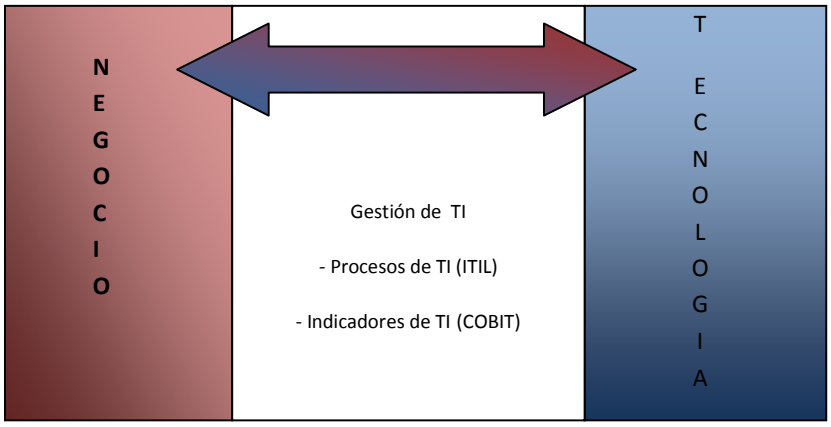


Figura 2. 3 Gestión de TI
Fuente: Curso COBIT –CEC-Instructor: Ing. Mark Jaramillo, Página 4

2.3.2 ITIL[39]

En la actualidad las organizaciones dependen de TI para satisfacer los objetivos corporativos y las necesidades del negocio, entregando valor a los clientes, para que esto ocurra de forma gestionada, responsable y repetible la empresa debe asegurar que los servicios de TI son de alta calidad y que deben:

- Satisfacer las necesidades de la empresa.
- Satisfacer los requisitos de los usuarios
- Cumplir con normativas vigentes
- TI debe entregarse con eficiencia y eficacia
- TI debe mejorarse en forma continua

La gestión de servicios de TI cubre la planificación, diseño, implementación, operación, apoyo y mejora de los servicios para que sean apropiados a las necesidades del negocio.

ITIL proporciona un marco de trabajo con prácticas integrales, consistentes y coherentes para la gestión de servicios de TI así como los procesos relacionados, la promoción de alta calidad para lograr eficiencia y eficacia.

El rol de ITIL es brindar orientación al nivel más bajo que pueda aplicarse, para implementar ITIL se requieren conocimientos específicos de los procesos del negocio.

[39] Alineando COBIT 4.1, ITIL V3 4.1, ITIL v3 e ISO/IEC 27002 en beneficio del Negocio, Reporte del ITGI y la OGC.

ITIL refleja el ciclo de vida de los servicios de TI, cuya guía está separada en 5 volúmenes como se describen a continuación:

- Service Strategy (SS)
- Service Design (SD)
- Service Transition (ST)
- Service Operation (SO)
- Continual Service Improvement (CSI)

Estrategia de Servicio (SS)	**Diseño del Servicio (SD)**	**Transición del Servicio (ST)**	**Operación del Servicio (SO)**	**Mejora Continua del Servicio (CSI)**
Gestión del servicio • Ciclo de vida del servicio • Activos del servicio y creación de valor • Tipos y estructuras de proveedores de servicios • Estrategia, mercados y oferta • Gestión financiera • Gestión del portafolio de servicios • Gestión de la demanda • Diseño organizacional, cultura y desarrollo • Estrategia de aprovisionamiento • Automatización e interfaces de servicios • Herramienta para estrategias • Desafíos y riesgos	Diseño balanceado • Requisitos, indicadores, actividades y limitantes • Arquitectura orientada al servicio • Gestión de servicios de negocio • Modelos de diseño de servicios • Gestión del catálogo de servicios • Gestión de niveles de servicios • Capacidad y disponibilidad • Continuidad de servicios de TI • Seguridad de la información • Gestión de proveedores • Gestión de datos y de la información • Gestión de aplicaciones • Roles y herramientas • Análisis de impacto en el negocio • Desafíos y riesgos • Paquete de diseño de servicios • Criterios de aceptación de servicios • Documentación • Aspectos ambientales • Marco de trabajo • Maduración de procesos	• Objetivos, principios, políticas, contexto, roles y modelos • Planificación y soporte • Gestión del cambio • Activos del servicio y gestión de la configuración • Liberación y distribución • Validación y prueba del servicio • Evaluación • Gestión del conocimiento • Gestionando las comunicaciones y el compromiso • Gestión de partes interesadas • Sistema de gestión de configuraciones • Introducción por etapas • Desafíos y riesgos • Tipos de activos	Equilibrio en la operación del servicio • Salud operacional • Comunicación • Documentación • Eventos, incidentes y problemas • Atención de requerimientos • Gestión de accesos • Monitoreo y control • Gestión de la infraestructura y el servicio • Gestión de instalaciones y del Data Center • Seguridad física y de la información • Mesa de servicios • Gestión técnica de operaciones de TI y de aplicaciones • Roles, responsabilidades y estructuras organizacionales • Soporte tecnológico a la operación del servicio • Gestionando los cambios, proyectos y riesgos • Desafíos • Guía complementaria	• Objetivos, métodos y técnicas • Cambio organizacional • Propiedad • Drivers • Gestión de niveles de servicios • Medición del servicio • Gestión del conocimiento • Benchmarking • Modelos, estándares y calidad • Proceso de mejoramiento de los siete pasos CSI • Retorno sobre la inversión (ROI) y aspectos de negocio • Roles • Matriz RACI • Herramientas de soporte • Implementación • Gobierno •Comunicaciones • Desafíos y riesgos • Innovación, corrección y mejoramiento • Apoyo de las mejores prácticas a la mejora continua del servicio (CSI)

Tabla 2. 1 Tópicos de ITIL

Fuente: Alineando COBIT 4.1, ITILV3 e ISO/IEC 27002 en beneficio del negocio, publicado por OGC e IT Gobernance Institute, pág. 16

Actualmente existe un esquema de certificación ITIL a personas que van desde una apreciación a nivel de fundamentos hasta un nivel avanzado.

El itSMF provee una red accesible de expertos de la industria, fuentes de información y eventos para ayudar a los países miembros a abordar problemas de gestión de servicios de TI y obtener la entrega de servicios consistentes de buena calidad, gracias a la adopción de buenas prácticas.

2.3.3 ISO/IEC[40]

El objetivo del estándar es brindar información a los encargados de implementar la seguridad de la información en una organización. Es una buena práctica para el desarrollo y mantenimiento de normas de seguridad y prácticas de gestión de una empresa con el fin de mejorar la confianza en la seguridad de la información para relaciones con otras empresas. Se definen estrategias de controles de seguridad que se encuentran organizados bajo dominios. La norma detalla la importancia de la gestión del riesgo aclarando que no se debe aplicar todo, únicamente lo relevante.

Los principios de la norma son los puntos de partida para implementar seguridad de la información. Se basan en cualquiera de los requisitos legales o en las mejores prácticas generalmente aceptadas.

Las mediciones basadas en los requisitos legales son: protección y sigilo de datos personales, protección de información interna y la protección de los derechos de propiedad intelectual.

Las mejores prácticas mencionadas en la norma incluyen: política de seguridad de la información, asignación de la responsabilidad de seguridad de la información, escalamiento de problemas y gestión de la continuidad del negocio.

[40] Alineando COBIT 4.1, ITIL V3 4.1, ITIL v3 e ISO/IEC 27002 en beneficio del Negocio, Reporte del ITGI y la OGC.

Es necesario considerar varios factores para la implementación de un sistema de gestión de seguridad de la información:

- Política de seguridad, objetivos y actividades que reflejan los objetivos del negocio.
- Consideración de aspectos culturales de la organización.
- Apoyo y compromiso de la alta dirección.
- Conocimiento de requisitos de seguridad, evaluación de riesgo y gestión de riesgo.
- La comunicación sobre la importancia de la seguridad se debe dirigir a todo el personal incluyendo los miembros de la dirección.
- La política de seguridad y sus medidas se deben comunicar a otras empresas que trabajan con la organización.
- Tener un sistema integral para la evaluación de desempeño, apoyando la mejora continua de suministro de información.

  Los componentes que se deben considerar son los siguientes:

- Política de seguridad.
- Organización para la seguridad.
- Clasificación de activos y su control.
- Seguridad del personal.
- Seguridad física y ambiental.
- Comunicación y gestión de operaciones.
- Control de acceso.
- Adquisición desarrollo y mantenimiento de sistemas.
- Gestión de la continuidad del negocio.

2.3.4 NIST[41]

El Instituto Nacional de Normas y Tecnología (National Institute of Standards), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos cuya misión es promover la innovación y la competencia industrial mediante normas y tecnología que mejoren la estabilidad económica y la calidad de vida.

Para facilidad de selección del Control de Seguridad sus procesos se organizan en 17 familias.

ID	FAMILIA	CLASE
AC	Access Control (Control de Acceso)	Técnico
AT	Awareness and Training (Sensibilización y Formación)	Operativo
AU	Audit and Accountability (Auditoría y Rendición de Costos)	Técnico
CA	Security Assessment and Authorization (Evaluación de la Seguridad y Autorización)	Gestión
CM	Configuration Management (Gestión de la configuración)	Operativo
CP	Contingency Planning (Plan de contingencia)	Operativo
IA	Identification and Authentication (Identificación y Autentificación)	Técnico
IR	Incident Response (Respuesta a incidentes)	Operativo
MA	Maintenance (Mantenimiento)	Operativo
MP	Media Protection (Medios de Protección)	Operativo

[41] ALVAREZ ÁLVAREZ GUSTAVO ALEXANDER, Universidad Nacional de Trujillo; NIST SP800-53 REV. 3 con COBIT 4.1, 2010.

PE	Physical and Environmental Protection (Protección Física y del medio ambiente)	Operativo
PL	Planning (Planeación)	Gestión
PS	Personnel Security (Seguridad del Personal)	Operativo
RA	Risk Assessment (Evaluación de Riesgos)	Gestión
SA	System and Services Acquisition (Sistemas y Servicios de Adquisición	Gestión
SC	System and Communications Protection (Sistemas De Protección y Comunicación)	Técnico
SI	System and Information Integrity (Integridad del Sistema y la Información)	Operación
PM	Program Management (Programa de Gestión)	Gestión

Tabla 2. 2 Clases, familias e Identificadores de Control de Seguridad

Fuente: NIST SP800-53 Rev. 3 con COBIT 4.1, Alvarez Alvarez, Gustavo Alexander, pag.2

Para gestionar el riesgo adecuadamente se debe:

1. Categorizar los sistemas de información (procesada, almacenada y transmitida)
2. Seleccionar los controles de seguridad (basado en el nivel de impacto y los requisitos mínimos de seguridad)
3. Implementar los controles de seguridad (aplicar y describir los controles empleados)
4. Evaluar los controles de seguridad con procedimientos de evaluación adecuados)
5. Autorizar los sistemas de información (determinando operaciones de riesgo para las organizaciones)

6. Monitorear los controles de seguridad (con evaluación, documentación y análisis)

Es necesario evaluar el estado actual de seguridad del sistema de información y el riesgo para las operaciones de la organización y los bienes, las personas, otras organizaciones, y la Nación. La organización investiga la vulnerabilidad del sistema de información explotados por la fuente de la amenaza y los controles de seguridad a cabo actualmente en el sistema como se describe en el plan de seguridad. La explotación de vulnerabilidades del sistema de información por una fuente de amenaza puede deberse a:

1. Falta de controles de seguridad
2. La fuerza insuficiente de controles de seguridad
3. Un aumento en la capacidad de la fuente de amenaza[42].

2.4 DETERMINACIÓN DE LAS MEJORES PRÁCTICAS PROPUESTAS POR COBIT MAPEADAS CON ITIL, ISO/IEC Y NIST A SER UTILIZADAS EN LA GESTION DE TIC'S EN SITES ALTERNOS

Con el apoyo de las buenas prácticas es posible gestionar adecuadamente y administrar un Site Alterno, por lo que a continuación se detalla aquellos procesos que se deben considerar.

A continuación se describen los 4 dominios de COBIT cada uno de los cuales consta de sus respectivos procesos y sus objetivos de control:

El dominio Planear y Organizar permitirá evaluar y administrar los Riesgos de TI de tal manera que el Site Alterno sea utilizado en el momento adecuado

[42] NIST SP800-53 Rev. 3 con COBIT 4.1, Alvarez Alvarez, Gustavo Alexander, pag.1-21

El dominio Adquirir e Implementar permitirá que se puedan realizar las adquisiciones para el Site Alterno adecuadamente y que todos los cambios sean correctamente gestionados.

El dominio Entregar y Dar Soporte, permitirá definir niveles de servicio, administrarlos adecuadamente con los proveedores del Site, gestionar adecuadamente el desempeño y la capacidad del Site, garantizar la seguridad de los sistemas, administrar la información y administrar el ambiente físico.

El dominio Monitorear y Evaluar permitirá que se cumplan todas las políticas, normas, leyes y regulaciones que deben cumplirse con ayuda de los Sites Principal y Alterno.

2.4.1 PLANEAR Y ORGANIZAR[43]

Dominio Planear y Organizar (PO), proporciona la dirección para la entrega de soluciones (AI) y la entrega de servicio (DS)

2.4.1.1 PO9 Evaluar y Administrar los Riesgos de TI

Las Entidades de Emisión de Tarjetas de Crédito y sus respectivos servicios son los más atractivos para robos de información y dinero por esta razón se ve la necesidad de realizar evaluaciones periódicas que permitan identificar riesgos que afecten a la Entidad como tal, a sus clientes o a los establecimientos que reciben pagos por este medio.

Entre los métodos de robos de los cuales personas han sido víctimas se puede describir: robos en compras, suplantación de idEntidad, venta de BDD con números de tarjetas, fechas de seguridad y códigos de seguridad, clonación de

[43] COBIT 4.1-2007. IT Governance Institute

tarjetas, extracción de claves, etc.; tanto para tarjetas nacionales como internacionales.

Se requiere un marco de trabajo de administración de riesgos que contenga estrategias de mitigación y riesgos residuales los que deben reducirse a un nivel aceptable. Cada uno de los objetivos de control del proceso PO9 fueron mapeados de la siguiente manera:

PO 9.1 mapeado con:

ITIL: SD 9.5, SD 4.5.5.1

ISO/IEC: 14.1.1, 14.1.2

NIST: RA-1

PO 9.2 mapeado con:

ITIL: SS 9.5, SD 4.5.5.1, SD 4.5.5.2

ISO/IEC: 14.1.1, 14.1.2

NIST: RA-1

PO 9.3 mapeado con:

ITIL: SS 9.5, SD 4.5.5.2, ST 9, CSI 5.6.3

ISO/IEC: 13.1.1, 13.1.2

NIST: RA-3, RA-5

PO 9.4 mapeado con:

ITIL: SS 9.5, SD 4.5.5.2, SD 8.1, ST 4.6

ISO/IEC: 5.1.2, 14.1.2

NIST: RA-3, RA-4

PO 9.5 mapeado con:

ITIL: SS 9.5, SD 4.5.5.3, ST, ST 4.6

NIST: IR-1, IR-4

PO 9.6 mapeado con:

ITIL: SS 9.5, SD 4.5.5.4

NIST: IR-1, IR-4

2.4.2 ADQUIRIR E IMPLEMENTAR[44]

Dominio Adquirir e Implementar (AI), proporciona las soluciones y las pasa para convertirlas en servicios

2.4.2.1 AI3 Adquirir y mantener infraestructura tecnológica

Las Entidades de Emisión de Tarjetas de Crédito deben contar con procesos para adquirir, implementar y actualizar infraestructura tecnológica tanto en el Site Principal como en el Alterno, además se debe garantizar que exista un soporte tecnológico continuo para las aplicaciones.

[44] COBIT 4.1-2007. IT Governance Institute

Se debe incluir una revisión periódica de los requerimientos del negocio, administración de parches y estrategias de actualización, riesgos evaluación de vulnerabilidades y requerimientos de seguridad.

Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y software del Site Alterno.

Además sería ideal contar con un plan de mejoras que permita aumentar la capacidad, la vida útil de la inversión, etc.

Cada uno de los objetivos de control del proceso AI3 fueron mapeados de la siguiente manera:

AI 3.1 mapeado con:

ITIL: SD 3.6.3

AI 3.2 mapeado con:

ITIL: SD 4.6.5.1, SO 5.4

ISO/IEC: 12.1.1

AI 3.3 mapeado con:

ITIL: SO 5.4, SO 5.5, SO 5.7, SO 5.8, SO 5.9, SO 5.10, SO 5.11

ISO/IEC: 9.1.5, 9.2.4, 12.4.2, 12.5.2, 12.6.1

AI 3.4 mapeado con:

ITIL: ST 4.4.5.1, ST 4.4.5.2, ST 4.4.5.3, ST 4.4.5.7, ST 4.5.7

ISO/IEC: 10.1.4

2.4.2.2 AI6 Administrar cambios

Para las Entidades Emisoras de Tarjetas de Crédito la imagen que brindan a sus usuarios es muy importante por lo cual afectaría mucho que por causa de algún cambio necesario se ocasionarían molestias a Usuarios, por lo que todos los cambios relacionados con la infraestructura y aplicaciones en ambiente de producción deben administrarse formalmente y controladamente, lo que garantiza reducción de riesgos que impactan negativamente a estabilidad de los equipos e integridad de información y aplicaciones.

Por lo que se ve la necesidad de notificar al personal involucrado, disponer de contingencias en el caso de que se presenten problemas, detallar el cambio, definir responsables del cambio, mantener un flujo de aprobación para los mismos, justificar la necesidad de llevarlo a cabo, determinar impactos, identificar la necesidad de reiniciar los servicios o servidores.

Cada uno de los objetivos de control del proceso AI6 fueron mapeados de la siguiente manera:

AI 6.1 mapeado con:

ITIL: ST 4.2.6.1, ST 5, ST 6, ST 6.3, ST 6.4, SO 4.6.1

NIST: CM-1, CM-3

AI 6.2 mapeado con:

ITIL: ST 4.2.6.2, ST 4.2.6.3, ST 4.2.6.4, ST 4.2.6.5, ST 4.2.6.6, ST 4.2.6.8, ST 4.6, SO 4.3.5.1, SO 4.3.5.2, SO 4.3.5.3

ISO/IEC: 10.1.2, 12.5.1, 12.5.3, 12.6.1

AI 6.3 mapeado con:

ITIL: ST 4.2.6.9

ISO/IEC: 10.1.2, 11.5.4, 12.5.1, 12.5.3, 12.6.1, CM-3

AI 6.4 mapeado con:

ITIL: ST 3.2.13, ST 3.2.14, ST 4.1.5.3, ST 4.1.6

ISO/IEC: 10.1.2

AI 6.5 mapeado con:

ITIL: ST 4.2.6.4, ST 4.2.6.7, ST 4.4.5.10, ST 4.4.5.9, SO 4.3.5.5

ISO/IEC: 10.1.2

2.4.3 ENTREGAR Y DAR SOPORTE[45]

Dominio Entregar y Dar Soporte (DS), recibe las soluciones y las hace utilizables por los usuarios finales.

[45] COBIT 4.1-2007. IT Governance Institute

2.4.3.1 DS1 Definir y administrar los niveles de servicio

Las Entidades de Tarjetas de Crédito deberían contar con una estructura organizacional con información que permita una gestión adecuada de niveles de servicio en la que se tenga definido roles, tareas y responsabilidades de proveedores.

Es necesario que se cuente con Acuerdos de Niveles de Servicios (SLAs) para los procesos críticos de TI y Acuerdos de Niveles de Operación (OLAs) para los procesos técnicos, la información debe estar organizada en un catálogo de servicios que los describe, los organiza y detalla.

Es necesario que se monitoree continuamente el desempeño y se reporten en formatos, de tal modo que se puedan identificar tendencias positivas y negativas tanto de servicios individuales como en conjunto

Cada uno de los objetivos de control del proceso DS1 fueron mapeados de la siguiente manera:

DS 1.1 mapeado con:

ITIL: SS 2.6, SS 4.3, SS 4.4, SS 7.2, SS 7.3, SS 7.5, SD 4.2.5.1, SD 4.2.5.9

ISO/IEC: 10.2.1

DS 1.2 mapeado con:

ITIL: SS 4.2, SS 4.3, SS 5.4, SS 5.5, SS 7.2, SS 7.3, SS 7.4, SS 7.5, SS 8.2, SD 3, SD 3.1, SD 3.2, SD 3.4, SD 3.5, SD 3.6, SD 4.1

ISO/IEC: 10.2.1

DS 1.3 mapeado con:

ITIL: SD 4.2.5.2, SD APÉNDICE F

ISO/IEC: 10.2.1

DS 1.4 mapeado con:

ITIL: SD 4.2.5.5, SD APÉNDICE F

DS 1.5 mapeado con:

ITIL: SS 5.3, SD 4.2.5.3, SD 4.2.5.6, SD 4.2.5.7, SD 4.2.5.10, SD 4.3.8,

DS 1.6 mapeado con:

ITIL: SD 4.2.5.4, SD 4.2.5.5, SD 4.2.5.8

NIST: SA-9

2.4.3.2 DS2 Administrar los servicios de terceros

Debido al alto costo de mantener un Site Caliente que es el que por lo general disponen las Entidades de Tarjetas de Crédito, en ocasiones se ve la necesidad de rentar ciertos servicios a proveedores los cuales deben encontrarse plenamente descritos, deben estar categorizados considerando las funciones, tipo de beneficio, criticidad, etc.

Se deben identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de manera segura y que permita una alta disponibilidad del mismo.

La administración del riesgo debe considerar Acuerdos de Confidencialidad NDAs, contratos de garantía, viabilidad de continuidad de servicio con un proveedor, conformidad de los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos.

Todo lo descrito anteriormente con la finalidad de asegurar que en el momento en que la Entidad deba utilizar el Site Alterno tenga el control de la situación y la disponibilidad esperada.

Cada uno de los objetivos de control del proceso DS2 fueron mapeados de la siguiente manera:

DS 2.1 mapeado con:

ITIL: SS 7.3, SD 4.7.5.1

ISO/IEC: 6.2.1

DS 2.2 mapeado con:

ITIL: SD 4.2.5.9, SD 4.7.5.2, SD 4.7.5.4, SD 4.7.5.5

ISO/IEC: 6.2.3, 10.2.3, 15.1.4

NIST: PS-7

DS 2.3 mapeado con:

ITIL: SD 4.7.5.3, SD 4.7.5.5

ISO/IEC: 6.2.1, 6.2.3, 8.1.2, 8.13, 10.2.3, 10.8.2

NIST: SA-9

DS 2.4 mapeado con:

ITIL: SD 4.7.5.4

ISO/IEC: 6.2.3, 10.2.1, 10.2.2. 12.4.2, 12.5.

2.4.3.3 DS3 Administrar el desempeño y la capacidad

Se debe establecer un plan para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad con costos aceptables de tal modo que se puedan procesar las cargas de trabajo definidas en los SLAs.

Es importante alcanzar un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares con la finalidad de minimizar riesgos y evitar interrupciones de servicio, tratando que incluso el cambio del Site Principal al Alterno sea un evento imperceptible para los Usuarios.

Se debe monitorear continuamente el desempeño y la capacidad de los recursos de TI, emitir reportes de excepción con recomendaciones y acciones correctivas.

El administrar el desempeño y la capacidad nos permitirá identificar incluso en qué condiciones realizar el cambio de Site, así como el nivel que soportaría el Site Principal que en determinado momento podría ser solventado por el Alterno.

Cada uno de los objetivos de control del proceso DS3 fueron mapeados de la siguiente manera:

DS 3.1 mapeado con:

ITIL: SD 4.3.5.1, SD APÉNDICE J, CSI 5.6.2

ISO/IEC: 10.3.1

DS 3.2 mapeado con:

ITIL: SD 4.3.5.2, SD 4.3.5.3, SO 4.1.5.2, SO 4.1.5.3, SO 5.4, CSI 4.3

ISO/IEC: 10.3.1

DS 3.3 mapeado con:

ITIL: SD 4.3.5.1, SD 4.3.5.2, SD 4.3.5.3, SD 4.3.5.7, SD 4.3.8

ISO/IEC: 10.3.1

DS 3.4 mapeado con:

ITIL: SD 4.3.5.3, SD 4.3.5.4, SD 4.4, SD 4.4.5.1, SD 4.4.5.2, SO 4.6.5, CSI 5.6.1

DS 3.5 mapeado con:

ITIL: SD 4.3.5.4, SD 4.3.5.5, SD 4.3.5.6, SD 4.4.5.1

2.4.3.4 DS4 Garantizar la continuidad del servicio

El principal objetivo de disponer de un Site Alterno en una Entidad Emisora de Tarjetas de Crédito es mantener la continuidad del servicio en el caso de que se presenten problemas en el Site Principal, pero para que ello se lleve a cabo de una manera ordenada es necesario desarrollar un plan en base al marco de trabajo y la experiencia de eventos anteriores, que incluso permitirá reducir el impacto en las funciones y procesos claves de la Entidad.

Es importante centrar la atención en los procesos críticos para establecer prioridades en situaciones de recuperación, asegurando también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales.

Se debe realizar un entrenamiento del plan de continuidad de TI con el personal involucrado, planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios.

Se ve la necesidad de contar con un Gerente encargado de este proceso que permita una gestión adecuada del mismo.

Cada uno de los objetivos de control del proceso DS4 fueron mapeados de la siguiente manera:

DS 4.1 mapeado con:

ITIL: SD 4.5, SD 4.5.5.1, CSI 5.6.3

ISO/IEC: 6.1.6, 6.1.7, 14.1.1, 14.1.2, 14.1.4

NIST: CP-1, CP-6, CP-7, CP-8

DS 4.2 mapeado con:

ITIL: SD 4.5.5.2, SD 4.5.5.3, SD

ISO/IEC: 6.1.6, 6.1.7, 14.1.3

NIST: CP-2, CP-4, CP-9

DS 4.3 mapeado con:

ITIL: SD 4.4.5.2, SD 4.5.5.4

ISO/IEC: 14.1.1, 14.1.2

DS 4.4 mapeado con:

ITIL: SD 4.5.5.4

ISO/IEC: 14.1.5

NIST: CP-5

DS 4.5 mapeado con:

ITIL: SD 4.5.5.3, SD 4.5.5.4

ISO/IEC: 14.1.5

NIST: CP-4

DS 4.6 mapeado con:

ITIL: SD 4.5.5.3, SD 4.5.5.4

ISO/IEC: 14.1.5

NIST: CP-3

DS 4.7 mapeado con:

ITIL: SD 4.5.5.3, SD 4.5.5.4

ISO/IEC: 14.1.5

DS 4.8 mapeado con:

ITIL: SD 4.5.5.3, SD 4.5.5.4

ISO/IEC: 14.1.1, 14.1.3

NIST: CP-7, CP-10

DS 4.9 mapeado con:

ITIL: SD 4.5.5.2, SO 5.2.3

ISO/IEC: 10.5.1

NIST: CP-6, CP-9

DS 4.10 mapeado con:

ITIL: SD 4.5.5.3, SO 4.5.5.4

ISO/IEC: 14.1.5

2.4.3.5 DS5 Garantizar la seguridad de los sistemas

Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI con la finalidad de mantener la integridad de la información y proteger los activos de TI.

Es necesario identificar los requerimientos, vulnerabilidades y amenazas de seguridad para minimizar el impacto en incidentes y problemas detectados. Se debe establecer medidas correctivas para la prevención, detección y corrección de software malicioso que afecte tanto el Site Principal como el Alterno.

En este proceso se contempla la gestión adecuada de claves criptográficas con sus respectivos procedimientos para cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso e incluso archivo para garantizar la protección contra modificaciones o uso inadecuado de las mismas.

Se ve la necesidad de garantizar que la tecnología es resistente al sabotaje y revele lo estrictamente necesario. Es importante asegurar que todos los usuarios y su actividad en sistemas sean identificables de mantera única, validar constantemente y depurar los permisos de accesos brindados así como las aprobaciones para la obtención de los mismos. Cada uno de los objetivos de control del proceso DS4 fueron mapeados de la siguiente manera:

DS 5.1 mapeado con:

ITIL: SD 4.6, SO 5.13

ISO/IEC: 6.1.1, 6.1.2, 6.2.3, 6.2.2

DS 5.2 mapeado con:

ITIL: SD 4.6.4, SD 4.6.5.1

ISO/IEC: 5.1.1, 5.1.2, 6.1.2, 6.1.5, 8.2.2, 11.1.1, 11.7.1, 11.7.2

NIST: PL-1, PL-2, PL-4, SC-1

DS 5.3 mapeado con:

ITIL: SO 4.5

ISO/IEC: 5.1.1, 5.1.2, 6.1.2, 6.1.5, 8.2.2, 11.1.1, 11.7.1, 11.7.2

NIST: IA-1, IA-2, IA-4

DS 5.4 mapeado con:

ITIL: SO 4.5, SO 4.5.5.1, SO 4.5.5.2, SO 4.5.5.3, SO 4.5.5.4, SO 4.5.5.5, SO 4.5.5.6

ISO/IEC: 6.1.5, 6.2.1, 6.2.2, 8.1.1, 8.3.1, 8.3.3, 10.1.3, 11.1.1, 11.2.1, 11.2.2, 11.2.4, 11.3.1, 11.5.1, 11.5.3, 11.6.1

NIST: AC-2, IA-4, PS-6

DS 5.5 mapeado con:

ITIL: SO 4.5.5.6, SO 5.13

ISO/IEC: 6.1.8, 10.10.2, 10.10.3, 10.10.4, 12.6.1, 13.1.2, 15.2.2, 15.3.1

NIST: AU-6, CA-2, CA-6, CA-7, CM-4, RA-5, SI-4

DS 5.6 mapeado con:

ITIL: SD 4.6.5.1, SD 4.6.5.2

ISO/IEC: 8.2.3, 13.1.1, 13.1.2, 13.2.1, 13.2.3

NIST: IR-1, IR-6

DS 5.7 mapeado con:

ITIL: SO 5.4

ISO/IEC: 6.1.4, 9.1.6, 9.2.1, 9.2.3, 10.6.2, 10.7.4, 10.10.1. 10.10.3, 10.10.4, 10.10.5, 10.10.6, 11.3.2, 11.3.3, 11.4.4, 11.5.1, 11.5.4, 11.5.5, 11.5.6, 11.6.2, 11.7.1, 11.7.2, 12.4.1, 12.6.1, 13.1.2, 13.2.3, 15 2.2, 15 3.2

NIST: PE-4, SA-5, SC-3

DS 5.8 mapeado con:

ISO/IEC: 10.8.4, 12.2.3, 12.3.2, 15.1.6

NIST: SC-12, SC-13

DS 5.9 mapeado con:

ISO/IEC: 10.4.1, 10.4.2

NIST: SC-18, SI-3, SI-7, SI-8

DS 5.10 mapeado con:

ITIL: SO 5.5

ISO/IEC: 6.2.1, 10.6.2, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.6.2

NIST: AC-4, SC-7, SI-4

DS 5.11 mapeado con:

ISO/IEC: 6.2.1, 10.6.1, 10.6.2, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.6.2

NIST: AU-10, SC-9, SC-11, SC-16, SC-23

2.4.3.6 DS11 Administrar los datos

Se deben establecer procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos así como para la eliminación apropiada de los mismos, para garantizar la disponibilidad y calidad de información requerida.

Las Entidad Emisora de Tarjetas de Crédito debe realizar respaldos periódicos y probar la funcionalidad de los mismos mediante reanudaciones, este proceso será repetitivo entre el Site Principal y el Alterno a quien continuamente se le realizarán restauraciones de BDD de la información previamente respaldada.

Es necesario validar que todos los datos que se espera procesar han cumplido su flujo y se han procesado por completo.

Entre la información que debe respaldarse en las Entidades se menciona: análisis de crédito, información de establecimientos, información de tarjetas, caja, legal, información para servicio al cliente, procesos batch[46], procesos de ajuste, liquidaciones, inversiones, logística, conciliaciones, activos, huellas, firmas, información SMS, información de Call Center entre otras.

Cada uno de los objetivos de control del proceso DS4 fueron mapeados de la siguiente manera:

DS 11.1 mapeado con:

ITIL: SD 5.2

ISO/IEC: 10.8.1

NIST: MP-1, SI-10, SI-12

DS 11.2 mapeado con:

ITIL: SD 5.2, SD 5.6

ISO/IEC: 10.5.1, 10.7.1, 15.1.3

NIST: MP-4

DS 11.3 mapeado con:

ITIL: SD 10.7.1, SD 10.7.2, 12.4.3

DS 11.4 mapeado con:

ISO/IEC: 9.2.6, 10.7.1, 10.7.2

NIST: MP-5, MP-6

[46] Procesos que se corren por la noche en los servidores Iseries.

DS 11.5 mapeado con:

ITIL: SO 5.2.3

ISO/IEC: 10.5.1

NIST: CP 9, CP 10

DS 11.6 mapeado con:

ITIL: SD 5.2

ISO/IEC: 10.5.1, 10.7.3, 10.8.3, 10.8.4, 12.4.2, 12.4.3

NIST: AC-1, AC-3, AC-15, AC-16, MP-1, MP-2, MP-4, MP-5, MP-6, SI-10, SI-12

2.4.3.7 DS12 Administrar el ambiente físico

Tanto el Site Principal como el Alterno deben contar con instalaciones bien diseñadas y correctamente administradas con una protección adecuada de equipos así como del personal que acude a ellos.

La selección de instalaciones apropiadas incluye factores ambientales, distribución,

Control de acceso, iluminación, extinguidores, contingencia contra inundaciones, etc.; para lo cual se debe contar con un asesoramiento técnico y controles periódicos para validar que las medidas de seguridad están disponibles.

Además se debería contar con dispositivos y equipo especializado para monitorear y controlar el ambiente. Procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas para personal interno y externo.

Cada uno de los objetivos de control del proceso DS 12 fueron mapeados de la siguiente manera:

DS 12.1 mapeado con:

ISO/IEC: 9.1.1, 9.1.3, 9.1.6

NIST: PE-1, PE-18

DS 12.2 mapeado con:

ITIL: SO

ISO/IEC: 9.1.1, 9.1.2, 9.1.3, 9.2.5, 9.2.7

NIST: PE-3, PE-4, PE-16, PE-19

DS 12.3 mapeado con:

ITIL: SO, SO

ISO/IEC: 6.2.1, 9.1.2, 9.1.5, 9.1.6, 9.2.5

NIST: PE-2, PE-6, PE-7, PE-8

DS 12.4 mapeado con:

ITIL : SO

ISO/IEC : 9.1.4, 9.2.1, 9.2.2, 9.2.3, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15

DS 12.5 mapeado con:

ITIL : SO 5.12

ISO/IEC : 9.2.2, 9.2.4

NIST: PE-1

2.4.4 MONITOREAR Y EVALUAR[47]

Dominio Monitorear y Evaluar (ME), monitorear todos los procesos para asegurar que se sigue la dirección provista.

2.4.4.1 ME3 Garantizar el cumplimiento regulatorio

Es necesario establecer procesos, políticas, estándares, procedimientos de revisiones, metodologías, para garantizar el cumplimiento de leyes, regulaciones y requerimientos contractuales.

En el cumplimiento de normativas ejerce un papel muy importante el Site Alterno, el cual entrará en funcionamiento una vez que se determina que el Site Principal no está dentro de los parámetros permitidos, para ellos deberían generarse alarmas de diferentes colores que permitan alertar y contar con procedimientos en cada caso, las penalidades en caso de incumplimiento podrían ser desde sanciones laborales, sanciones empresariales, sanciones a proveedores y en casos extremos sanciones penales, por lo que se debe contar con el asesoramiento legal necesario.

Cada uno de los objetivos de control del proceso ME3 fueron mapeados de la siguiente manera:

[47] COBIT 4.1-2007. IT Governance Institute

ME 3.1 mapeado con:

ISO/IEC: 6.1.6, 15.1.1, 15.1.2, 15.1.4

NIST: SA-9

ME 3.2 no está mapeado con ninguno.

ME 3.3 mapeado con:

ISO/IEC: 6.1.6, 15.1.1, 15.1.2, 15.1.4

NIST: SA-9

ME 3.4 mapeado con:

ISO/IEC: 6.1.6, 15.1.1, 15.1.2, 15.1.4

NIST: SA-9

ME 3.5 no está mapeado con ninguno.

CAPÍTULO 3

PROPUESTA DE GESTIÓN DE LAS TIC's PARA UN SITE ALTERNO.

3.1 CASO DE ESTUDIO ENTIDAD EMISORA DE TARJETAS DE CRÉDITO

Para una correcta implementación es importante que el personal entienda qué hacer, cómo hacerlo y por qué es importante hacerlo, es preferible utilizar un lenguaje común que permita seguir un conjunto de objetivos, asuntos y prioridades, y que serán de gran utilidad en el Site Alterno que disponen las Entidades Bancarias.

Para esta guía de gestión propuesta se ha tomado como referencia documentos en los que COBIT se mapea con ITIL, ISO/IEC Y NIST.

A continuación la descripción de los pasos efectuados para obtener la guía:

3.2 DESARROLLO DE LA PROPUESTA[48]

A continuación se describe el desarrollo de la propuesta.

3.2.1 ELABORACION

Para la elaboración de la presente guía de gestión se ha considerado:

La gobernabilidad que proporciona una política de gestión y un marco de control, para facilitar: asignación de propietarios, responsabilidades, rendición de cuentas para actividades de TI, definición de objetivos, prioridades, asignación de

[48] Alineando COBIT 4.1, ITIL V3 4.1, ITIL v3 e ISO/IEC 27002 en beneficio del Negocio, Reporte del ITGI y la OGC.

recursos, identificación de riesgos, administración de recursos con eficacia y eficiencia, monitoreo y evaluación de actividades críticas y medidas correctivas.

La Entidad Bancaria debe definir los servicios que necesita solventar con el Site Alterno, con objetivos claros, descripción de los servicios que debe brindar una vez que ha sido levantado, niveles de servicio, contratos que se deben respetar, requerimientos de clientes para establecer prioridades relativas para que los recursos se asignen de manera equitativa y viable.

3.2.2 PRIORIZACIÓN

Las Entidades Bancarias necesitan priorizar dónde y cómo utilizar las mejores prácticas, se requiere un plan de acción eficaz que se adapte a las circunstancias y necesidades particulares.

Es importante es que la alta dirección asuma el liderazgo del gobierno de TI y defina la gestión que se va a seguir, se debe establecer un comité para comunicar los aspectos de TI a la alta dirección y administración de la Entidad Bancaria.

3.2.3 PLANIFICACIÓN

A la Entidad Bancaria, se le sugiere llevar a cabo los siguientes pasos:

1. Establecer un marco organizativo, con objetivos y responsabilidades claras, participación de involucrados, quienes impulsarán la implementación y la asumirán como una iniciativa propia.
2. Alinear la estrategia con los objetivos del negocio, obtener una buena comprensión del entorno empresarial, los riesgos, las directrices, objetivos, acuerdos de nivel de servicios y métricas.

3. Entender y definir los riesgos.
4. Definir las áreas objetivo y determinar las áreas de proceso de TI críticos para la entrega de valor y gestionarlas adecuadamente.
5. Analizar la capacidad vigente e identificar brechas, identificar los lugares donde se necesitan mejoras.
6. Desarrollar estrategias para mejorar e identificar los proyectos de prioridad que ayudarán a mejorar la gestión y el gobierno de las áreas importantes, basada en beneficio potencial y facilidad de implementación, se deben impulsar proyectos de mejora continua.
7. Medición de resultados del desempeño actual y monitoreo de resultados.
8. Repetir los pasos 2 al 7 con la mayor frecuencia posible.

3.2.4 SELECCIÓN DE LOS PROCESOS A SER MAPEADOS EN ESTA GUÍA DE GESTIÓN

A continuación se va a escoger los procesos que van a ser mapeados en esta guía de gestión para el Site Alterno de una Entidad emisora de Tarjetas de Crédito. Las mejores prácticas de TI deben ajustarse a los requisitos del negocio y ser integradas entre sí y con los procedimientos internos, ofreciendo un marco general de control basado en un modelo de procesos de TI que debería adaptarse a cada organización y los estándares y prácticas específicas abarcan áreas determinadas.

Para una adecuada gestión de un Site Alterno en una Entidad Bancaria se han seleccionado 11 procesos, puesto que a nuestro criterio son los que están más relacionados a una adecuada gestión, sin embargo de acuerdo a la situación de la Entidad Bancaria se podrían incluir mas procesos.

3.2.4.1 Planear y Organizar[49]

A través de este dominio es posible diseñar las tácticas y estrategias que se deben seguir, de tal forma que la tecnología de la información pueda contribuir para alcanzar los objetivos para los cuales fue creado el Site Alterno y apoyando las necesidades que tiene la Entidad Emisora de Tarjetas de Crédito.

A través de este dominio de COBIT también es posible que la visión de la empresa sea planeada y comunicada, todo ello se puede alcanzar en base a una organización y una infraestructura tecnológica correctamente diseñada para las funciones que debe cumplir el Site.

Para alcanzar los objetivos planteados se definirá la infraestructura a adquirir y las implementaciones que se llevarán a cabo, así como las directrices para el tipo de servicio que se pretende brindar con el Site.

A través de este dominio se puede verificar si están alineándose las estrategias de TI al negocio, validar si la empresa está alcanzando el óptimo de sus recursos con este Site Alterno, si entienden todas las personas dentro de la organización los objetivos de TI, determinar si se entienden y administran los riesgos de TI del Site Alterno y finalmente si es apropiada la calidad de los sistema de TI para las necesidades del negocio.

PO9 Evaluar y Administrar los Riesgos de TI

Las Entidades de Emisión de Tarjetas de Crédito y sus respectivos servicios son los más atractivos para robos de información y dinero por esta razón se ve la necesidad de realizar evaluaciones periódicas que permitan identificar riesgos que afecten a la Entidad como tal, a sus clientes o a los establecimientos que reciben pagos por este medio.

[49] COBIT 4.1-2007. IT Governance Institute

Entre los métodos de robos de los cuales personas han sido víctimas se puede describir: robos en compras, suplantación de idEntidad, venta de BDD con números de tarjetas, fechas de seguridad y códigos de seguridad, clonación de tarjetas, extracción de claves, etc.; tanto para tarjetas nacionales como internacionales.

Se requiere un marco de trabajo de administración de riesgos que contenga estrategias de mitigación y riesgos residuales los que deben reducirse a un nivel aceptable.

PO9.1 Marco de Trabajo de Administración de Riesgos, es necesario que se establezca un marco de trabajo de administración de riesgos que podrían sufrir el Site Principal como el Alterno, mismo que debe estar alineado a los objetivos de la Entidad Emisora de Tarjetas de Crédito.

PO9.2 Establecimiento del Contexto del Riesgo, es necesario que se determine el ambiente en el cual el marco de trabajo de evaluación de riesgos se debe aplicar para obtener los resultados esperados, de tal modo que se determina el contexto interno, el contexto externo de las evaluaciones de riegos, el objetivo que se pretende alcanzar al realizar la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.3 Identificación de Eventos, Identificar las amenazas que puedan tener un alto impacto en las operaciones críticas de la Entidad Emisora de Tarjetas de Crédito, en ámbito regulatorio, legal, tecnológico, comercial, de talento humano, operativo, etc. determinar la naturaleza del impacto y llevar un registro los riesgos.

PO9.4 Evaluación de Riesgos de TI, de manera continua se deben evaluar los riesgos tanto en el Site Principal como en el Alterno, usando métodos cualitativos y cuantitativos, la probabilidad de ocurrencia y el impacto a los riesgos inherentes y residuales, partiendo del portafolio de servicios.

PO9.5 Respuesta a los Riesgos, es necesario desarrollar y mantener un proceso de respuesta a riesgos diseñado de tal manera que asegure que los controles efectivos bajen la probabilidad de ocurrencia, este proceso debería contener

estrategias para evitar riesgos, métodos para reducir riesgos, identificación de riesgos, responsables, niveles de tolerancia, entre otros.

PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos, priorizar y planear todos los niveles de respuesta a riesgos, obtener la aprobación para las acciones a tomar en cada caso, asegurándose de que cada responsable cumpla el papel que le corresponda el momento indicado, cuando se presenten problemas en el Site Principal y se deba utilizar el Site Alterno.

3.2.4.2 Adquirir e Implementar[50]

El Site Alterno fue creado con la finalidad de cumplir una cantidad de objetivos para que se ejecuten se deben brindar soluciones las que pueden adquirirse e implementarse, también se contempla desarrollos internos y sus respectivas implementaciones.

Se incluye los cambios y el mantenimiento a aplicaciones, para asegurar que el Site Alterno funcionará de la manera esperada, en el momento que se presenten los desastres.

Por medio de este dominio se pude identificar si es probable que los nuevos proyectos para el Site Alterno generen soluciones que satisfagan las necesidades del negocio, si es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto, si trabajarán adecuadamente los nuevos sistemas para el funcionamiento del Site una vez sean implementados y si los cambios no afectarán a las operaciones actuales del negocio, sino mas bien son un apoyo al Site Principal.

[50] COBIT 4.1-2007. IT Governance Institute

AI3 Adquirir y mantener infraestructura tecnológica

Las Entidades de Emisión de Tarjetas de Crédito deben contar con procesos para adquirir, implementar y actualizar infraestructura tecnológica tanto en el Site Principal como en el Alterno, además se debe garantizar que exista un soporte tecnológico continuo para las aplicaciones.

Se debe incluir una revisión periódica de los requerimientos del negocio, administración de parches y estrategias de actualización, riesgos evaluación de vulnerabilidades y requerimientos de seguridad.

Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y software del Site Alterno.

Además sería ideal contar con un plan de mejoras que permita aumentar la capacidad, la vida útil de la inversión, etc.

AI3.1 Plan de Adquisición de infraestructura tecnológica, generar un plan de adquisición para disponer de una infraestructura tecnológica adecuada a las necesidades del Site Alterno.

AI3.2 Protección y disponibilidad del recurso de la infraestructura, implementar medidas de control interno de tal manera que se cuida y protege tanto el hardware como el software que nos permite que el Site Alterno se encuentre disponible.

AI3.3 Mantenimiento de la infraestructura, disponer de una estrategia de mantenimiento para que tanto la infraestructura como los sistemas que forman parte del Site Alterno, prolonguen su tiempo de mundo.

AI3.4 Ambiente de prueba de factibilidad, desarrollar pruebas para soportar la efectividad y eficiencia, se debe considerar la confidencialidad, la configuración de hardware y software.

AI6 Administrar cambios

Para las Entidades Emisoras de Tarjetas de Crédito la imagen que brindan a sus usuarios es muy importante por lo cual afectaría mucho que por causa de algún cambio necesario se ocasionarían molestias a Usuarios, por lo que todos los cambios relacionados con la infraestructura y aplicaciones en ambiente de producción deben administrarse formalmente y controladamente, lo que garantiza reducción de riesgos que impactan negativamente a estabilidad de los equipos e integridad de información y aplicaciones.

Por lo que se ve la necesidad de notificar al personal involucrado, disponer de contingencias en el caso de que se presenten problemas, detallar el cambio, definir responsables del cambio, mantener un flujo de aprobación para los mismos, justificar la necesidad de llevarlo a cabo, determinar impactos, identificar la necesidad de reiniciar los servicios o servidores.

AI6.1Estándares y procedimientos para cambios, se debe mantener un procedimiento para mantenimiento y ejecución de parches, parámetros de sistema y servicio, y plataformas fundamentales.

AI6.2 Evaluación de impacto, priorización y autorización, asegurarse de que todas las solicitudes de cambio se evalúan de una manera ordenada en cuanto a impactos y funcionalidad, se deberá categorizar los cambios y priorizarlos de tal modo que el Site Alterno no se vea afectado

AI6.3 Cambios de emergencia, establecer un proceso para definir, plantear y autorizar cambios los cambios que son de emergencia, con el debido justificativo y posteriormente se ve la necesidad de documentar lo sucedido.

AI6.4 Seguimiento y reporte del estatus de cambio, se debe realizar un seguimiento adecuado para que se mantenga actualizados a los solicitantes de

cambio, a los involucrados, informándoles los cabios y procedimientos que se están realizando.

AI6.5 Cierre y documentación del cambio, es necesario documentar todos los cambios que se produzcan en el Site con sus respectivos procedimientos.

3.2.4.3 Entregar y Dar Soporte[51]

Este dominio está directamente relacionado a la entrega de servicios requeridos para el funcionamiento del Site Alterno, incluye las operaciones que se realizan a diario, permite el entrenamiento del personal involucrado, cuida aspectos de seguridad y sobretodo la continuidad de los servicios que se debe continuar brindando luego de un desastre. Por lo que los servicios deben estar claramente definidos pero se debe tener especial énfasis en los más críticos de tal manera que se disponga de prioridades.

Por medio de este dominio es posible identificar si el procesamiento de información también es considerado en este dominio, puesto que el Site Alterno debería procesar de manera casi exacta al Site Principal, si se están entregando los servicios de TI de acuerdo con las prioridades del negocio, si se están optimizados los costos de TI para el Sita Alterno Caliente, si es capaz la fuerza del trabajo de utilizar los sistemas de TI de manera productiva y segura, si están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad en el Site Alterno.

DS1 Definir y administrar los niveles de servicio

Las Entidades de Tarjetas de Crédito deberían contar con una estructura organizacional con información que permita una gestión adecuada de niveles de

[51] COBIT 4.1-2007. IT Governance Institute

servicio en la que se tenga definido roles, tareas y responsabilidades de proveedores.

Es necesario que se cuente con Acuerdos de Niveles de Servicios (SLAs) para los procesos críticos de TI y Acuerdos de Niveles de Operación (OLAs) para los procesos técnicos, la información debe estar organizada en un catálogo de servicios que los describe, los organiza y detalla.

Es necesario que se monitoree continuamente el desempeño y se reporten en formatos, de tal modo que se puedan identificar tendencias positivas y negativas tanto de servicios individuales como en conjunto

DS1.1 Marco de trabajo de la administración de los niveles de servicio, se debe definir un marco de trabajo que permita una adecuada gestión de los niveles de servicio que requiere el Site Alterno.

DS1.2 Definición de servicios, es necesario definir los servicios con sus respectivos detalles y características por medio de un catálogo de servicios que estará disponible.

DS1.3 Acuerdos de niveles de servicios, acordar los niveles de servicios para los procesos críticos y menos críticos de la Entidad Emisora de Tarjetas de Crédito.

SD1.4 Acuerdos de niveles de operación, es necesario mantener acuerdos de niveles de operación y en función de ello se llevarían a cabo las actividades.

DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio, es importante que se lleve un control que permita identificar el correcto cumplimiento de niveles de servicio que deben llevarse a cabo.

DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos, se deben realizar revisiones periódicas a los acuerdos de niveles de servicio y a los contratos firmados con la finalidad de identificar si al momento el Site Alterno está alcanzando los objetivos para los que fue creado.

DS2 Administrar los servicios de terceros

Debido al alto costo de mantener un Site Caliente que es el que por lo general disponen las Entidades de Tarjetas de Crédito, en ocasiones se ve la necesidad de rentar ciertos servicios a proveedores los cuales deben encontrarse plenamente descritos, deben estar categorizados considerando las funciones, tipo de beneficio, criticidad, etc.

Se deben identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de manera segura y que permita una alta disponibilidad del mismo.

La administración del riesgo debe considerar Acuerdos de Confidencialidad NDAs, contratos de garantía, viabilidad de continuidad de servicio con un proveedor, conformidad de los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos.

Todo lo descrito anteriormente con la finalidad de asegurar que en el momento en que la Entidad deba utilizar el Site Alterno tenga el control de la situación y la disponibilidad esperada.

DS2.1 Identificación de todas las relaciones con los proveedores, tener identificados todos los servicios de los proveedores y categorizarlos en base al tipo, mantener documentación técnica y de organización que cubren los roles y responsabilidades a cumplirse.

DS2.2 Gestión de relaciones con proveedores, para una gestión adecuada de relaciones con proveedores y cumplimiento de los acuerdos es necesario que se disponga de SLAs para los servicios prestados por proveedores del Site Alterno.

DS2.3 Administración de riesgos del proveedor, es importante identificar los riesgos para posteriormente mitigarlos, y a través de los contratos se pueda asegurar que el proveedor cumplirá, además se deben firmar acuerdos de confidencialidad NDAs, garantías y viabilidad de continuidad en base al

cumplimiento, para que una vez que el Site Alterno entre en funcionamiento no se tengan problemas por incumplimiento.

DS2.4 Monitoreo del desempeño del proveedor, se debe monitorear para garantizar que se están cumpliendo nos SLAs acordados y que el desempeño es competitivo versus a otros proveedores que brindan servicios similares para Sites Alternos.

DS3 Administrar el desempeño y la capacidad

Se debe establecer un plan para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad con costos aceptables de tal modo que se puedan procesar las cargas de trabajo definidas en los SLAs.

Es importante alcanzar un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares con la finalidad de minimizar riesgos y evitar interrupciones de servicio, tratando que incluso el cambio del Site Principal al Alterno sea un evento imperceptible para los Usuarios.

Se debe monitorear continuamente el desempeño y la capacidad de los recursos de TI, emitir reportes de excepción con recomendaciones y acciones correctivas.

El administrar el desempeño y la capacidad se puede identificar incluso en qué condiciones realizar el cambio de Site, así como el nivel que soportaría el Site Principal que en determinado momento podría ser solventado por el Alterno.

DS3.1 Planeación del desempeño y la capacidad, es necesario establecer un plan el que contenga la capacidad actual y el desempeño de los recursos de TI.

DS3.2 Capacidad y desempeño actual, revisar periódicamente si la capacidad y el desempeño actual cumplen los SLAs.

DS3.3 Capacidad y desempeño futuros, realizar análisis para identificar los requerimientos próximos tanto en capacidad como en rendimiento de recursos de TI.

DS3.4 Disponibilidad de recursos de TI, una gestión adecuada debería asegurar la disponibilidad de los planes de contingencia de la capacidad y rendimiento de cada uno de los recursos de TI.

DS3.5 Monitoreo y reporte

DS4 Garantizar la continuidad del servicio

El principal objetivo de disponer de un Site Alterno en una Entidad Emisora de Tarjetas de Crédito es mantener la continuidad del servicio en el caso de que se presenten problemas en el Site Principal, pero para que ello se lleve a cabo de una manera ordenada es necesario desarrollar un plan en base al marco de trabajo y la experiencia de eventos anteriores, que incluso permitirá reducir el impacto en las funciones y procesos claves de la Entidad.

Es importante centrar la atención en los procesos críticos para establecer prioridades en situaciones de recuperación, asegurando también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales.

Se debe realizar un entrenamiento del plan de continuidad de TI con el personal involucrado, planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios.

Se ve la necesidad de contar con un Gerente encargado de este proceso que permita una gestión adecuada del mismo.

DS4.1 Marco de trabajo de continuidad de TI, se debe desarrollar un marco de trabajo para continuidad de TI que permita la recuperación de desastres y defina las contingencias en cada caso, se deben identificar los recursos críticos, para

administrar la continuidad se deberá redactar la cobertura de cada rol, así como las tareas y responsabilidades para cada caso.

DS4.2 Planes de continuidad de TI, desarrollar un plan basado en el marco de trabajo con la finalidad de reducir el impacto que pueda tener el evento dado, es decir en el caso de requerir utilizar el Site Alterno se cuenta con este plan que explicará a detalle los pasos a seguir.

DS4.3 Recursos críticos de TI, es necesario que se definan los recursos que mayor impacto tienen para la Entidad, puesto que en base a esa prioridad se levantarían.

DS4.4 Mantenimiento del plan de continuidad de TI, el plan de continuidad debe actualizarse periódicamente, para que refleje de manera continua los requerimientos.

DS4.5 Pruebas del plan de continuidad de TI, es necesario que se ejecuten varias pruebas de funcionalidad de tal manera que se evidencie la aplicabilidad del plan que se está tomando como referencia.

DS4.6 Entrenamiento del plan de continuidad de TI, a todo el personal involucrado se le debe capacitar y luego verificar los resultados obtenidos en las pruebas para analizar el nivel en el que se encuentran o identificar la necesidad de nuevas capacitaciones y entrenamiento.

DS4.7 Distribución del plan de continuidad de TI, se debe distribuir el plan para que se difunda de tal manera que pueda alcanzarse el éxito esperado y es importante que se encuentren accesibles en el momento del desastre.

DS4.8 Recuperación y reanudación de los servicios de TI, planear las acciones a tomar durante el período que TI está recuperando y reanudando los servicios.

DS4.9 Almacenamiento de respaldos fuera de las instalaciones, es importante almacenar fuera de las instalaciones del Site Principal todos los respaldos, controladores, configuraciones, para en caso de desastre no se vean afectadas.

DS4.10 Revisión post reanudación, luego de la reanudación del plan se debe realizar una supervisión, la gerencia debe determinar si la gerencia de TI ha establecido procedimientos para valorar lo que se realizó adecuadamente y actualizar lo que no fue adecuado.

DS5 Garantizar la seguridad de los sistemas

Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI con la finalidad de mantener la integridad de la información y proteger los activos de TI.

Es necesario identificar los requerimientos, vulnerabilidades y amenazas de seguridad para minimizar el impacto en incidentes y problemas detectados. Se debe establecer medidas correctivas para la prevención, detección y corrección de software malicioso que afecte tanto el Site Principal como el Alterno.

En este proceso se contempla la gestión adecuada de claves criptográficas con sus respectivos procedimientos para cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso e incluso archivo para garantizar la protección contra modificaciones o uso inadecuado de las mismas.

Se ve la necesidad de garantizar que la tecnología es resistente al sabotaje y revele lo estrictamente necesario.

Es importante asegurar que todos los usuarios y su actividad en sistemas sean identificables de mantera única, validar constantemente y depurar los permisos de accesos brindados así como las aprobaciones para la obtención de los mismos.

DS5.1 Administración de la seguridad de TI, administrar la seguridad al nivel más alto posible para el Site Alterno, para que se cumplan con los objetivos por el cual fue creado.

DS5.2 Plan de seguridad de TI, se debe contar con un plan de seguridad que contenga políticas, procedimientos, servicios, personal, hardware software

DS5.3 Administración de idEntidad, todas las personas para acceder a cada aplicación deben autenticarse adecuadamente de tal modo que se pueda rastrear cada actividad realizada.

DS5.4 Administración de cuentas de usuario, las cuentas de usuario deben ser gestionadas adecuadamente tanto para entregarlas como para revocarlas, adicionalmente es necesario que continuamente se revisen los permisos concedidos.

DS5.5 Pruebas, vigilancia y monitoreo de la seguridad, garantizar que la seguridad del Site Alterno sea probada y monitoreada, para detección de actividades inusuales o anormales.

DS5.6 Definición de incidente de seguridad, es necesario que se identifiquen los incidentes con la finalidad de que puedan ser tratados adecuadamente.

DS5.7 Protección de la tecnología de seguridad, evitar el sabotaje e impedir que se revele información innecesaria.

DS5.8 Administración de llaves criptográficas, desarrollar procedimientos para encriptación, revocación, cambio, distribución y uso de llaves criptográficas que estén implementadas.

DS5.9 Prevención, detección y corrección de software malicioso, mantener procedimientos y medidas preventivas, de detección, de corrección, contar con parches actualizados para proteger los sistemas y la información.

DS5.10 Seguridad de la red, se deben establecer permisos de seguridad en la red como firewalls, dispositivos de seguridad, controles de virus.

DS5.11 Intercambio de datos sensitivos, existen transacciones de datos sensibles que se intercambian solo a través de rutas con los debidos controles para proporcionar autenticidad.

DS11 Administrar los datos

Se deben establecer procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos así como para la eliminación apropiada de ellos, para garantizar la disponibilidad, calidad, oportunidad de contar con la información requerida.

Las Entidad Emisora de Tarjetas de Crédito debe realizar respaldos periódicos y probar la funcionalidad de los mismos mediante reanudaciones, este proceso será repetitivo entre el Site Principal y el Alterno a quien continuamente se le realizarán restauraciones de BDD de la información previamente respaldada.

Es necesario validar que todos los datos que se espera procesar han cumplido su flujo y se han procesado por completo.

Entre la información que debe respaldarse en las Entidades se menciona: análisis de crédito, información de establecimientos, información de tarjetas, caja, legal, información para servicio al cliente, procesos batch, procesos de ajuste, liquidaciones, inversiones, logística, conciliaciones, activos, huellas, firmas, información SMS, información de Call Center entre otras.

DS11.1 Requerimientos del negocio para la administración de datos, validar que los datos que se reciben en la Entidad de Emisión de Tarjetas de Crédito se reciben y procesan completa y correctamente.

DS11.2 Acuerdos de almacenamiento y conservación, procedimientos para archivo, almacenamiento y retención de datos.

DS11.3 Sistema de administración de librerías y medios, procedimiento para garantizar que los medios almacenados tengan usabilidad el momento en que sean requeridos.

DS11.4 Eliminación, protección de datos sensitivos el momento en que se lleva a cabo la eliminación.

DS11.5 Respaldo y restauración, con una periodicidad definida se debe respaldar las aplicaciones, la información, la configuración, etc. del Site principal, para que puedan ser restauradas en el Site Alterno.

DS11.6 Requerimientos de seguridad para la administración de datos, procedimientos para recepción, procesamiento, almacén y salida de datos.

DS12 Administrar el ambiente físico

Tanto el Site Principal como el Alterno deben contar con instalaciones bien diseñadas y correctamente administradas con una protección adecuada de equipos así como del personal que acude a ellos.

La selección de instalaciones apropiadas incluye factores ambientales, distribución,

Control de acceso, iluminación, extinguidores, contingencia contra inundaciones, etc.; para lo cual se debe contar con un asesoramiento técnico y controles periódicos para validar que las medidas de seguridad están disponibles.

Además se debería contar con dispositivos y equipo especializado para monitorear y controlar el ambiente. Procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas para personal interno y externo.

DS12.1 Selección y diseño del centro de datos, diseñar y definir centros de datos para el Site Alterno, considerando el riesgo asociado a los desastres.

DS12.2 Medidas de seguridad física, se deben definir zonas de seguridad, habitaciones con ventilación, ubicación de equipo crítico, monitoreo y resolución de incidentes presentados en este lugar.

DS12.3 Acceso físico, procedimientos para autorizar, limitar, revocar el acceso a locales, edificios y áreas de acuerdo a las necesidades del negocio.

DS12.4 Protección contra factores ambientales, es importante disponer de procedimientos o controles que impidan que factores ambientales pongan en peligro la infraestructura, el sitio en el que se encuentra el Site Alterno.

DS12.5 Administración de instalaciones físicas,

3.2.4.4 Monitorear y Evaluar[52]

Dominio Monitorear y Evaluar (ME), monitorear todos los procesos para asegurar que se sigue la dirección provista.

Todos los procesos que se cumplen para mantener el Site Alterno funcionando como se debe, necesitan ser monitoreados continuamente para validar suficiencia y calidad del servicio, se designará personal dedicado a estas funciones.

En este proceso se advierte sobre la necesidad de asegurar procesos de control independientes los que son provistos de auditorías internas y externas.

A través de este dominio es posible medir el desempeño del Site de TI para detectar los problemas antes de que sea demasiado tarde, incluso identificar el momento óptimo en el que se debe realizar el cambio del Site Principal al Alterno, se puede identificar si la gerencia garantiza que los controles internos son efectivos y eficientes para el correcto funcionamiento del Site, si puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio, si se miden y se reportan los riesgos, el control, el cumplimiento y el desempeño.

[52] COBIT 4.1-2007. IT Governance Institute

ME3 Garantizar el cumplimiento regulatorio

Es necesario establecer procesos, políticas, estándares, procedimientos de revisiones, metodologías, para garantizar el cumplimiento de leyes, regulaciones y requerimientos contractuales.

En el cumplimiento de normativas ejerce un papel muy importante el Site Alterno mismo que entrará en funcionamiento una vez que se pueda identificar en el Site Principal no está dentro de los parámetros permitidos, para ellos deberían generarse alarmas de diferentes colores que permitan alertar y contar con procedimientos en cada caso, se debe considerar que las penalidades en caso de incumplimiento podrían ser desde sanciones laborales, sanciones empresariales, sanciones a proveedores y en casos extremos sanciones penales, por lo que se debe contar con el asesoramiento legal necesario.

ME3.1 Identificar los requerimientos de las leyes, regulaciones, cumplimientos contractuales, uno de los justificativos por el cual el Site Alterno existe es para evitar incurrir en multas o sanciones debidos a incumplimientos.

ME3.2 Optimizar la respuesta a requerimientos externos, constantemente es importante se optimice la atención a peticiones solicitadas.

ME3.3 Evaluación del cumplimiento con requerimientos externos, confirmar el cumplimiento de políticas, estándares y procedimientos.

ME3.4 Aseguramiento positivo del cumplimiento, definir e implementar procedimientos para obtener, confirmaciones que se ha llevado a cabo acciones correctivas para resolver brechas de cumplimiento

ME3.5 Reportes integrados, se requiere disponer de reportes sobre requerimientos legales y contractuales.

3.3 MATRIZ DE GESTIÓN DEL SITE ALTERNO

Para el desarrollo de la matriz se ha considerado varios aspectos:

3.3.1 MADUREZ DE LOS PROCESOS DE TI

Los modelos de madurez varían del 0 al 5, según se describe a continuación:

0 No Existente, no se aplican procesos administrativos en lo absoluto

1 Inicial / Ad hoc, los procesos son ad-hoc y desorganizados

2 Repetible pero Intuitivo, los procesos siguen un patrón regular

3 Proceso Definido, los procesos se documentan y se comunican

4 Administrado y Medible, los procesos se monitorean y se miden

5 Optimizado, las buenas prácticas se siguen y se automatizan

3.3.2 FACILITADORES

Se disponen de dos facilitadores:

P Facilitador Primario, es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

S Facilitador Secundario, es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

Blanco (vacío), podría aplicarse, sin embargo los requerimientos son satisfechos más apropiadamente por otro criterio.

Se considera el facilitador que tiene cada uno de los requerimientos de del negocio[53].

3.3.3 MATRIZ RACI

Una matriz RACI identifica:

R, quien es responsable

A, quien debe rendir cuentas

C, quien debe ser consultado

I, quien debe ser Informado

Las funciones pueden ser asignadas a:

CEO, Director Ejecutivo

CFO, Director Financiero

Ejecutivo del Negocio

CIO, Director de Información, algunas veces Director de Tecnología.

Dueño del Proceso del Negocio

Jefe de Operaciones

Arquitecto en Jefe

Jefe de Desarrollo

Jefe de Administración de TI

PMO, Director de administración de proyectos

Cumplimiento, Auditoría, Riesgo y Seguridad

Equipo de Despliegue

[53] COBIT Conjunto de Herramientas de Implementación 3ª Edición, Gobernance, pág. 19.

Departamento de entrenamiento

Administrador del Servicio

Consejo de Directores

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Relacionar las metas del negocio con las de TI	C	I	A/R	R	C						
Identificar dependencias críticas y desempeño actual	C	C	R	A/R	C	C	C	C	C		C
Construir un plan estratégico para TI	A	C	C	R	I	C	C	C	C	I	C
Construir planes tácticos para TI	C	I		A	C	C	C	C	C	R	I
Analizar portafolios de programas y administrar portafolios de servicios y proyectos	C	I	I	A	R	R	C	R	C	C	I

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

Figura 3 1 Matriz RACI

Fuente: http://auditoriadesistemasunah.blogspot.com/2012/02/cobit-41-objetivos-de-control-para-la.html

3.3.4 TIPOS DE MÉTRICAS

Existen dos tipos de métricas:

Medidas de resultados, indican cuando las metas se han conseguido

Indicadores de desempeño, indican si es probable conseguir la meta.

3.3.5 MATRIZ MAPEADA CON ISO, NIST E ITIL A CADA PROCESO DE COBIT SELECCIONADO

A continuación se va a mostrar el mapeo respectivo de cada proceso de Cobit con NIST. ISO e ITIL, basado en los siguientes documentos:

- COBIT 4.1-2007 IT Governance Institute.
- Mapping of NIST SP800-53 Rev 1 With COBIT 4.1, 2007 IT Governance Institute
- Mapping of ITIL v3 With COBIT 4.1, 2008 IT Governance Institute
- Mapping of ISO/IEC 17799: with COBIT 4.0, publicado por Governance Institute
- ISO/IEC 27002:2005 Publicado por ISO y por IEC, derivado de la norma BS 7799 del gobierno británico, renombrada ISO/IEC 17799:2005, para proporcionar un marco de referencia del estándar para gestión de seguridad de información.
- Alineando COBIT 4.1, ITIL V3 4.1, ITIL v3 e ISO/IEC 27002 en beneficio del Negocio, Reporte del ITGI y la OGC.
- ALVAREZ ÁLVAREZ GUSTAVO ALEXANDER, Universidad Nacional de Trujillo; NIST SP800-53 REV. 3 con COBIT 4.1, 2010.

A continuación se muestran las matrices correspondientes a los 11 procesos de COBIT con su respectivo mapeo:

- ✓ PO9, Evaluar y Administrar los riesgos de TI – Tabla 3.1
- ✓ AI3, Adquirir y mantener una Infraestructura Tecnológica – Tabla 3.2
- ✓ AI6, Administrar cambios – Tabla 3.3

- ✓ DS1, Definir y administrar los niveles de servicio – Tabla 3.4
- ✓ DS2, Administrar los servicios de terceros – Tabla 3.5
- ✓ DS3, Administrar el desempeño y la capacidad – Tabla 3.6
- ✓ DS4, Garantizar la continuidad del servicio – Tabla 3.7
- ✓ DS5, Garantizar la seguridad de los sistemas – Tabla 3.8
- ✓ DS11, Administración de datos – Tabla 3.9
- ✓ DS12, Administración del ambiente físico – Tabla 3.10
- ✓ ME3, Garantizar el cumplimiento con requerimientos externos – Tabla 3.11

PO9 Evaluar y administrar los riesgos de TI.- Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se den adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los interesados y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia		
MARCO	**No.**	**PREGUNTAS**
COBIT	PO 9.1	Marco de Trabajo de Administración de riesgos. Área clave: Alineamiento al marco de riesgo empresarial. Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización
ITIL	SD 9.5	Riesgos
	SD 4.5.5.1	Inicio
ISO/IEC	14.1.1	Incluir la seguridad de información en el proceso de gestión de continuidad del negocio.
	14.1.2	Continuidad del negocio y evaluación de riesgos.
NIST	RA-1	Evaluación de riesgos políticas y procedimientos.
COBIT	PO 9.2	Establecimiento del contexto del riesgo. Área clave: Contexto interno y externo; metas de cada evaluación Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.
ITIL	SS 9.5	Riesgos
	SD 4.5.5.1	Inicio
	SD 4.5.5.2	Requisitos y estrategia
ISO/IEC	14.1.1	Incluir la seguridad de información en el proceso de gestión de continuidad del negocio.
	14.1.2	Continuidad del negocio y evaluación de riesgos.
NIST	RA-1	Evaluación de riesgos. Seguridad de la categorización.

COBIT	PO 9.3	Identificación de eventos. Área clave: Amenazas importantes que exploten vulnerabilidades tienen impacto negativo en el negocio. Registro de riesgos. Identificar eventos(una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.
ITIL	SS 9.5	Riesgos
	SD 4.5.5.2	Requisitos y estrategia
	ST 9	Desafíos, factores críticos de éxito y riesgos
	CSI 5.6.3	Gestión de continuidad de servicios de TI
ISO/IEC	13.1.1	Reporte de eventos de seguridad de información
	13.1.2	Reporte de debilidades de seguridad
NIST	RA-3	Evaluación de riesgos
	RA-5	Evaluación de riesgos . Escaneo de vulnerabilidad
COBIT	PO 9.4	Evaluación de riesgos de TI. Área clave: Probabilidad e impacto de todos los riesgos identificados. Evaluación cuantitativa y cualitativa. Riesgos residual e inherente. Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riegos inherentes y residuales se debe determinar de forma individual, por categoría y con base de portafolio.
ITIL	SS 9.5	Riesgos
	SD 4.5.5.2	Requisitos y estrategia
	SD 8.1	Análisis de impacto en el negocio
	ST 4.6	Evaluación
ISO/IEC	5.1.2	Revisión de la política de seguridad de la información
	14.1.2	Continuidad del negocio y evaluación de riesgos.
NIST	RA-3	Evaluación de riesgos
	RA-4	Actualización de Evaluación de riesgos .
COBIT	PO 9.5	Respuesta a los riesgos. Área Clave: Controles económicamente efectivos que mitiguen la exposición, Estrategias de gestión del riesgo en términos de evitar, mitigar o aceptar.

		Desarrollar y mantener un proceso de respuesta a los riesgos diseñado para asegurar controles efectivos en costo mitigan la exposición en forma continua. El proceso e respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia de los riesgos.
ITIL	SS 9.5	Riesgos
	SD 4.5.5.3	Implementación
	ST 4.6	Evaluación
NIST	IR-1	Respuesta a incidentes, políticas y procedimientos.
	IR-4	Respuesta a incidentes. Manejo de incidentes
COBIT	PO 9.6	Mantenimiento y monitoreo de un plan de acción de riesgos. Área Clave: Priorización y planeamiento de las respuestas al riesgo. Costos beneficios y responsabilidades. Monitoreo de desviaciones. Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.
ITIL	SS 9.5	Riesgos
	SD 4.5.5.4	Etapa 4- Operación continua
NIST	IR-1	Respuesta a incidentes, políticas y procedimientos.
	IR-4	Respuesta a incidentes. Manejo de incidentes

Tabla 3. 1 PO9 Evaluar y Administrar los Riesgos de TI

AI3 Adquirir y mantener una infraestructura tecnológica.- Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo a las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continua para las aplicaciones del negocio.		
MARCO	**No.**	**PREGUNTAS**
COBIT	AI 3.1	Plan de Adquisición de Infraestructura y Tecnología. Áreas clave: Plan de Adquisición, implementación y mantenimiento para la infraestructura, en línea con las necesidades del negocio y la dirección tecnológica. Generar un plan para adquirir, implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de la capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica.
ITIL	SD 3.6.3	Diseño de la arquitectura tecnológica
COBIT	AI 3.2	Protección y disponibilidad de la infraestructura. Área clave: Protección de recursos utilizando mediciones de seguridad y auditabilidad. Uso de infraestructura sensitiva. Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollar e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso
ITIL	SD 4.6.5.1	A
	SO 5,4	Gestión y soporte de servidores
ISO/IEC	12.1.1	Análisis y especificación de los requisitos de seguridad
COBIT	AI 3.3	Mantenimiento de la infraestructura. Área clave: Control de cambios, gestión de parches, estrategias de actualización y requerimientos de seguridad
ITIL	SO 5.4	Gestión y soporte de servidores
	SO 5.5	Gestión de redes
	SO 5.7	Administración de bases de datos
	SO 5.8	Gestión de servicios de directorio
	SO 5.9	Soporte de estaciones de trabajo
	SO 5.10	Gestión de middleware
	SO 5.11	Gestión Internet / web

ISO/IEC	9.1.5	Trabajo en áreas seguras
	9.2.4	Mantenimiento de equipos
	12.4.2	Protección de los datos de prueba del sistema
	12.5.2	Revisión técnica de las aplicaciones luego de cambios en el sistema operativo
	12.6.1	Control de vulnerabilidades técnicas
COBIT	AI 3.4	Ambiente de prueba de factibilidad. Área clave: Entornos de desarrollo y pruebas; pruebas de factibilidad e integración.
ITIL	ST 4.4.5.1	Planificación
	ST 4.4.5.2	Preparación para la construcción, pruebas y despliegue
	ST 4.4.5.3	Construcción y pruebas
	ST 4.5.5.7	Limpieza y cierre de las pruebas
	ST 4.5.7	Gestión de información
ISO/IEC	10.1.4	Separación de los entornos de desarrollo, pruebas y producción.

Tabla 3. 2 AI3 Adquirir y Mantener una Infraestructura Tecnológica

AI6 Administrar cambios.- Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionado con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.		
MARCO	**No.**	**PREGUNTAS**
COBIT	AI 6.1	Estándares y procedimientos para cambios. Áreas clave:
ITIL	ST 4.2.6.1	Procedimiento de cambio normal
	ST 5	Actividades comunes de operación en la transición del servicio
	ST 6	Organización para la transición del servicio
	ST 6.3	Modelos organizacionales para apoyar la transición de servicios
	ST 6.4	Relación de la transición del servicio con otras etapas del ciclo de vida
	SO 4.6.1	Gestión de cambios (actividades operativas)
NIST	CM-1	Gestión de configuración, políticas y procedimientos
	CM-3	Gestión de configuración, control de gestión de cambios
COBIT	AI 6.2	Evaluación de impacto, priorización y autorización. Área clave: Evaluar impacto, categorizar, priorizar y autorizar.
ITIL	ST 4.2.6.2	Crear y registrar la solicitud de cambio
	ST 4.2.6.3	Revisar la solicitud de cambio
	ST 4.2.6.4	Valorar y evaluar el cambio
	ST 4.2.6.5	Autorizar el cambio
	ST 4.2.6.6	Coordinar la implementación del cambio
	ST 4.2.6.8	Consejo consultivo de cambios
	ST 4.6	Evaluación
	SO 4.3.5.1	Selección por menú
	SO 4.3.5.2	Aprobación financiera
	SO 4.3.5.3	Otras aprobaciones
ISO/IEC	10.1.2	Gestión de cambios
	12.5.1	Procedimientos de control de cambios
	12.5.3	Restricciones en los cambios a los paquetes de software
	12.6.1	Control de vulnerabilidades técnicas
COBIT	AI 6.3	Cambios de emergencia. Área clave: Proceso para definir, escalar, probar, documentar, evaluar y autorizar cambios de emergencia.
ITIL	ST 4.2.6.9	Cambios de emergencia.
ISO/IEC	10.1.2	Gestión de cambios
	11.5.4	Uso de utilitarios del sistema
	12.5.1	Procedimiento de control de cambios
	12.5.3	Restricciones en los cambios a los paquetes de software
	12.6.1	Control de vulnerabilidades técnicas

	CM-3	Gestión de configuración, control de gestión de cambios
COBIT	AI 6.4	Seguimiento y reporte de estado de los cambios . Área clave: Seguimiento y reporte de todos los cambios (rechazados, aprobados, en curso y concluidos)
ITIL	ST 3.2.13	Asegurar la calidad de un servicio nuevo o modificado
	ST 3.2.14	Mejora proactiva de la calidad durante la transición del servicio
	ST 4.1.5.3	Planificar y coordinar la transición del servicio
	ST 4.1.6	Brindar soporte al proceso de transición
ISO/IEC	10.1.2	Gestión de cambios
COBIT	AI 6.5	Cierre y documentación del cambio. Área clave: Implementación de cambios y actualización de la documentación.
ITIL	ST 4.2.6.4	Valorar y evaluar el cambio
	ST 4.2.6.7	Revisar y cerrar el registro del cambio
	ST 4.4.5.10	Revisar y cerrar la transición del servicio
	ST 4.4.5.9	Revisar y cerrar un despliegue
	SO 4.3.5.5	Cierre
ISO/IEC	10.1.2	Gestión de cambios

Tabla 3. 3 AI6 Administrar Cambios

DS1.- Definir y administrar los niveles de servicio.- Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.

MARCO	No.	PREGUNTAS
COBIT	DS 1.1	Marco de trabajo de la Administración de los niveles de servicio. Áreas clave: Proceso formal de gestión de niveles de servicio y alineación continua con los requerimientos del negocio. Facilitar el entendimiento común entre el cliente y el proveedor
ITIL	SS 2.6	Funciones y procesos a través del ciclo de vida
	SS 4.3	Desarrollar activos estratégicos
	SS 4.4	Preparar la ejecución
	SS 7.2	Estrategia y diseño
	SS 7.3	SS 4.2
	SS 7.5	Estrategia y mejora
	SD 4.2.5.1	Diseñar marcos ANS
	SD 4.2.5.9	Desarrollar contratos y relaciones
O/I E C	10.2.1	Entrega de Servicios
COBIT	DS 1.2	Definición de servicios. Áreas claves: Servicios definidos baseado en las características del servicio y los requerimientos del negocio en un catálogo de servicios
ITIL	SS 4.2	Desarrollar las ofertas
	SS 4.3	Desarrollar activos estratégicos
	SS 5.4	Métodos de gestión del portafolio de servicios
	SS 5.5	Gestión de la demanda
	SS 7.2	Estrategia y diseño
	SS 7.3	Estrategia y transiciones
	SS 7.4	Estrategia y operaciones
	SS 7.5	Estrategia y mejora
	SS 8.2	Interfaces de servicio
	SD 3	Principios de diseño de servicio
	SD 3.1	Metas
	SD 3.2	Diseño Balanceado
	SD 3.4	Identificar y documentar los requisitos y drivers del negocio
	SD 3.5	Actividades de diseño
	SD 3.6	Aspectos de diseño
	SD 4.1	Gestión del catálogo del servicio
O/I E C	10.2.1	Entrega de servicios

COBIT	DS 1.3	Acuerdos de niveles de servicio (ANS). Áreas clave: Definir los ANS basándose en los requerimientos del cliente y las capacidades de TI. Métricas, roles y responsabilidades de los servicios
ITIL	SD 4.2.5.2	Requisitos acordados y documentados de los nuevos servicios; definir los requisitos de los niveles de servicio
ITIL	SD APENDICE F	Ejemplos de ANS y acuerdos de niveles de operación
ISO/IEC	10.2.1	Entrega de servicios
COBIT	DS 1.4	Acuerdos de niveles de operación: Áreas clave: Definición de entrega técnica para soportar los ANS
ITIL	SD 4.2.5.5	Examinar y revisar los acuerdos suscritos y el alcance del servicio
ITIL	SD APENDICE F	Ejemplos de ANS y acuerdos de niveles de operación
COBIT	DS 1.5	Monitoreo y reporte del cumplimiento de los niveles de servicio. Área clave: Monitoreo continuo del desempeño del servicio
ITIL	SS 5.3	Gestión del portafolio de servicios
ITIL	SD 4.2.5.3	Monitorear el desempeño del servicio contra el ANS
ITIL	SD 4.2.5.6	Generar reportes del servicio
ITIL	SD 4.2.5.7	Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio
ITIL	SD 4.2.5.10	Reclamos y reconocimientos
ITIL	SD 4.3.8	Gestión de la información
ITIL	CSI 4.2	Reportes del servicio
ITIL	CSI 4.3	Mediciones del servicio
ISO/IEC	10.2.2	Monitoreo y revisión de los servicios de terceros
ISO/IEC	10.2.3	Gestión de cambios a los servicios de terceros
COBIT	DS 1.6	Revisión de los acuerdos de niveles de servicio y de los contratos. Áreas clave: Revisión periódica de los ANS y mejorar los contratos para mayor efectividad y vigencia
ITIL	SD 4.2.5.4	Comparar medir y mejorar la satisfacción del cliente
ITIL	SD 4.2.5.5	Examinar y revisar dos acuerdos suscritos y el alcance del servicio
ITIL	SD 4.2.5.8	Examinar y revisar los ANS, alcance del servicio y los acuerdos del servicio
NIST	SA-9	Sistemas y Servicios de Adquisición - Información externa de Sistemas y Servicios

Tabla 3. 4 DS 1 Definir y Administrar los Niveles de Servicio

DS2.- Administrar los servicios de terceros.- La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere que un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

MARCO	No.	PREGUNTAS
COBIT	DS 2.1	Identificación de todas las relaciones con proveedores. Áreas clave: Categorizar los servicios según el tipo de proveedor, significacia y criticidad
ITIL	SS 7.3	Estrategia y transiciones
	SD 4.7.5.1	Evaluación de nuevos proveedores y contratos
O/IEC	6.2.1	Identificación de riesgos relacionados con terceros
COBIT	DS 2.2	Gestión de relaciones con proveedores. Áreas clave: Enlace respecto a temas del cliente y el proveedor. Confianza y transparencia
ITIL	SD 4.2.5.9	Desarrollar contratos y relaciones
	SD 4.7.5.2	Clasificación de proveedores y mantenimiento de la BDD de proveedores y contratos
	SD 4.7.5.4	Gestión y desempeño de proveedores y contratos
	SD 4.7.5.5	Renovación y /o términos de contratos
ISO/IEC	6.2.3	Considerar la seguridad en los acuerdos con terceros
	10.2.3	Gestión de cambios a los servicios de terceros
	15.1.4	Protección de datos y privacidad de la información personal
NIST	PS-7	Seguridad del personal de proveedores
COBIT	DS 2.3	Administración de riesgos del proveedor. Áreas clave: Identificación de riesgo, conformidad contractual y viabilidad de proveedores
ITIL	SD 4.7.5.3	Nuevos proveedores y contratos
	SD 4.7.5.5	Renovación y /o términos de contrato
ISO/IEC	6.2.1	Identificación de riesgos relacionados con terceros
	6.2.3	Considerar la seguridad en los acuerdos con terceros
	8.1.2	Verificación
	8.1.3	Términos y condiciones del empleo
	10.2.3	Gestión de cambios a los servicios de terceros
	10.8.2	Acuerdos de intercambio
NIST	SA-9	Sistemas y Servicios de Adquisición. Sistemas y Servicios para información externa

COBIT	DS 2.4	Monitoreo del desempeño del proveedor. Área clave: Satisfacer los requerimientos del negocio, adhesión a los contratos y desempeño competitivo
ITIL	SD 4.7.5.4	Gestión y desempeño de proveedores y contratos
ISO/IEC	6.2.3	Considerar la seguridad en los acuerdos con terceros
	10.2.1	Entrega de servicios
	10.2.2	Monitoreo y revisión de los servicios de terceros
	12.4.2	Protección de los datos de prueba del sistema
	12.5.5	Outsoursing de desarrollo de software

Tabla 3. 5 DS 2 Administrar los Servicios de Terceros

DS3.- Administrar el desempeño y la capacidad.- La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.		
MARCO	**No.**	**PREGUNTAS**
COBIT	DS 3.1	Planeación del desempeño y la capacidad. Áreas clave: Asegurar que las capacidades y los desempeños cumplen con los ANS
ITIL	SD 4.3.5.1	Gestión de la capacidad para el negocio
	SD APÉNDICE J	Contenido típico de un plan de capacidad
	CSI 5.6.2	Gestión de la capacidad
	10.3.1	Gestión de la capacidad
COBIT	DS 3.2	Capacidad y desempeño actual. Área clave: Evaluación de los desempeños y capacidades actuales
ITIL	SD 4.3.5.2	Gestión de la capacidad del servicio
	SD 4.3.5.3	Gestión de la capacidad de los componentes
	SO 4.1.5.2	Notificación de eventos
	SO 4.1.5.3	Detección de eventos
	SO 5.4	Gestión de soporte de servidores
	CSI 4.3	Mediciones del servicio
O/I E C	10.3.1	Gestión de la capacidad
COBIT	DS 3.3	Capacidad y desempeño futuros. Áreas claves: Pronóstico de requerimiento de recursos. Transferencia de las cargas de trabajo
ITIL	SD 4.3.5.1	Gestión de la capacidad para el negocio
	SD 4.3.5.2	Gestión de la capacidad del servicio
	SD 4.3.5.3	Gestión de la capacidad de los componentes
	SD 4.3.5.7	Modelamiento y tendencias
	SD 4.3.8	Gestión de la información
O/I E C	10.3.1	Gestión de la capacidad
COBIT	DS 3.4	Disponibilidad de recursos de TI. Áreas clave: Provisión de recursos, contingencias, tolerancia y fallas de priorización de recursos
ITIL	SD 4.3.5.3	Gestión de la capacidad de los componentes
	SD 4.3.5.4	Actividades de soporte de la gestión de capacidad
	SD 4.4	Gestión de la disponibilidad
	SD 4.4.5.1	Actividades reactivas de la gestión de la disponibilidad
	SD 4.4.5.2	Actividades proactivas de la gestión de la disponibilidad
	SO 4.6.5	Gestión de la disponibilidad (actividades operativas)
	CSI 5.6.1	Gestión de la disponibilidad

COBIT	DS 3.5	Monitoreo y reporte. Áreas clave: Mantenimiento y afinamiento de performance y capacidad, reporte de la disponibilidad de servicio al negocio
ITIL	SD 4.3.5.4	Actividades de soporte de la gestión de la capacidad
	SD 4.3.5.5	Gestión y control de umbrales
	SD 4.3.5.6	Gestión de la demanda
	SD 4.4.5.1	Actividades reactivas de la gestión de la disponibilidad

Tabla 3. 6 DS 3 Administrar el Desempeño y la Capacidad

DS4.-Garantizar la continuidad del Servicio.- La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimizar la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.		
MARCO	**No.**	**PREGUNTAS**
COBIT	DS 4.1	Marco de Trabajo de continuidad de TI. Área Clave: Enfoque consistente y corporativo a la gestion de continuidad
ITIL	SD 4.5	Gestión de la continuidad de Servicios de TI
	SD 4.5.5.1	Inicio etapa1
	CSI 5.6.3	Gestión de continuidad de servicios de TI
ISO/IEC	6.1.6	Relación con las autoridades
	6.1.7	Relación con grupos de interés especial
	14.1.1	Incluir la seguridad de información en el proceso de gestión de continuidad del negocio
	14.1.2	Continuidad del negocio y evaluación de riesgos
	14.1.4	Marco de planificación de continuidad del negocio
NIST	CP-1	Plan de contingencia políticas y procedimientos
	CP-6	Plan de contingencia, Sites de almacenamiento
	CP-7	plan de contingencia, sitios de procesamiento
	CP-8	plan de contingencia, servicios de telecomunicaciones
COBIT	DS 4.2	Planes de continuidad de TI. Áreas Clave: Planes individuales de continuidad, análisis de impacto del negocio, resiliencia, procesamiento alternativo y recuperación
ITIL	SD 4.5.5.2	Requisitos y estrategia
	SD 4.5.5.3	Implementación
	SD	Contenido típico de un plan de recuperación
ISO/IEC	6.1.6	Relación con las autoridades
	6.1.7	Relación con grupos de interés especial
	14.1.3	Desarrollar e implementar planes de continuidad que incluyan la seguridad de la información
NIST	CP-2	Plan de contingencia para los sistemas de información
	CP-4	Pruebas del plan de contingencia
	CP-9	Plan de contingencia de los backup de los sistemas de información
COBIT	DS 4.3	Recursos críticos de TI. Áreas clave: centrarse en la infraestructura crítica, resiliencia y priorización, repuesta para diferentes períodos de tiempo
ITIL	SD 4.4.5.2	Actividades proactivas de la gestión de la disponibilidad
	SD 4.5.5.4	Operación continua

ISO/IEC	14.1.1	Incluir la seguridad de información en el proceso de gestión de continuidad del negocio
	14.1.2	Continuidad del negocio y evaluación de riesgos
COBIT	DS 4,4	Mantenimiento del plan de continuidad de TI. Área clave: control de cambios para reflejar los requerimientos cambiantes del negocio
ITIL	SD 4.5.5.4	Operación continua
ISO/IEC	14.1.5	Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
NIST	CP-5	Actualización del plan de contingencia
COBIT	DS 4.5	Pruebas del plan de continuidad. Áreas clave: Pruebas regulares, implementación del plan de acción
CITIL	SD 4.5.5.3	Implementación
	SD 4.5.5.4	Operación continua
ISO/IEC	14.1.5	Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
NIST	CP-4	Pruebas del plan de contingencia
COBIT	DS 4.6	Entrenamiento del plan de continuidad. Área clave: Entrenamiento regular para todas las partes involucradas
CITIL	SD 4.5.5.3	Implementación
	SD 4.5.5.4	Operación continua
ISO/IEC	14.1.5	Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
NIST	CP-3	Entrenamiento de contingencia
COBIT	DS 4.7	Distribución del plan Continuidad de TI. Área clave: Distribución segura y adecuada a todas las partes autorizadas
CITIL	SD 4.5.5.3	Implementación
	SD 4.5.5.4	Operación continua
ISO/IEC	14.1.5	Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
COBIT	DS 4.8	Recuperación y reanudación del Servicio de TI. Áreas clave: Planificación del periodo cuando TI se esté recuperando y reanudando servicios. Entendimiento del negocio y soporte a la inversión
ITIL	SD 4.5.5.2	Actividades proactivas de la gestión de la disponibilidad
	SD 4.5.5.4	Operación continua
ISO/IEC	14.1.1	Incluir la seguridad de información en el proceso de gestión de continuidad del negocio
	14.1.3	Mantener o restaurar operaciones para asegurar la disponibilidad de la información

NIST	CP-7	Plan de continuidad de procesos de Site alternos
	CP-10	Plan de continuidad de recuperación y reconstitución de sistemas de información
COBIT	DS 4.9	Almacenamiento y respaldo fuera de las instalaciones
CITIL	SD 4.5.5.2	Requisitos y estrategia
	SO 5.2.3	Respaldo y restauración
ISO/IE	10.5.1	Respaldo de la información
NIST	CP-6	Plan de contingencia, Sites de almacenamiento
	CP-9	Plan de contingencia de los backup de los sistemas de información
COBIT	DS 4.10	Revisión Post Reanudación. Áreas clave: Evaluación regular de los planes
CITIL	SD 4.5.5.3	Implementación
	SD 4.5.5.4	Operación continua
ISO/IE	14.1.5	Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio

Tabla 3. 7 DS 4 Garantizar la Continuidad del Servicio

DS5- Garantizar la seguridad de los sistemas.- La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.		
MARCO	**No.**	**PREGUNTAS**
COBIT	DS 5.1	Administración de la seguridad de TI Áreas clave: Ubicar la gestión de seguridad a la alto nivel para cumplir las necesidades del negocio
ITIL	SD 4.6	Gestión de la seguridad de la información.
	SO 5.13	Gestión de seguridad de la información y la operación del servicio
ISO/IEC	6.1.1	Compromiso de la gerencia con la seguridad de la información
	6.1.2	Coordinación para la seguridad de la información
	6.2.3	Considerar la seguridad en los acuerdos de terceros
	6.2.2	Educación, entrenamiento y concientización en seguridad de información
COBIT	DS 5.2	Plan de seguridad de TI. Áreas de seguridad: Traducción de requerimientos de negocio, riesgo y cumplimiento en un plan de seguridad
ITIL	SD 4.6.4	Políticas, principios y conceptos básicos
	SD 4.6.5.1	Controles de seguridad (cobertura a alto nivel, sin detalle)
ISO/IEC	5.1.1	Documento de la política de seguridad de la información
	5.1.2	Revisión de la política de seguridad de la información
	6.1.2	Coordinación para la seguridad de la información
	6.1.5	Acuerdos de confidencialidad
	8.2.2	Educación, entrenamiento y concientización en seguridad de información
	11.1.1	Políticas de control de acceso
	11.7.1	Computación móvil y las comunicaciones
	11.7.2	Teletrabajo

NIST	PL-1	Planeación de políticas de seguridad y procedimientos
	PL-2	Planeación del plan de seguridad del sistema
	PL-4	Planeación para reglas del manejo de la información para usuarios
	SC-1	Políticas y procedimientos de protección de sistemas y comunicación
COBIT	DS 5.3	Administración de identidad. Área clave: Identificación de todos los usuarios (internos, externos y temporales) y su actividad
ITIL	SO 4.5	Gestión de acceso
ISO/IEC	5.1.1	Documento de la política de seguridad de la información
	5.1.2	Revisión de la política de seguridad de la información
	6.1.2	Coordinación para la seguridad de la información
	6.1.5	Acuerdos de confidencialidad
	8.2.2	Educación, entrenamiento y concientización en seguridad de información
	11.1.1	Políticas de control de acceso
	11.7.1	Computación móvil y las comunicaciones
	11.7.2	Teletrabajo
NIST	IA-1	Políticas y procedimientos de Identificación y autentificación
	IA-2	Identificación y autentificación de usuarios
	IA-4	Gestión de Identificación
COBIT	DS 5.4	Administración de cuentas de usuario. Área clave: Gestión del ciclo de vida de las cuentas de usuario y privilegios de acceso
ITIL	SO 4.5	Gestión de acceso
	SO 4.5.5.1	Peticiones de accesos
	SO 4.5.5.2	Verificación
	SO 4.5.5.3	Habilitar privilegios
	SO 4.5.5.4	Monitorear el estado de la identidad
	SO 4.5.5.5	Registro y seguimiento de accesos
	SO 4.5.5.6	Eliminar o restringir privilegios
ISO/IEC	6.1.5	Acuerdos de confidencialidad
	6.2.1	Identificación de riesgos relacionados con terceros
	6.2.2	Considerar la seguridad al tratar con los clientes
	8.1.1	Roles y responsabilidades
	8.3.1	Responsabilidades del cese
	8.3.3	Eliminación de privilegios de acceso
	10.1.3	Segregación de funciones
	11.1.1	Políticas de control de acceso
	11.2.1	Registro de usuarios

	11.2.2	Gestión de privilegios
	11.2.4	Revisión de derechos de acceso a usuarios
	11.3.1	Uso de contraseñas
	11.5.1	Procedimientos de seguros de inicio de sesión
	11.5.3	Sistema de gestión de contraseñas
	11.6.1	Restricción de accesos a la información
NIST	AC-2	Control de Acceso. Gestión de Cuentas
	IA-4	Identificación y autentificación de gestión de identificador
	PS-6	Seguridad del personal. Niveles de Acceso
COBIT	DS 5.5	Pruebas, vigilancia y monitoreo de la seguridad. Áreas clave: Pruebas proactivas de la implementación de seguridad. Acreditación oportuna. Reporte oportuno de eventos inusuales
ITIL	SO 4.5.5.6	Eliminar y restringir privilegios
	SO 5.13	Gestión de seguridad de la información y la operación del servicio
ISO/IEC	6.1.8	Revisión independiente de la seguridad de la información
	10.10.2	Monitoreo del uso del sistema
	10.10.3	Protección de logs
	10.10.4	Logs de administrador y de operador
	12.6.1	Control de vulnerabilidad técnicas
	13.1.2	Reporte de debilidades de seguridad
	15.2.2	Verificación de cumplimiento técnico
	15.3.1	Controles de auditoría de sistemas de información
NIST	AU-6	Auditoría y rendición de costos. Análisis reporte y monitoreo de auditoría
	CA-2	Evaluación de la seguridad y autorización. Evaluación de la seguridad
	CA-6	Evaluación de la seguridad y autorización. Acreditación de seguridad
	CA-7	Evaluación de la seguridad y autorización. Monitoreo continuo
	CM-4	Gestión de la configuración. Monitorear la configuración de cambios
	RA-5	Evaluación de Riesgos. Escaneo de la vulnerabilidad
	SI-4	Integridad del sistema y la información. Técnicas y herramientas para monitorear los sistemas de información

COBIT	DS 5.6	Definición de incidente de seguridad. Áreas clave: Definición y clasificación de las características de los incidentes de seguridad.
ITIL	SD 4.6.5.1	Controles de seguridad (cobertura de alto nivel, sin detalle)
	SD 4.6.5.2	Gestión de Brechas de seguridad e incidentes
ISO/IEC	8.2.3	Procesos disciplinarios
	13.1.1	Reporte de eventos de seguridad de información
	13.1.2	Reporte de debilidades de seguridad
	13.2.1	Responsabilidades y procedimientos
	13.2.3	Recolección de evidencia
NIST	IR-1	Políticas y procedimientos de respuesta a incidentes
	IR-6	Reporte de incidentes
COBIT	DS 5.7	Protección de la tecnología de seguridad. Área clave: Resistencia de manipulación
ITIL	SO 5.4	Gestión y soporte de servidores
ISO/IEC	6.1.4	Proceso de autorización para las instalaciones de procesamiento de información
	9.1.6	Áreas de acceso público, despacho y recepción
	9.2.1	Ubicación y protección de equipos
	9.2.3	Seguridad de cableado
	10.6.2	Seguridad de los servicios de red
	10.7.4	Seguridad de la documentación de sistemas
	10.10.1	Logs de auditoría
	10.10.3	Protección de logs
	10.10.4	Logs de administrador y de operador
	10.10.5	Logs de fallas
	10.10.6	Sincronización de relojes
	11.3.2	Equipos desatendidos de usuario
	11.3.3	Políticas de escritorios y pantallas limpias
	11.4.3	Identificación de equipos en redes
	11.4.4	Protección de puertos de configuración y diagnóstico remoto
	11.5.1	Procedimientos seguros de inicio de sesión
	11.5.4	uso de utilitarios del sistema
	11.5.5	Período de inactividad de sesión
	11.5.6	Limitación del tiempo de conexión
	11.6.2	Aislamiento de sistemas sensitivos
	11.7.1	Computación móvil y las comunicaciones
	11.7.2	Telégrafo
	12.4.1	Control de software de operaciones
	12.6.1	Control de vulnerabilidades técnicas
	13.1.2	Reporte de debilidades de seguridad
	13.2.3	Recolección de evidencia
	15.2.2	Verificación de cumplimiento técnico
	15.3.2	Protección de las herramientas de auditoría de sistemas

NIST	PE-4	Protección física y del medio ambiente. Accesos de control para medios de trasmisión
	SA-5	Sistemas y Servicio de Adquisición. Documentación de sistemas de información
	SC-3	Sistemas de protección y comunicación, funciones de seguridad
COBIT	DS 5.8	Administración de claves criptográficas. Áreas clave: Gestión del ciclo de vida de llaves criptográficas
ISO/IEC	10.8.4	Mensajería electrónica
	12.2.3	Integridad de mensajes
	12.3.1	Política de uso de controles criptográficos
	12.3.2	Gestión de llaves
	15.1.6	Regulación de controles criptográficos
NIST	SC-12	Sistemas de protección y comunicación, gestión y establecimiento de claves criptográficas
	SC-13	Sistemas de protección y comunicación, uso de criptografía validada
COBIT	DS 5.9	Prevención detección y corrección de software malicioso. Áreas clave: Parches de actualización, control de virus y protección de malware
ISO/IEC	10.4.1	Controles contra el código malicioso
	10.4.2	Controles contra el código moil
NIST	SC-18	Sistemas de protección y comunicación, códigos móviles
	SI-3	Integridad del Sistema y la información. Protección de código malicioso
	SI-7	Integridad del Sistema y la información, integridad de información y software
	SI-8	Integridad del Sistema y la información. Protección de spam
COBIT	DS 5.10	Seguridad de la red. Áreas clave: controles para autorizar acceso y flujos de información desde y hacia las redes
ITIL	SO 5.5	Gestión de redes
ISO/IEC	6.2.1	Identificación de riesgos relacionados con terceros
	10.6.1	Controles de red
	10.6.2	Seguridad de los servicios de red
	11.4.1	Política de uso de los servicios de red
	11.4.2	Autentificación de usuarios para conexiones externas
	11.4.3	Identificación de equipos en redes
	11.4.4	Protección de puertos de configuración y diagnóstico remoto
	11.4.5	Segregación en redes
	11.4.6	Control de conexiones en la red
	11.4.7	Control de enrutamiento en la red
	11.6.2	Aislamiento de sistemas sensitivos

NIST	AC-4	Control de Acceso. Forzar flujos de información
	SC-7	Sistemas de protección y comunicación,
	SI-4	Integridad del sistema y la información, técnicas y herramientas para monitorear los sistemas de información
COBIT	DS 5.11	Intercambio de datos sensitivos. Áreas clave: Ruta confiable y controles de autenticación, constancia de recepción y no repudio
ISO/IEC	6.2.1	Identificación de riesgos relacionados con terceros
	10.6.1	Controles de red
	10.6.2	Seguridad de los servicios de red
	11.4.1	Política de uso de los servicios de red
	11.4.2	Autenticación de usuarios para conexiones externas
	11.4.3	Identificación de equipos en redes
	11.4.4	Protección de puertos de configuración y diagnóstico remoto
	11.4.5	Segregación en redes
	11.4.6	Control de conexiones en la red
	11.4.7	Control de enrutamiento en la red
	11.6.2	Aislamiento de sistemas sensitivos
NIST	AU-10	Auditoría y revisión de costos, no repudio.
	SC-9	Sistemas de protección y comunicación, confidencialidad de la transmisión
	SC-11	Sistemas de protección y comunicación, rutas confiables
	SC-16	Sistemas de protección y comunicación, parámetros de transmisión de seguridad
	SC-23	Sistemas de protección y comunicación, sesión de autenticidad

Tabla 3. 8 DS 5 Garantizar la Seguridad de los Sistemas

DS11 Administración de Datos.- Una efectiva administración de datos requiere de la identificación. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para la administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.		
MARCO	**No.**	**PREGUNTAS**
COBIT	DS 11.1	Requerimientos del negocio para la gestión de datos. Área clave: Diseño de formulario de entrada. Minimizando errores u omisiones. Procedimientos de manejo de errores.
ITIL	SD 5.2	Gestión de los datos y la información
ISO/IEC	10.8.1	Políticas y procedimientos para el intercambio de información
NIST	MP-1	Medios de protección, políticas y procedimientos
	SI-10	Integridad del sistema y la información, validación y autenticidad
	SI-12	Integridad del sistema y la información, manejo de salida y retención.
COBIT	DS 11.2	Acuerdos para el almacenamiento y la conservación. Área clave: Preparación de documentos. Segregación de funciones.
ITIL	SD 5.2	Gestión de los datos y la información
	SO 5.6	Almacenamiento y archivo
ISO/IEC	10.5.1	Respaldo de la información
	10.7.1	Gestión de medios removibles
	15.1.3	Protección de registros organizacionales
NIST	MP – 4	Medios de protección.
COBIT	DS 11.3	Sistema de gestión de librería de medios. Área clave: Integridad y exactitud
ISO/IEC	10.7.1	Gestión de medios removibles
	10.7.2	Eliminación de medios
	12.4.3	Control de acceso al código fuente de los programas
COBIT	DS 11.4	Eliminación. Área clave: Detección, reporte y corrección
ISO/IEC	9.2.6	Eliminación o reutilización segura de equipos
	10.7.1	Gestión de medios removibles
	10.7.2	Eliminación de medios

NIST	MP – 5	Medios de protección. Transporte de medios
	MP – 6	Medios de protección. Saneamiento y disposición de medios
COBIT	DS 11.5	Respaldo y restauración. Área Clave: Requisitos legales. Mecanismos de recuperación y reconstrucción.
ITIL	SO 5.2.3	Respaldo y restauración
ISO/IEC	10.5.1	Respaldo de la información
NIST	CP 9	Plan de contingencia. Sistema de respaldos de la información
	CP 10	Plan de contingencia. Sistema de recuperación y reconstitución de la información
COBIT	DS 11.6	Requisitos de seguridad para la gestión de datos. Área Clave: Ingreso de datos por personal autorizado
ITIL	SD 5.2	Gestión de los datos y la información
ISO/IEC	10.5.1	Respaldo de la información
	10.7.3	Procedimientos para el manejo de la información
	10.8.3	Medios de almacenamiento físico en tránsito
	10.8.4	Mensajería electrónica
	12.4.2	Protección de datos de prueba de sistema
	12.4.3	Control de acceso al código fuente de los programas
NIST	AC – 1	Control de acceso políticas y procedimientos
	AC – 3	Control de acceso. Forzar accesos
	AC – 15	Control de acceso. Marcar automatización
	AC – 16	Control de acceso. Etiquetado automatizado
	MP – 1	Medios de protección, políticas y procedimientos
	MP – 2	Medios de protección, acceso de medios
	MP – 3	Medios de protección, etiquetado de medios
	MP – 4	Medios de protección, almacenamiento de medios
	MP – 5	Medios de protección, transporte de medios
	MP – 6	Medios de protección, disposición de medios
	SI – 10	Integridad del sistema y la información, validación y autenticidad
	SI – 12	Integridad del sistema y la información, manejo de salida y retención.

Tabla 3. 9 DS 11 Administración de Datos

DS12 Administración del ambiente físico.- La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos del centro de datos (Site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. la administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de computo y al personal.		
MARCO	**No.**	**PREGUNTAS**
COBIT	DS 12.1	Selección y diseño para el centro de datos. Área Clave: Selección de sitio basada en estrategia tecnológica, riesgo y requerimientos legales y regulatorios
ISO/IEC	9.1.1	Perímetro de seguridad física
	9.1.3	Seguridad de oficinas, salas e instalaciones
	9.1.6	Áreas de acceso público, despacho y recepción
NIST	PE – 1	Protección Física y del medio ambiente
	PE – 18	Protección Física y del medio ambiente
COBIT	DS 12.2	Medidas de seguridad física. Áreas Clave: Aseguramiento de la ubicación, incluyendo protección para acceso no autorizado, riesgos naturales e interrupciones de energía
ITIL	SO	Apéndice E. Descripción detallada de la gestión de las instalaciones
ISO/IEC	9.1.1	Perímetro de seguridad física
	9.1.2	Controles físicos de ingreso
	9.1.3	Seguridad de oficinas, salas e instalaciones
	9.2.5	Seguridad de los equipos fuera de las instalaciones
	9.2.7	Eliminar la propiedad
NIST	PE – 3	Protección Física y del medio ambiente, control de acceso físicos
	PE – 4	Protección Física y del medio ambiente, controles de acceso para medios de transmisión
	PE – 5	Protección Física y del medio ambiente, control de acceso para desplegar medios
	PE – 16	Protección Física y del medio ambiente, entrega y remoción
	PE – 19	Protección Física y del medio ambiente, información
COBIT	DS 12.3	Acceso físico. Areas clave: Acceso controlado a los locales
ITIL	SO	Apéndice E. Descripción detallada de la gestión de las instalaciones
	SO	Apéndice F. Controles de acceso físico

ISO/IEC	6.2.1	Identificación de riesgos relacionados con terceros
	9.1.2	Controles físicos de ingreso
	9.1.5	Trabajo en áreas seguras
	9.1.6	Área de acceso público, despacho y recepción
	9.2.5	Seguridad de los equipos fuera de las instalaciones
NIST	PE – 2	Protección Física y del medio ambiente, autorizaciones de acceso físico
	PE – 6	Protección Física y del medio ambiente, monitoreo físico de acceso
	PE – 7	Protección Física y del medio ambiente, control de visitantes
	PE – 8	Protección Física y del medio ambiente, registros de accesos
COBIT	DS 12.4	Protección contra factores ambientales. Área clave: monitoreo y control de factores ambientales
ITIL	SO	Apéndice E. Descripción detallada de la gestión de las instalaciones
ISO/IEC	9.1.4	Protección contra amenazas externas y ambientales
	9.2.1	Ubicación y protección de equipos
	9.2.2	Servicios de soporte
	9.2.3	Seguridad de cableado
NIST	PE – 9	Protección física y del medio ambiente, encendido de equipos y cableado
	PE – 10	Protección física y del medio ambiente, apagado de emergencia
	PE – 11	Protección física y del medio ambiente, prendido de emergencia
	PE – 12	Protección física y del medio ambiente, luces de emergencia
	PE – 13	Protección física y del medio ambiente, protección de incendios
	PE – 14	Protección física y del medio ambiente, controles de humedad y temperatura
	PE – 15	Protección física y del medio ambiente, protección de daños por agua
COBIT	DS 12.5	Gestión de instalaciones físicas. Áreas clave: Gestión de instalaciones de conformidad a los requerimientos de negocio, legales o regulatorios.
ITIL	SO 5.12	Gestión del centro de datos e instalaciones
ISO/IEC	9.2.2	Servicios de soporte
	9.2.4	Mantenimiento de equipos
NIST	PE – 1	Protección física y del medio ambiente, políticas y procedimientos.

Tabla 3. 10 DS 12 Administración del Ambiente Físico

ME3 Garantizar el cumplimiento con requerimientos externos.- Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio.		
MARCO	**No.**	**PREGUNTAS**
COBIT	ME 3.1	Identificación de los requisitos legales, regulatorios y de cumplimiento contractual. Área Clave: Identificación continua de requerimientos de cumplimiento para su incorporación en las políticas y prácticas
ISO/IEC	6.1.6	Relación con las autoridades que tengan impacto potencial en TI
	15.1.1	Identificación de legislación aplicable
	15.1.2	Derechos de propiedad intelectual
	15.1.4	Protección de datos y privacidad de la información personal
NIST	SA – 9	Protección Física y del medio ambiente
COBIT	ME 3.2	Optimización de respuesta a requerimientos externos. Áreas Clave: Revisión y ajuste de políticas y prácticas para asegurar el cumplimiento
COBIT	ME 3.3	Evaluación del cumplimiento con requerimientos externos. Áreas clave: Confirmación del cumplimiento
ISO/IEC	6.1.6	Relación con las autoridades que tengan impacto potencial en TI
	15.1.1	Identificación de legislación aplicable
	15.1.2	Derechos de propiedad intelectual
	15.1.4	Protección de datos y privacidad de la información personal
NIST	SA – 9	Protección Física y del medio ambiente
COBIT	ME 3.4	Aseguramiento positivo del cumplimiento. Área clave: Reportar garantía de cumplimiento y confirmación de las acciones correctivas
ISO/IEC	6.1.6	Relación con las autoridades que tengan impacto potencial en TI
	15.1.1	Identificación de legislación aplicable
	15.1.2	Derechos de propiedad intelectual
	15.1.4	Protección de datos y privacidad de la información personal
COBIT	ME 3.5	Reportes integrados. Áreas clave: Reportes integrados de cumplimiento de la empresa

Tabla 3. 11 ME 3 Garantizar el Cumplimiento con Requerimientos Externos

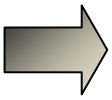
3.3.6 MATRIZ DE CADA PROCESO DE COBIT SELECCIONADO CON SUS REPECTIVAS ENTRADAS Y SALIDAS

La información mostrada en las siguientes matrices fue tomada de COBIT 4.1.

A continuación se muestran las matrices correspondientes a los 11 procesos de COBIT seleccionados con sus respectivas entradas y salidas:

- ✓ Entradas y Salidas de PO9 (Evaluar y Administrar los riesgos de TI) – Tabla 3.12
- ✓ Entradas y Salidas de AI3 (Adquirir y mantener una Infraestructura Tecnológica) – Tabla 3.13
- ✓ Entradas y Salidas de AI6 (Administrar cambios) – Tabla 3.14
- ✓ Entradas y Salidas de DS1 (Definir y administrar los niveles de servicio) – Tabla 3.15
- ✓ Entradas y Salidas de DS2 (Administrar los servicios de terceros) – Tabla 3.16
- ✓ Entradas y Salidas de DS3 (Administrar el desempeño y la capacidad) – Tabla 3.17
- ✓ Entradas y Salidas de DS4 (Garantizar la continuidad del servicio) – Tabla 3.18
- ✓ Entradas y Salidas de DS5 (Garantizar la seguridad de los sistemas) – Tabla 3.19
- ✓ Entradas y Salidas de DS11 (Administración de datos) – Tabla 3.20
- ✓ Entradas y Salidas de DS12 (Administración del ambiente físico) – Tabla 3.21
- ✓ Entradas y Salidas de ME3 (Garantizar el cumplimiento con requerimientos externos) – Tabla 3.22

DESDE	ENTRADAS
PO1	Planes estratégicos y tácticos de TI, portafolio de servicios de TI
PO10	Plan de administración de riesgo de proyecto
DS2	Riesgos de proveedores
DS4	Resultados de pruebas de contingencia
DS5	Amenazas y vulnerabilidades de seguridad
ME1	Tendencias y eventos de riesgos históricos
ME4	Apetito empresarial de riesgos de TI

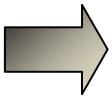


SALIDAS	HACIA						
Evaluación de riesgos	PO1	DS4	DS5	DS12	ME4		
Reporte de riesgos	ME4						
Directrices de administración de riesgos relacionados con TI	PO6						
Planes de acciones correctivas para riesgos relacionados con TI	PO4	AI6					

Tabla 3. 12 Entradas y Salidas de PO9[54]

[54] COBIT 4.1-2007. IT Governance Institute

DESDE	ENTRADAS
PO3	Plan de infraestructura de tecnología; estándares y oportunidades, actualizaciones periódicas del "estado de tecnología"
PO8	Estándares de adquisición y desarrollo
PO10	Directrices de administración de proyecto y planes detallados de proyecto
AI1	Estudio de factibilidad de los requerimientos del negocio
AI6	Descripción del proceso de cambio
DS3	Plan de desempeño y capacidad (requerimientos)

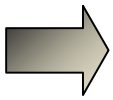


SALIDAS	HACIA						
Decisiones de adquisición	AI5						
Sistema configurado para realizar prueba / instalación	AI7						
Requerimientos de ambiente físico	DS12						
Actualizaciones de estándares de tecnología	PO3						
Requerimientos de monitoreo del sistema	DS3						
Conocimiento de la infraestructura	AI4						
OLAs planeadas inicialmente	DS1						

Tabla 3. 13 Entradas y Salidas de AI3[55]

[55] COBIT 4.1-2007. IT Governance Institute

DESDE	ENTRADAS
P02	Clasificaciones de datos asignados
P09	Valoración de riesgo
AI2	Especificación de disponibilidad, continuidad y recuperación
AI4	Manuales, de usuario, técnicos, operativos de soporte y de administración
DS1	SLA´S Y OLA´S

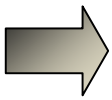


SALIDAS	HACIA						
Resultados de las prueba de contingencia	P09						
Criticidad de puntos de configuración de IT	DS9						
Plan de mantenimiento de respaldo y protección	DS11	DS13					
Umbrales de incidente/desastre	DS8						
Requerimientos de servicios contra desastres incluyendo roles y responsabilidades	DS1	DS2					
Reporte de desempeños de los procesos	ME1						

Tabla 3. 14 Entradas y Salidas de AI6[56]

[56] COBIT 4.1-2007. IT Governance Institute

DESDE	ENTRADAS
PO1	Planes tácticos y estratégicos, portafolio se servicios de TI
PO2	Clasificaciones de datos asignados
PO5	Portafolio de servicios de TI actualizado
AI2	Planes iniciales de SLAs
AI3	Planes iniciales de OLAs
DS4	Requerimientos de servicio en caso de desastre incluyendo roles y responsabilidades
ME1	Entrada de desempeño hacia la planeación de TI

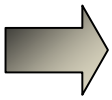


SALIDAS	HACIA						
Reporte de revisión de contrato	DS2						
Reportes de desempeño de los procesos	ME1						
Requerimientos de servicios nuevos/ actualizados	PO1						
SLAs	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLAs	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Portafolio de Servicios Actualizado	PO1						

Tabla 3. 15 Entradas y Salidas de DS1[57]

[57] COBIT 4.1-2007. IT Governance Institute

DESDE	ENTRADAS
PO1	Estrategia de contratación de TI
PO8	Estándares de adquisición
AI5	Arreglos contractuales, requerimientos de administración de relaciones con terceros
DS1	SLAs, reporte de revisión de contrato
DS4	Requerimientos de servicio contra desastre incluyendo roles y responsabilidades.

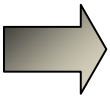


SALIDAS	HACIA						
Reportes de desempeño de los procesos	ME1						
Catálogo del proveedor	AI5						
Riesgos del proveedor	PO9						

Tabla 3. 16 Entradas y Salidas de DS2[58]

[58] COBIT 4.1-2007. IT Governance Institute

DESDE	ENTRADAS
AI2	Especificaciones de disponibilidad, continuidad y de recuperación.
AI3	Requerimientos de monitoreo del sistema
DS1	SLAs

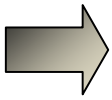


SALIDAS	HACIA						
Información sobre desempeño y capacidad	PO2	PO3					
Plan de desempeño y capacidad (requerimientos)	PO5	AI1	AI3	ME1			
Cambios requeridos	AI6						
Reportes de desempeño del proceso	ME1						

Tabla 3. 17 Entradas y Salidas DS3[59]

[59] COBIT 4.1-2007. IT Governance Institute

DESDE	ENTRADAS
P02	Clasificaciones de datos asignados
P09	Valoración de riesgo
AI2	Especificación de disponibilidad, continuidad y recuperación
AI4	Manuales, de usuario, técnicos, operativos de soporte y de administración
DS1	SLA´S Y OLA´S

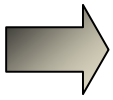


SALIDAS	HACIA						
Resultados de las prueba de contingencia	P09						
Criticidad de puntos de configuración de IT	DS9						
Plan de mantenimiento de respaldo y protección	DS11	DS13					
Umbrales de incidente/desastre	DS8						
Requerimientos de servicios contra desastres incluyendo roles y responsabilidades	DS1	DS2					
Reporte de desempeños de los procesos	ME1						

Tabla 3. 18 Entradas y Salidas de DS4[60]

[60] COBIT 4.1-2007. IT Governance Institute

DESDE	ENTRADAS
P02	Arquitectura de información; clasificación de datos asignados
PO3	Estándares de tecnología
PO9	Evaluación de riesgo
AI2	Especificaciones de controles de seguridad en las aplicaciones
DS1	OLAs

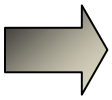


SALIDAS	HACIA						
Definición de incidentes de seguridad	DS8						
Requerimientos específicos de entrenamiento sobre conciencia de seguridad	DS7						
Reportes de desempeño del proceso	ME1						
Cambios de seguridad requeridos	AI6						
Amenazas y vulnerabilidades de seguridad	PO9						
Políticas y planes de seguridad de TI	DS11						

Tabla 3. 19 Entradas y Salidas de DS5[61]

[61] COBIT 4.1-2007. IT Governance Institute

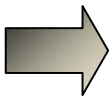
DESDE	ENTRADAS
P02	Diccionario de datos; clasificaciones de datos asignados
AI4	Manuales de usuario, de operación, de soporte, técnicos y de administración
DS1	OLAs
DS4	Plan de protección y de almacenamiento de respaldos



SALIDAS	HACIA						
Reportes de desempeño del proceso	ME1						
Instrucciones del operador para administración de datos	DS13						

Tabla 3. 20 Entradas y Salidas de DS11[62]

DESDE	ENTRADAS
P02	Clasificaciones de datos asignados
P09	Valoración de riesgo
AI3	Requerimientos del ambiente físico

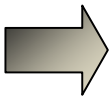


SALIDAS	HACIA						
Reportes de desempeño de los procesos	ME1 ME1						

Tabla 3. 21 Entradas y Salidas de DS12[63]

[62] COBIT 4.1-2007. IT Governance Institute
[63] COBIT 4.1-2007. IT Governance Institute

DESDE	ENTRADAS
*	Requerimientos de cumplimiento legal y regulatorio
PO6	políticas de TI



SALIDAS	HACIA						
Catálogo de requerimientos legales y regulatorios relacionados con la prestación del servicio de TI	PO4	ME4					
Reporte sobre el cumplimiento de las actividades de TI con los requerimientos externos y regulatorios	ME1						

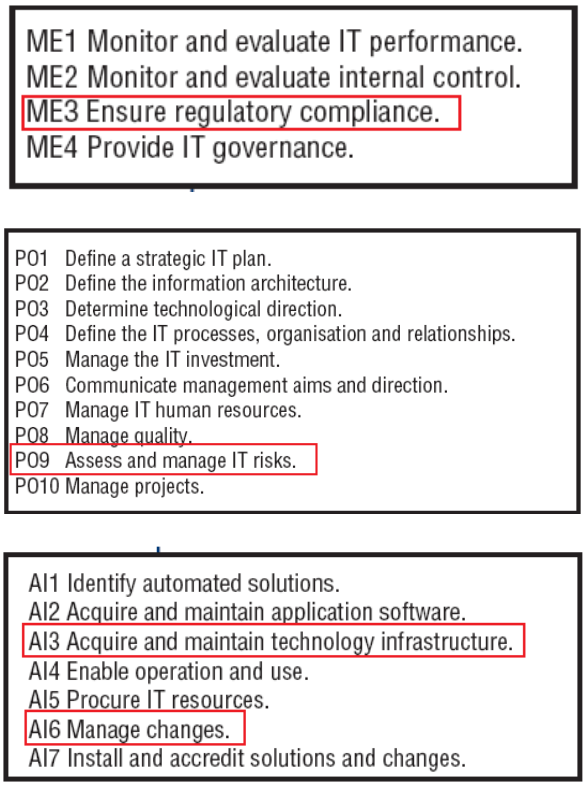
Tabla 3. 22 Entradas y Salidas de ME3[64]

[64] COBIT 4.1-2007. IT Governance Institute

3.3.7 GENERACIÓN DE LA MATRIZ DE EVALUACIÓN

Para la generación de la matriz de evaluación para el Site Alterno se procedió de la siguiente manera:

1. Se seleccionó los 11 procesos a ser evaluados como se muestra en la Fig. 3.2. Para explicar el desarrollo de la matriz se seleccionó el Proceso AI6 Administrar los cambios (proceso que fue tomado porque se realizan cambios entre el Site Principal y el Site Alterno, los cuales deben garantizar una gestión adecuada que evite impactos negativos y pérdidas para el negocio), dicho proceso contempla factores primarios, secundarios y en blanco.



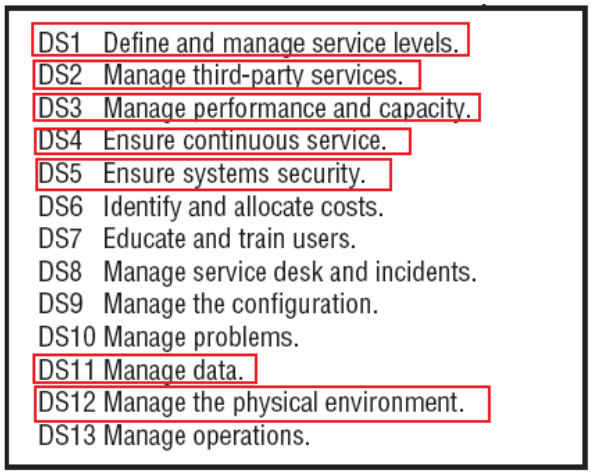


Figura 3.2 Requerimientos del Negocio para el AI6
Fuente: COBIT 4.1-2007. IT Governance Institute

2. Se describió el proceso AI6 según el Manual de COBIT:

"Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionado con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción", como se indica en la Fig. 3.3.

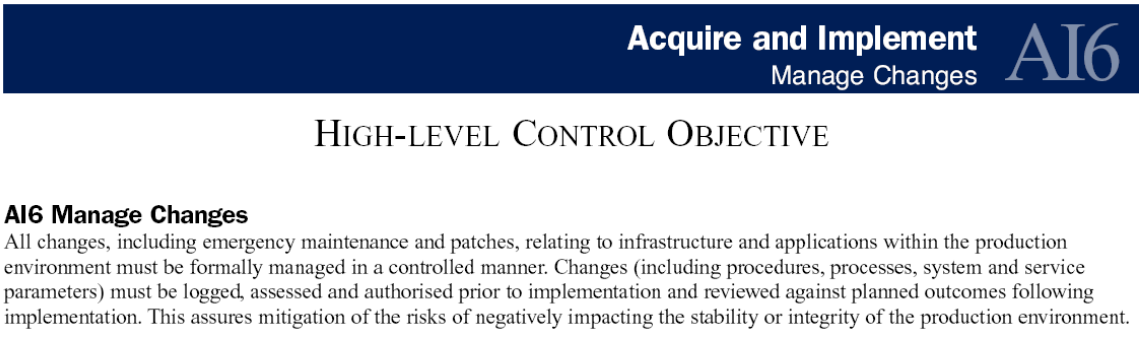


Figura 3.3 Adquirir e Implementar AI6
Fuente: COBIT 4.1-2007. IT Governance Institute

3. Se detalló cada uno de los objetivos de control. El AI6 tiene 5 según se detalla a continuación:

AI 6.1 Estándares y procedimientos para cambios

AI 6.2 Evaluación de impacto, priorización y autorización

AI 6.3 Cambios de emergencia

AI 6.4 Seguimiento y reporte de estado de los cambios

AI 6.5 Cierre y documentación del cambio

4. Para un mejor análisis mapeamos cada uno de los objetivos de control de COBIT con ITIL, ISO/IEC Y NIST, existen documentos emitidos por ISACA en los que COBIT está mapeado con ITIL, COBIT mapeado con ISO/IEC Y COBIT está mapeado con NIST. A continuación se encuentra el mapeo para cada uno de los objetivos de control.

El AI 6.1 se mapea de la siguiente manera:

En ITIL con: ST 4.2.6.1, ST 5, ST 6, ST 6.3, ST 6.4, SO 4.6.1

En NIST con: CM-1, CM-3

AI 6.2 mapeado con:

En ITIL con: ST 4.2.6.2, ST 4.2.6.3, ST 4.2.6.4, ST 4.2.6.5, ST 4.2.6.6, ST 4.2.6.8, ST 4.6, SO 4.3.5.1, SO 4.3.5.2, SO 4.3.5.3

En ISO/IEC con: 10.1.2, 12.5.1, 12.5.3, 12.6.1

AI 6.3 mapeado con:

En ITIL con: ST 4.2.6.9

En ISO/IEC con: 10.1.2, 11.5.4, 12.5.1, 12.5.3, 12.6.1, CM-3

AI 6.4 mapeado con:

En ITIL con: ST 3.2.13, ST 3.2.14, ST 4.1.5.3, ST 4.1.6

En ISO/IEC con: 10.1.2

AI 6.5 mapeado con:

En ITIL con: ST 4.2.6.4, ST 4.2.6.7, ST 4.4.5.10, ST 4.4.5.9, SO 4.3.5.5

En ISO/IEC con: 10.1.2

5. De los siete requerimientos del Negocio: Efectividad, Eficiencia, Cumplimiento, Confiabilidad, Integridad, Confidencialidad y Disponibilidad se califican los que tienen factor primario P o factor secundario S y los que están en blanco no se consideran, como se muestra en la Fig. 3.4.

Para el AI6 tenemos:

4 requerimientos con factor primario: Efectividad, Eficiencia, Integridad, Disponibilidad

1 requerimiento con factor secundario: Confiabilidad.

2 requerimientos en blanco: Confidencialidad y Cumplimiento.

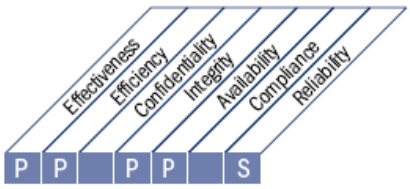


Figura 3 4 Requerimientos del Negocio AI6
Fuente: COBIT 4.1-2007. IT Governance Institute

6. Para obtener los resultados de los factores de calidad de control se consideran: Efectividad, Eficiencia, Cumplimiento, Confiabilidad, con calificaciones de 0 a 5. Como se indica en la Fig. 3.5.

- 0 —> No existente
- 1 —> Ad hoc
- 2 —> Repetible
- 3 —> Proceso definido
- 4 —> Administrado y Medido
- 5 —> Optimizado

MATURITY MODEL

AI6 Manage Changes

Management of the process of *Manage changes* that satisfies the business requirement for IT of *responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework* is:

0 Non-existent when
There is no defined change management process and changes can be made with virtually no control. There is no awareness that change can be disruptive for IT and business operations, and no awareness of the benefits of good change management.

1 Initial/*Ad Hoc* when
It is recognised that changes should be managed and controlled. Practices vary and it is likely that unauthorised changes take place. There is poor or non-existent documentation of change, and configuration documentation is incomplete and unreliable. Errors are likely to occur together with interruptions to the production environment caused by poor change management.

2 Repeatable but Intuitive when
There is an informal change management process in place and most changes follow this approach; however, it is unstructured, rudimentary and prone to error. Configuration documentation accuracy is inconsistent and only limited planning and impact assessment takes place prior to a change.

3 Defined Process when
There is a defined formal change management process in place, including categorisation, prioritisation, emergency procedures, change authorisation and release management, and compliance is emerging. Workarounds take place and processes are often bypassed. Errors may still occur and unauthorised changes occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalised, to support planned rollouts of new applications and technologies.

4 Managed and Measurable when
The change management process is well developed and consistently followed for all changes, and management is confident that there are minimal exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimise the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked. Configuration documentation is generally accurate. IT change management planning and implementation are becoming more integrated with changes in the business processes, to ensure that training, organisational changes and business continuity issues are addressed. There is increased co-ordination between IT change management and business process redesign. There is a consistent process for monitoring the quality and performance of the change management process.

5 Optimised when
The change management process is regularly reviewed and updated to stay in line with good practices. The review process reflects the outcome of monitoring. Configuration information is computer-based and provides version control. Tracking of changes is sophisticated and includes tools to detect unauthorised and unlicensed software. IT change management is integrated with business change management to ensure that IT is an enabler in increasing productivity and creating new business opportunities for the organisation.

Figura 3 5 Modelo de Madurez AI6
Fuente: COBIT 4.1-2007. IT Governance Institute

Para el AI6:

Se califican Efectividad y Eficiencia por tener factor Primario.

Se califica Confiabilidad por tener valor factor Secundario

Cumplimiento está en blanco no se debe calificar.

7. Se debe obtener el promedio de los resultados de los factores de calidad de control.

8. Para obtener los resultados de los factores de calidad del riesgo se consideran Integridad, Confidencialidad y Disponibilidad y se califican del mismo modo que en el paso 6.

Para el AI6:

Se califican Integridad y Disponibilidad por tener factor primario

No se tiene factor secundario

Confidencialidad no se considera por cuanto está en blanco.

9. A los resultados de los factores de calidad del riesgo se les multiplica por la vulnerabilidad con valores de 0 cuando casi no es vulnerable hasta 10 cuando es extremadamente vulnerable, para poner énfasis en el cuidado que se debe tener con los mismos.

Vulnerabilidad en AI6 es 7

Integridad * Vulnerabilidad = 5 *7 = 35

Confidencialidad * Vulnerabilidad (No se calcula para el ejemplo porque está en blanco)

Disponibilidad * Vulnerabilidad = 5 *7 = 35

10. Se obtiene el promedio de resultados de los factores de calidad del riesgo.

11. Para determinar el peso técnico, relacionado con el área de Infraestructura, se determina cuantos objetivos de control tiene cada proceso de COBIT, a cada objetivo se le da un valor, un valor más alto indica mayor importancia, la suma de los pesos técnicos de cada uno de los 4 dominios debe ser 100.

11. Para determinar el peso político, relacionado con la dirección de la Entidad, se determina cuantos objetivos de control tiene cada proceso de COBIT, a cada objetivo se le da un valor, un valor más alto indica mayor importancia, la suma de los pesos políticos de cada uno de los 4 dominios debe ser 100.

12. El peso total para cada objetivo corresponde al promedio del peso técnico y del peso político.

13. Se obtienen promedios para obtener las calificaciones finales de todos los objetivos de control. A continuación se muestra la matriz para el AI6. Como se muestra en Fig. 3.6.

Para visualizar la Matriz completa (Ver Anexo 6)

MARCO	No.	PREGUNTAS
COBIT	AI 6.1	Estándares y procedimientos para cambios. Áreas clave:
ITIL	ST 4.2.6.1	Procedimiento de cambio normal
	ST 5	Actividades comunes de operación en la transición del servicio
	ST 6	Organización para la transición del servicio
	ST 6.3	Modelos organizacionales para apoyar la transición de servicios
	ST 6.4	Relación de la transición del servicio con otras etapas del ciclo de vida
	SO 4.6.1	Gestión de cambios (actividades operativas)
NIST	CM-1	Gestión de configuración, políticas y procedimientos
	CM-3	Gestión de configuración, control de gestión de cambios

RESPUESTAS			PUNTA	EVIDE	OBS.	EFECTIV	EFICIEN	CUMPLIMIE	CONFIABILID	INTEGRID	CONF	DISPONIBILIDA	I	C	D
SI	NO	N/A													
si			3			5	5		5	5		5	7	35	0	35

Figura 3 6 Matriz de Evaluación AI6
Fuente: Curso COBIT –CEC-Instructor: Ing. Mark Jaramillo
Elaborado por autores

13. Los valores obtenidos se pasan a la pestaña resumen. Como se indica en la Fig. 3.7.

ADQUIRIR E IMPLEMENTAR						RESULTADOS DE RIESGO			VULNERABILIDAD	RESULTADOS DE CONTROL				MADUREZ	
PROCESOS						IMPACTO				EFECTIVIDAD	EFICACIA	CUMPLIM	CONFIABIL	CALIF.	RESULT.
No.	EMPRESA	COBIT	PESO TECNICO	PESO POLITICO	PESO TOTAL	I	C	D							%
1	Adquirir y mantener una infraestructura tecnológica	AI3	70	60	65	50,00	0,00	50,00	75,00	70	70	0,00	0,00	3,5	70
2	Administrar cambios	AI6	30	40	35	42,00	0,00	42,00	78,00	84	84	0,00	84,00	3,5	70
			100	100	100				76,50						70,00

Figura 3 7 Matriz de Evaluación Resumen AI
Fuente: Curso COBIT –CEC-Instructor: Ing. Mark Jaramillo
Elaborado por autores

14. Se requiere poner atención en aquellos procesos cuyo grado de madurez es bajo y tomar acciones para mejorar, para lo cual se debe revisar los mapeos que tiene dicho proceso, ir a la fuente respectiva (ITIL, ISO/IEC, NIST) y aplicar esos conocimientos.

Nota: A continuación en la Fig. 3.8, se esquematiza el modelo que se está utilizando:

El valor de i corresponde a cada uno de los factores de calidad (7 para todos los casos).

El valor de j corresponde a cada uno de los objetivos de control (220 repartidos entre los 34 procesos).

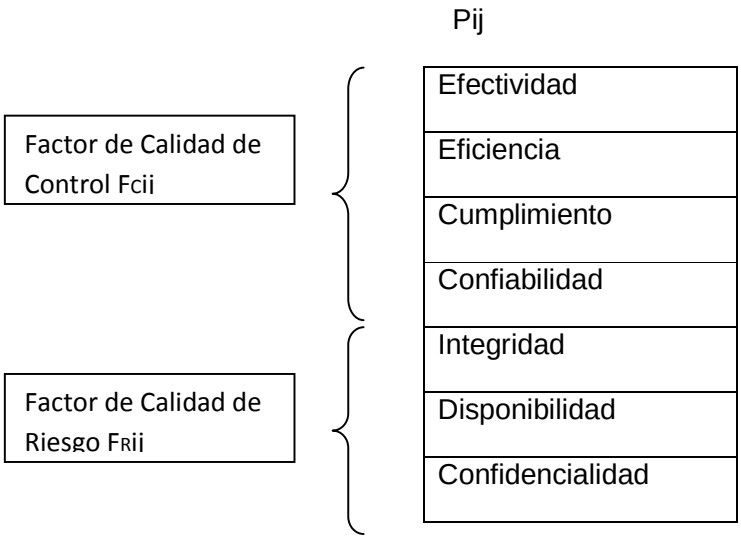


Figura 3 8 Procedimiento para obtener la Matriz de Evaluación
Fuente: autores

CAPÍTULO 4

EVALUACIÓN DE LA APLICABILIDAD DE LA PROPUESTA EN PACIFICARD

La validación del modelo no se pudo realizar con una muestra amplia, ni fue validada por expertos, por cuanto es un procedimiento extenso que requiere tiempo, considerando que existen: Bancos Privados, Cooperativas de Ahorro y Crédito, Mutualistas, Sociedades Financieras, Tarjetas de Crédito, Seguros Privados, Banca Pública, entre otras, ello no está al alcance de una tesis de grado y tomaría demasiado tiempo, por lo que se prefirió desarrollar una matriz con una lógica interna matemática que utiliza la metodología CRAMM con técnicas para el análisis y gestión de riesgos y fue aplicada en Pacificard, los resultados obtenidos mediante los cálculos permitieron identificar la situación actual en la gestión del Site Alterno de la empresa, los que fueron coherentes respecto a los cuatro dominios de COBIT que fueron mapeados con ITIL, ISO/IEC, NIST y permitieron identificar aquellos aspectos que se podría mejorar, por lo que se puede decir que el modelo es válido.

Pacificard para mantenerse en el mercado ecuatoriano como una de las principales tarjetas de crédito, cumple estándares establecidos por la Superintendencia de Bancos, Mastercard y Visa Internacional.

Para cumplir con las normativas establecidas por la Superintendencia de Bancos, Pacificard cumple con las leyes que aquí se establecen de acuerdo a lo indicado por Basilea.

Una de las normas que debe cumplir Pacificard es la resolución JB-2005-834 respecto a la Gestión de Riesgo Operativo para mitigar y monitorear los riesgos derivados de fallas en procesos, personas, tecnología de información y eventos

externos como el riesgo legal. Esta norma determinó plazos para que las Entidades implanten sistemas de gestión de riesgos operativos.

Para identificar el riesgo en los procesos se deben identificar procesos estratégicos, productivos, operativos, de apoyo, para lo cual se debería contar con un mapa de procesos y la cadena de valor de la Entidad.

Para determinar el riesgo de personas se puede hacer ingeniería social, se debe validar que la Entidad garantice condiciones laborales idóneas, realizar evaluaciones en varios ámbitos y contar con una Base de Datos de información respecto a la trayectoria de cada empleado.

Para fijar los riesgos de eventos externos se debe analizar y cuantificar los servicios públicos, los desastres naturales, los atentados, los actos delictivos, entre otros.

Para la identificar los riesgos de tecnologías de información las instituciones deben disponer una adecuada información respecto a la administración de tecnología, operaciones para satisfacción de requerimientos, recursos, servicios, procesos de adquisición, infraestructura, etc. Deben usarse estándares, herramientas, técnicas para gestionar y mitigar los riesgos.

Al momento Pacificard está certificada por la norma ISO 9001:2008 y cumple con la documentación y manuales que indica la norma.

Por ser un emisor de Mastercard y Visa cumple con la documentación que exige PCI para asegurar la seguridad en transacciones e información de crédito y datos de clientes y tarjetas de crédito.

Con la presente evaluación se pretende determinar si es factible o no aplicar la propuesta de gestión de TIC’s para el Site Alterno de Pacificard, considerando los aspectos: técnico, operacional, legal y económico.

4.1 ASPECTOS TÉCNICOS

Para la evaluación técnica de esta propuesta se consideró, el Site Alterno de Pacificard que este momento ya existe, está ubicado en la ciudad de Quito, mientras que el Site Principal está en la ciudad de Guayaquil.

La factibilidad de poder acatar esta guía se debe sujetar a las decisiones tomadas por la Gerencia General de Pacificard, en conjunto con la Gerencia de Infraestructura y de Seguridad de la Información, actualmente Pacificard tiene su Site Alterno en la ciudad de Quito.

La matriz de Pacificard se encuentra en la ciudad de Guayaquil y cuenta con sedes en las ciudades de Quito, Cuenca y Ambato, para las otras ciudades como: Galápagos, Riobamba, Ibarra, etc. se ayudan de la infraestructura del Banco del Pacífico.

Es importante mencionar que cada lugar cuenta con su respectivo Ruteador, Firewall y Servidor eSafe, para alcanzar una seguridad aceptable en la salida que se tiene al Internet, a Mastercard Internacional y Visa Internacional.

Se cuenta con un detalle de equipos por usuarios donde se describe el nombre del empleado, el usuario, el departamento en el que labora, el nombre del servidor al que accede, la dirección IP, el tipo de equipo, la ubicación exacta y la ciudad.

Se dispone de información como configuración de los servidores, características de los procesadores, característica de la memoria, características de los discos duros, puertos usados por los servidores, entre otros.

Se cuenta con la configuración de los discos y dispositivos de backup y restore con indicaciones de la ciudad y servidores donde se encuentran.

Del mismo modo se cuenta con un detalle de impresoras y escáneres que deben ser restaurados así como la configuración de los mismos con el respectivo detalle de equipo, marca, modelo, número de serie, área y edificio en el que se encuentran

Cada uno de los racks tiene su respectivo diagrama que incluye las ubicaciones de los switch con cantidad que puertos, velocidad y de UPS.

Con respecto al acceso a Internet se cuenta con dirección IP para dar permisos y restricciones al Internet al personal indicado.

Para los equipos de comunicaciones se cuenta con los siguientes listados:

Listado de direcciones IP utilizadas en la red Pacificard con máscara, Gateway, oficina y ciudad.

Listado de direcciones IP utilizadas en routers con red, equipo, canal, marca de equipo, enlace, estado, observaciones.

Listado de direcciones IP utilizadas para replicación con red, equipo, uso, enlace, estado y observaciones.

Listado de direcciones IP utilizadas para cajas con red, equipo, uso y observaciones

Se realizan pruebas periódicas con la finalidad de asegurar el correcto funcionamiento de equipos de backup validando que los procesos de recuperación son viables y están debidamente actualizados.

Se dispone de listados de aplicaciones críticas y los servidores donde se encuentran, software utilizado, licencias, etc.

Conclusión: Esta propuesta de gestión es factible técnicamente en razón de que Pacificard cuenta con la mayor parte de equipos necesarios para el cumplimiento de esta propuesta.

4.2 ASPECTOS OPERACIONALES

En cada uno de los equipos que deben levantarse se cuenta con una priorización y responsable de levantarlos.

Al administrador de recuperación se le debe informar los cambios producidos en adquisición de nuevos equipos, licenciamiento de software, actualizaciones en los sistemas operacionales, contratistas, proveedores de servicios, clientes importantes, direcciones y contactos de proveedores, usuarios importantes en la restauración de servicios, mejoras o nuevas implementaciones a nivel de redes, enlaces, comunicaciones, procesos nuevos o eliminados, ubicaciones físicas.

Se cuenta con pruebas iniciales para verificar la funcionalidad del software de cada uno de los sistemas o aplicaciones críticas bajo determinadas situaciones para determinar posibles fallos de implementación, de calidad, de usabilidad u otros.

Se realizan pruebas funcionales para ensayar el funcionamiento del sistema con usuarios e instituciones involucradas, con varios escenarios.

Finalmente se llevan a cabo las pruebas de integración que son aquellas en que se verifica todos los componentes comprometidos en el funcionamiento, especialmente en el momento en el que el Site Principal no esté disponible y el Alterno debe realizar sus funciones.

Para el correcto funcionamiento del Site Alterno se involucra a personal interno y externo quienes tienen funciones determinadas, para el personal interno se cuenta con el organigrama respectivo de indica la jerarquía bajo la cual se rige Pacificard, con respecto a personal externo disponen de un listado de proveedores clave de hardware y software con información de: nombre de la empresa, contacto comercial, teléfonos, contacto comercial, teléfonos, dirección de la oficina, etc. Todo ello para proveedores de hardware, software, base de datos, comunicaciones.

Se cuenta con un listado de actividades que deben ejecutarse entre los procedimientos que con más frecuencia se llevan a cabo constan:

Caída de energía eléctrica

Ataques de Hackers y virus

Incendio en el centro de cómputo

Contingencia para comunicaciones

Contingencia para Switch transaccional

En los que se describe las situaciones a seguir en cada caso e incluso el momento en el que el Site Alterno debe utilizarse y los momentos en los cuales es necesario escalar a proveedores externos el problema.

Para el caso de Site Alterno se cuentan con las indicaciones de métodos de conexión al mismo, bajar los servicios de Base de Datos y Aplicaciones en el Site Principal para levantarlos en el Alterno, configuración de esquema de comunicaciones de dirección del host, Ruteador, puerto, etc.; verificación de las rutas de conectividad, arranque de la Base de Datos, verificación del motor de Base de datos, procedimiento para levantar equipos de comunicaciones, validación de transaccionalidad, se cuenta con un listado de actividades para la recuperación de cada equipo crítico.

Conclusión: La propuesta de gestión es factible operativamente por cuanto existe personal destinado a funciones específicas del Site Alterno, con quienes se coordinaría las aquellas funciones adicionales que se requiere se ejecuten. Sin embargo se ve la necesidad de contratar a un técnico a tiempo completo para supervisión y la ejecución de las prácticas que se están planteando en esta guía, será responsable de mantenerla actualizada, realizar la difusión a los involucrados, capacitar en lo concerniente a este tema, garantizar el cumplimiento, entre otros temas relacionados.

4.3 ASPECTOS LEGALES

Pacificard se debe regir a las leyes impuestas por la Superintendencia de Bancos, actualmente la normativa ecuatoriana se rige a Basilea.

Se cuenta con personas responsables de notificar a los involucrados los cambios en leyes, normas emitidas por organismos de control, riesgo y políticas de la institución, así como la actualización de los documentos y llevar el debido control de cambios.

A continuación se describen las leyes que deben cumplir las Entidades Bancarias:

Ley de Propiedad Intelectual

Constitución de la República

Ley General de Instituciones del Sistema Financiero

Ley General de Seguros Privados - Codificación

Ley de Seguridad Social

Decreto 194 - Cooperativas

Decreto 3270 - Mutualistas

Ley de Almacenes Generales de Depósitos

Ley de Burós de Información

Ley de Cheques

Ley de Creación de la Red de Seguridad Financiera

Ley del Banco del IESS

Resolución JB-2005-834 - Gestión de Riesgo Operativo

Verified by Visa

MasterCard SecureCode

En el Anexo 4, se encuentran detalladas algunas leyes.

Conclusión: Es factible legalmente en razón de que las mejores prácticas para la gestión de un Site Alterno van a permitir procedimientos más ordenados y a la vez serán un apoyo para el cumplimiento de políticas, normativas y leyes, y que tampoco se están contraponiendo a ninguna ley vigente, sino mas bien apoya al cumplimiento de las mismas.

4.4 ASPECTOS ECONÓMICOS

Al momento Pacificard cuenta con la infraestructura de un Site Alterno caliente, por lo que todos los costos relacionados a él, ya están contemplados en el presupuesto, sin embargo se desea que el mismo sea gestionado adecuadamente; tanto el Gerente de recuperación de desastres como el Administrador de recuperación de desastres ya contratados tendrán papeles fundamentales.

4.4.1 COSTO DEL PROYECTO

Horas Laborables: 8 horas diarias, 40 horas semanales, 160 horas mensuales aproximadamente.

Precio de un técnico en el Mercado: USD$ 1.500,00 (9,75 Hora / Técnico)

Costo Anual del técnico: USD$ 18.000,00

Cada hora que Pacificard deje de brindar sus servicios pierde cantidades que exceden el valor mencionado si se consideran las multas, las captaciones que deja de percibir y los usuarios que se retiran debido al mal servicio.

4.4.2 INGRESOS

Para llevar este proyecto como una inversión se planifica que debido al buen servicio cada día se incluirán 3 tarjetahabientes diarios el primer año, adicionales a los que normalmente se suscriben, el costo por mantenimiento de la tarjeta es 30 dólares en promedio.

PRIMER AÑO

30,00 USD$ * 3 TARJETAS * 5 DÍAS * 4 SEMANAS * 12 MESES

= USD$ 21.600,00

SEGUNDO AÑO

30,00 USD$ * 4 TARJETAS * 5 DÍAS * 4 SEMANAS * 12 MESES

= USD$ 28.800,00

TERCER AÑO

30,00 USD$ * 5 TARJETAS * 5 DÍAS * 4 SEMANAS * 12 MESES

= USD$ 36.000,00

4.4.3 VALOR ACTUAL NETO (VAN)

Para calcular el valor presente neto de flujos de caja que se obtendrán en el futuro

Si VAN >= 0 entonces se acepta el proyecto

FE: es el flujo neto efectivo esperado en el período t

k: es la tasa de rendimiento requerida

$$\text{VPN} = FE_0 + \frac{FE_1}{(1+k)^1} + \frac{FE_2}{(1+k)^2} + \cdots + \frac{FE_n}{(1+k)^n}$$

Datos	Descripción
10,21%	Tasa anual de descuento
-54.000	Costo inicial
21.600	Rendimiento del primer año
28.800	Rendimiento del segundo año
36.000	Rendimiento del tercer año
Fórmula	**Descripción (resultado)**
USD$ 14.701,93	Valor neto actual de esta inversión

Tabla 4.1 VAN del Proyecto[65]

4.4.4 TASA INTERNA DE RETORNO (TIR)

Para medir la rentabilidad del proyecto en términos porcentuales en una inversión

TIR: Tasa de interés activa efectiva

FE: Flujo efectivo

Si TIR > r entonces se acepta el proyecto[66]

$$FE_0 + \frac{FE_1}{(1+TIR)^1} + \frac{FE_2}{(1+TIR)^2} + \cdots + \frac{FE_n}{(1+TIR)^n} = 0$$[67]

[65] **Fuente: Propia**

[66] Fuente: Fundamentos de Administración Financiera Décimo segunda edición

Datos USD$	Descripción
-54.000	Costo inicial
21.600	Ingresos netos del primer año (3 tarjetas adicionales)
28.800	Ingresos netos del segundo año (4 tarjetas adicionales)
36.000	Ingresos netos del tercer año (5 tarjetas adicionales)
Fórmula	Descripción (resultado)
25%	Tasa interna de retorno de la inversión después de tres años
El TIR es 25% que es mayor a 10.21% tasa de interés efectiva	

Tabla 4.2 TIR del Proyecto

4.4.5 PERÍODO DE RECUPERACIÓN DE LA INVERSIÓN (PRI)

Para medir la rentabilidad del proyecto en términos de tiempo.

p: tiempo de vida del proyecto

Si PRI < p entonces se acepta el proyecto

AÑO	COSTOS USD$	BENEFICIOS USD$	FNC (FLUJO NETO DE CAJA) USD$	SFNC (SUMATORIA DEL FLUJO NETO DE CAJA) USD$
0	0,00	0,00	0,00	0,00
1	18.000,00	21.600,00	3.600,00	3.600,00
2	18.000,00	28.800,00	10.800,00	14.400,00
3	18.000,00	36.000,00	18.000,00	32.400,00

Tabla 4.3 Flujo de Caja del Proyecto

PRI=t2+|SFNC2|*(t3-t2)/(|SFNC2|+|SFNC3|

PRI=2+|14.400,00|*(3-2)/|14.400,00|+|32.400,00|

PRI= 0,307 años

Conclusión: La propuesta de gestión es factible económicamente por cuanto los indicadores así lo muestran, Pacificard al ser una Entidad que depende de la imagen institucional de brinda al público, no puede dejar de brindar el servicio para el que fue creado ni aun cuando existan problemas externos en muchos de estos inconvenientes les apoyará disponer de un Site Alterno, de tal manera que el costo que implique una buena gestión del mismo puede incluso llegar a determinar la supervivencia de la Entidad.

4.5 APLICABILIDAD DE LA PROPUESTA EN PACIFICARD[68]

4.5.1 ELABORACIÓN

Pacificard actualmente se encuentra apoyando la gobernabilidad a través de:

- Marcos de control, que actualmente están siendo exigidos por la norma ISO 9001:2008, cumpliendo con indicadores asignados para cada área y para cada tarea.
- Un área de seguridad de la información que monitorea todas las áreas de la empresa incluyendo operaciones y TI.
- Un área de detección y prevención de fraudes se aseguran las transacciones realizadas por Pacificard y la seguridad de sus clientes

[68] Alineando COBIT 4.1, ITIL V3 4.1, ITIL v3 e ISO/IEC 27002 en beneficio del Negocio, Reporte del ITGI y la OGC.

- Un área de cumplimiento Pacificard sigue todos los controles que implican asegurar que el dinero con el que está trabajando no proviene de negocios ilegales y que todas sus transacciones son lícitas de acuerdo a lo indicado por las leyes de la República ecuatoriana y CONSEP.
- Controles que cumplen lo solicitado por PCI para asegurar que no se tienen filtros de información, y que las transacciones realizadas por Pacificard son seguras.
- Manuales y asignación de responsabilidades y tareas para los miembros de TI.
- Servicio de mesa de ayuda con tiempos de respuesta establecidos para atención de requerimientos a usuarios.
- Sistema de manejo de formularios con responsables asignados para cada área.
- Para definir los requisitos del servicio y las definiciones del proyecto, tanto internamente como con los proveedores de servicios
- Niveles de acuerdos de servicio con proveedores externos a Pacificard, que deben cumplir determinadas peticiones que se establecen el momento de firmar un contrato.
- Requerimientos de TI, si se determina que es viable y rentable proceder, cumpliendo con un tiempo de elaboración y pruebas antes de la implantación que garanticen la ausencia de errores.
- Mejora continua mediante:
    - Planeación estratégica de la compañía para el año 2015
    - Análisis de la competencia en cuanto a Cartera, Facturación, número de tarjetas.
    - Marco para la auditoría, evaluación y una visión externa a través de: Benchmarking

- Verificación de la capacidad profesional o muestra de competencia en el mercado a través de:
    - Evaluaciones a proveedores donde se determina la calidad de su servicio.
    - Capacitación y evaluaciones constantes y periódicas al personal.
    - Certificaciones que garantizan que Pacificard cumple con normativas y procedimientos establecidos por diferentes empresas.

4.5.2 PRIORIZACIÓN

Pacificard para evitar implementaciones de estándares y mejores prácticas que no estén de acuerdo con las necesidades del negocio ha priorizado y determinado un plan para sus funciones y necesidades en particular.

Por requerimiento del negocio dispone de un área de TI y por requerimiento de la Superintendencia de Bancos, un área de Seguridad de la información.

Al igual que otras Entidades bancarias se tiene una Planificación de contingencias para la Recuperación de desastres informáticos.

También posee un Plan de continuidad del negocio.

El personal debe cumplir con la documentación desarrollada para la certificación ISO 9001:2008

4.5.3 PLANIFICACIÓN

Para asegurar obtener resultados positivos se tomará los siguientes pasos basados en la guía IT governance implementation guide del ITGI:

1. Establecer un marco organizativo con objetivos y responsabilidades claras donde cada involucrado asuma esta implementación como propia. Del área de sistemas se tienen 2 gerencias, gerencia de sistemas y gerencia de seguridad de la información, estas reportan directamente a la gerencia general, ayudando así a que sistemas pueda estar involucrado directamente en las decisiones administrativas que se tomen en Pacificard.
2. Alinear la estrategia de TI con los objetivos del negocio, Pacificard tiene objetivos de su plan estratégico para el año 2015, estos son monitoreados y evaluados mensualmente para determinar si están o no acercándose a la meta que aspira cumplir la empresa.
3. Para entender y definir los riesgos se ha considerado riesgos físicos, políticos, de seguridad del sistema, vulnerabilidades, patrones de desempeño, iniciativas.
4. Definir las áreas objetivo y determinar las áreas de proceso de TI que son críticas para la entrega de valor y gestionar dichas áreas de riesgo. Pacificard trabaja con 2 marcas internacionales, Mastercard y Visa, se debe asegurar que las transacciones que se mantienen con estas 2 marcas son seguras, así como las peticiones que pueden venir de Datafast.
5. Analizar la capacidad vigente e identificar las brechas, se realizará una evaluación de la capacidad de madurez para saber las áreas que necesitan mejoras.
6. Desarrollar estrategias de mejora y decidir cuáles son los proyectos de mayor prioridad que ayudarán a mejorar la gestión y el gobierno de estas áreas. Se perfilarán proyectos de mejora continua.
7. Medir los resultados con mecanismos de puntuación.
8. Repetir los pasos 2 al 7 con la frecuencia posible

Cuidados que deben ser tomados en cuenta:

- Se necesita un cambio cultural por lo cual se deben motivar estos cambios.
- Verificar que haya una comprensión clara de los objetivos
- Obtener un respaldo de la alta dirección
- Ubicarse primero en las áreas donde es más fácil realizar cambios y lograr mejoras
- Alinear las mejores prácticas

Las mejores prácticas de TI deben ajustarse a los requisitos del negocio y estar integradas entre sí, con la ayuda de procedimientos internos, para ello este proyecto se apoya en las mejores prácticas de COBIT, ITIL, ISO/IEC y NIST, donde cada uno de los 34 procesos de COBIT serán mapeados hacia ITIL, ISO/IEC y NIST.

4.5.4 SELECCIÓN DE LOS PROCESOS A SER MAPEADOS PARA PACIFICARD[69]

Pacificard como una empresa emisora de Tarjetas de Crédito, está consciente que la información y la tecnología son pilares fundamentales que cimientan la estabilidad de este negocio.

Adicionalmente considerando que es una empresa ecuatoriana, tiene en cuenta la importancia de cumplir con las regulaciones impuestas por empresas regulatorias como la Superintendencia de Bancos, CONSEP y por trabajar con marcas internacionales como MASTERCARD y VISA lo que estas empresas consideren es un negocio seguro, con el menor porcentaje de riesgos que realiza sus operaciones de forma transparente a la sociedad, accionistas, empleados y clientes.

[69] Alineando COBIT 4.1, ITIL V3 4.1, ITIL v3 e ISO/IEC 27002 en beneficio del Negocio, Reporte del ITGI y la OGC.

Tomando en cuenta estas premisas se ha escogido 11 procesos de COBIT para mantenernos alineados dentro de esta meta. A continuación se va a detallar porque se considero cada uno de estos procesos para PACIFICARD.

Planear y Organizar

Este proceso ayuda a Pacificard a definir tácticas y estrategias que deben ser cumplidas, con el fin de contribuir a alcanzar de los objetivos con los cuales fue implementado y creado su Site Alterno.

Es mandatorio planear, comunicar y administrar desde diferentes perspectivas, la realización de la visión estratégica para implementar una estructura organizacional y una estructura tecnológica adecuada.

Pacificard si tiene alineadas las estrategias de TI con las del negocio, para lo cual se tiene a los Gerentes de Tecnología y Seguridad de la información para el apoyo a toma de decisiones que beneficien al negocio y tecnología.

En la empresa se tiene el personal indispensable para la realización de actividades relacionadas con el negocio, distribuidos en un espacio físico acorde a sus funciones, que realizan funciones de una manera óptima evitando así el desperdicio de recursos, adicionalmente el Site Alterno que se encuentra ubicado en la ciudad de Quito, también se mantiene en constante operación y monitoreo, reportando y resolviendo cualquier evento, garantizando que en caso de un riesgo se pueda trabajar basados en este Site Alterno.

Todo el personal de la Organización está consciente de cuáles son las funciones de TI, y el personal que tiene funciones específicas a cumplir en el momento de ocurrencia de un riesgo sabe cuáles son las funciones que debe llevar a cabo.

PO9 Evaluar y Administrar los Riesgos de TI

Se debe dar mantenimiento a un marco de trabajo de administración de riesgos, el cual documenta riegos de TI, estrategias de mitigación y riesgos residuales. Estos planes para prevención y mitigación de riesgos.

PO9.1 Marco de trabajo de Administración de Riesgos, Pacificard tiene una planificación donde se detallan procedimientos y acciones a cumplir en caso de que se lleve a desarrollar uno de los riesgos que se detectaron en la evaluación de riesgos.

PO9.2 Establecimiento del Contexto del riesgo, adicionalmente si ocurriera uno de los riesgos no detallados, este plan ajustaría el incidente al proceso que más se ajuste a este evento, y se continuaría con el plan, luego de ocurrido el evento y en base a los procedimientos realizados se procederá a documentar este nuevo evento para el futuro.

PO9.3 Identificación de eventos, Pacificard determino que eventos pueden afectar las operaciones de tecnología y de la empresa, considerando al negocio como tal, aspectos regulatorios, legales, tecnológicos, comerciales, recursos humanos y operativos.

PO9.4 Evaluación de riesgos de TI, Se debe evaluar la probabilidad de impacto de los riesgos identificados.

PO9.5 Respuesta a los riesgos, le empresa ha considerado como se va a proceder en caso de un determinado riesgo, como debe responder el Site Alterno frente a estos eventos, determinando responsables y los niveles de tolerancia para los mismos.

PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos, Se tienen planes documentados y aprobados y pasos a seguir en caso de la ocurrencia de un riesgo, considerando los costos que la empresa puede afrontar y garanticen una continuidad en las operaciones del negocio, la aceptación de riesgos residuales y un monitoreo constante para reportar cualquier desviación a la alta dirección.

Adquirir e Implementar

Las soluciones de TI, deben ser identificadas, implementadas e integradas a los procesos del negocio, y considerando a una empresa que brinda servicios de Pago a sus clientes, debe mantener sistemas actualizados que soporten su competencia en el negocio.

Los planes realizados para la implementación y mantenimiento del Site Alterno deben garantizar que:

Se satisfacen las necesidades del negocio, se tienen tiempos, está dentro del presupuesto, una vez que fue creado, trabaja adecuadamente, los trabajos realizados para el Site Alterno.

AI3 Adquirir y mantener Infraestructura Tecnológica

Pacificard tiene procedimientos para la adquisición, implementación y actualización de Infraestructura Tecnológica para su Site Alterno.

AI3.1 Plan de Adquisición de Infraestructura Tecnológica, se tiene una evaluación de equipos que son vitales para los procesos del negocio que deben ser recuperados y como se van a ir comprando los equipos que pertenecen al Site Alterno, para ir asegurando poco su funcionamiento e integración con el sistema de Pacificard.

AI3.2 Protección y disponibilidad del recurso de infraestructura, se tienen procedimientos que garanticen que solo el personal autorizado puede acceder al Site Alterno, una vez determinados los fines y aprobaciones para su ingreso, adicionalmente se hacen pruebas en horas que no interrumpan el funcionamiento del negocio para asegurar que estos sistemas pueden funcionar en el momento de un evento especifico.

AI3.3 Mantenimiento de la Infraestructura, se tiene procedimientos para actualizar los equipos que se encuentran en el Site Alterno similares a los que se realizan en los equipos del Site principal, los cuales incluyen parches, estrategias de actualización, evaluación de vulnerabilidades y requerimientos de seguridad.

AI3.4 Ambiente de prueba de Factibilidad, Se tiene pruebas de efectividad y eficiencia, integración a lis sistemas del negocio. Migración de ambientes entre un Site y el Otro, control de versiones.

AI6 Adquirir y mantener Infraestructura Tecnológica

Todos los cambios, incluyendo procedimientos para emergencia y parches, se aplican formal y controladamente, garantizando que el Site Alterno va a funcionar como se espera cuando se llegue a necesitar, y que los tiempos de respuesta para realizar las configuraciones cuando este vaya a funcionar como principal sean los esperados.

AI6.1 Estándares y procedimientos para cambios, procedimientos de cambio formales para manejar de manera estándar todas las solicitudes.

AI6.2 Evaluación de impacto, priorización, y autorización. Se debe garantizar que las solicitudes de cambio sean estudiadas y priorizadas antes de una migración a producción.

AI6.3 Cambios de emergencia, se tiene procesos para estos cambios, que garanticen que siguen un proceso establecido, es posible que se realicen luego de la implantación de un cambio de este tipo.

AI6.4 Seguimiento y reporte del Status de cambio, sistemas de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del status de cambio de aplicaciones.

AI6.5 Cierre y documentación del cambio, cada vez que se ejecuten cambios, actualizar el sistema asociado, la documentación de usuario y procedimientos correspondientes.

Entregar y Dar Soporte

Se entregan los servicios requeridos, con prestación de servicios, administración de la seguridad, la continuidad, soporte a usuarios, administración de datos, cumpliendo con la entrega de servicios que requiere el negocio, optimizando costos, utilizando los sistemas de modo productivo y seguro, garantizando la confidencialidad, integridad y disponibilidad de servicios e información.

DS1 Definir y administrar los niveles de servicio

Pacificard cuenta con servicios de TI y niveles de servicio, así como monitoreo acerca del cumplimiento de los niveles de servicio.

Se debe dar mantenimiento a un marco de trabajo de administración de riesgos, el cual documenta riegos de TI, estrategias de mitigación y riesgos residuales. Estos planes para prevención y mitigación de riesgos.

DS1.1 Marco de trabajo de la Administración de los Niveles de Servicio, Acuerdos de niveles de servicio (SLAs) y acuerdos de niveles de operación (OLAs), incluyendo roles, tareas y responsabilidades de proveedores externos e internos y de los clientes.

DS1.2 Definición base de los servicios de TI sobre características de servicio que brinda el Site Alterno, organizados y almacenados de manera centralizada.

DS1.3 Acuerdos de niveles de servicio, Convenios de niveles de servicio para todos los procesos críticos de TI con base en requerimientos del cliente y procesos considerados como vitales para la continuidad del negocio.

DS1.4 Acuerdos de niveles de Operación, Asegurar que los niveles de acuerdos de operación expliquen cómo serán entregados y los servicios para soportar los SLAs de manera óptima.

DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio, monitoreo de niveles de servicio, con estadísticas par identificar tendencias positivas y negativas, en los procedimientos a seguir para mantener un Site Alterno.

DS1.6 Revisión de niveles de acuerdo de servicio y contratos, revisión de contratos con proveedores internos y externos ya que de un buen monitoreo y control de los mismos depende el éxito o fracaso del uso del Site alterno cuando se requiera su funcionamiento al 100%.

DS2 Administrar los servicios de terceros

De los servicios de terceros depende un gran porcentaje el éxito o fracaso del funcionamiento del Site Alterno, por eso se debe tener roles claros, responsabilidades y monitoreo de la efectividad y cumplimiento de dichos acuerdos.

DS2.1 Identificación de Todas las Relaciones con proveedores, se debe identificar los servicios de Pacificard que dependen de sus proveedores, teniendo en cuenta tiempos de respuesta y midiendo que tan crítico es el servicio de cada proveedor.

DS2.2 Gestión de Relaciones con Proveedores, gestión de relaciones con proveedores de Pacificard.

DS2.3 Administración de Riesgos del proveedor, Asegurar que los contratos están e acuerdo a requerimientos legales y regulatorios.

DS2.4 Monitoreo del desempeño del proveedor, asegurar que el proveedor está cumpliendo con los requerimientos del Site Alterno de Pacificard.

DS3 Administrar el desempeño y la capacidad

Proceso de revisión periódica del desempeño actual, y capacidad de recursos de TI, con pronóstico de necesidades futuras de almacenamiento y contingencias que satisfagan las necesidades que debe cumplir el Site Alterno.

DS3.1 Planeación del desempeño y la capacidad, asegurar la disponibilidad de la capacidad y desempeño con costos aceptables para un Site Alterno.

DS3.2 Capacidad y desempeño actual, de recursos de TI en intervalos regulares para determinar si existe suficiente capacidad de brindar servicios con base a niveles de servicio acordados.

DS3.3 Capacidad y desempeño futuros, de recursos de TI, minimizando riesgos de falla para el Site Alterno por falta de capacidad o degradación del desempeño.

DS3.4 Disponibilidad de Recursos de TI, Brindar capacidad y desempeño con cargas de trabajo normal, contingencias requerimientos de almacenamiento y ciclos de vida de los recursos de TI.

DS3.5 Monitoreo y reporte, monitoreo continuo para desempeño actual de TI para atender contingencias, y reportes de disponibilidad hacia el negocio de cómo se está manteniendo al Site Alterno.

DS4 Garantizar la continuidad del servicio

Pacificard está preocupada en brindar continuidad de servicios del negocio, para lo cual considera a TI como pilar fundamental, y mantiene y prueba planes de continuidad de TI.

Objetivos de Control para el DS4

DS4.1 Marco de Trabajo de continuidad de TI, desarrollo de un marco de trabajo de continuidad para TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización.

DS4.2 Planes de continuidad de TI; diseñados para disminuir el impacto de una interrupción mayor de procesos claves del negocio, apoyados en el adecuado funcionamiento del Site alterno con requerimientos de resistencia, procesamiento alternativo y capacidad de recuperación de todos los servicios críticos de TI.

DS4.3 Recursos Críticos de TI, definir puntos críticos del plan de continuidad de Pacificard, con prioridades en casos de recuperación, con lapsos de tiempo para cada recuperación crítica.

DS4.4 Mantenimiento del plan de continuidad de TI, con apoyo de la gerencia de TI se ejecutan procesos de control de cambios para asegurar el plan de continuidad de TI está actualizado, adicionalmente comunicación clara y oportuna de procedimientos y responsabilidades.

DS4.5 Pruebas del Plan de Continuidad de TI, probar el plan de continuidad de Pacificard de forma regular para asegurar que los sistemas se pueden recuperar de forma efectiva.

DS4.6 Entrenamiento del Plan de Continuidad de TI, asegurarse que el personal involucrado de Pacificard está preparado en los roles y procesos que se debe realizar en caso de desastres.

DS4.7 Distribución del plan de continuidad de TI, estrategia de distribución definida para que los planes se entreguen a las partes involucradas cuando se requiera, deben estar accesibles bajo cualquier escenario de desastre.

DS4.8 Recuperación y reanudación de los servicios de TI, acciones a tomar mientras se recuperan servicios, incluyendo activación del Site Alterno, comunicación a clientes, y procesos de reanudación.

DS4.9 Almacenamiento de respaldos fuera de las instalaciones, esta se mantiene en el Site alterno, ya que es la información que se requiere para la recuperación de TI, pegada a la política de clasificación de datos y prácticas de almacenamiento de datos.

DS4.10 Revisión Post Reanudación, una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

DS5 Garantizar la seguridad de los sistemas

Mantener la integridad de la información y proteger los activos de TI, requiere de un proceso de administración de seguridad, con roles y responsabilidades de seguridad, monitoreos y pruebas periódicas.

DS5.1 Administración de la seguridad de TI, en la organización para que la administración de la seguridad esté alineada a los requerimientos del negocio.

DS5.2 Plan de seguridad de TI, tener los requerimientos del negocio, riesgos y cumplimiento dentro de un plan de seguridad completo.

DS5.3 Administración de Identidad, asegurar que todos los usuarios y su actividad dentro de TI, es identificable de manera única.

DS5.4 Administración de cuentas del usuario, mediante la intranet se tiene un control de cuentas creadas, cerradas y responsables de solicitud y aprobación.

DS5.5 Pruebas, vigilancia y monitoreo de la seguridad, garantizar que la seguridad de TI es probada y monitoreada de modo proactivo.

DS5.6 Definición de incidente de seguridad, definir claramente y comunicar las características de incidentes de seguridad potenciales.

DS5.7 Protección de la tecnología de seguridad, garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad.

DS5.8 Administración de llaves criptográficas, políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución de llaves criptográficas, para garantizar la protección de las llaves.

DS5.9 Prevención, detección y corrección de software malicioso, medidas preventivas, detectivas y correctivas para proteger los sistemas de seguridad.

DS5.10 Seguridad de la red, técnicas de seguridad y procedimientos de administración asociados, para autorizar acceso y controlar los flujos de información dese y hacia redes.

DS5.11 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.

DS11 Administrar los datos

Identificación de requerimientos de datos, establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios.

DS11.1 Requerimientos del negocio para administración de datos, verificar que los datos que se espera para procesar, se reciben y procesan completamente, de forma precisa y a tiempo, con resultados apropiados a los requerimientos del negocio.

DS11.2 Acuerdos de almacenamiento y conservación, archivo, almacenamiento y retención de datos.

DS11.3 Sistemas de administración de librerías de medios, inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.

DS11.4 Eliminación, la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

DS11.5 Respaldo y restauración, de sistemas, aplicaciones, datos y documentación.

DS11.6 Requerimientos de seguridad para la Administración de datos, políticas y procedimientos para identificar a aplicar los requerimientos de seguridad.

DS12 Administrar el ambiente físico

La protección del equipo de cómputo y personal que labora en el Site Alterno, requiere de instalaciones bien diseñadas y bien administradas.

DS12.1 Selección y diseño del centro de datos, considerando riesgos como desastres u otros.

DS12.2 Medidas de seguridad física, perímetro de seguridad, ubicación de equipo crítico y área se envío.

DS12.3 Acceso Físico, otorgar, limitar y revocar el acceso al Site Alterno, registrando y monitoreando estos eventos.

DS12.4 Protección contra factores ambientales, instalación de dispositivos y equipo especializado para monitorear y controlar al ambiente.

DS12.5 Administración de instalaciones físicas, incluyendo equipos de comunicaciones y suministro de energía.

Monitorear y Evaluar

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio

abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

ME3 Garantizar el cumplimiento con Requerimientos Externos

Procesos de revisión que garanticen el cumplimiento de leyes, regulaciones y requerimientos contractuales.

ME3.1 Identificar los Requerimientos de las leyes, regulaciones y cumplimientos contractuales, leyes locales e internacionales, regulaciones y otros requerimientos externos que se deben de cumplir para incorporar en las políticas.

ME3.2 Optimizar la respuesta a Requerimientos externos, ajuste de políticas y estándares garantizando requisitos legales y regulatorios.

ME3.3 Evaluación del cumplimiento con requerimientos externos, cumplimiento de políticas, estándares y procedimientos con requerimientos legales y regulatorios.

ME3.4 Aseguramiento positivo del cumplimiento, garantía de cumplimiento a todas las políticas internas confirmando la ejecución de acciones correctivas.

ME3.5 Reportes integrados, integración de TI sobre reportes legales.

4.5.5 MATRIZ DE EVALUACION DEL SITE ALTERNO

A continuación, en la tabla 4.4 se muestra la Matriz de Gestión Propuesta, con los datos obtenidos de la evaluación realizada a Pacificard. Para ello se aplicó la Matriz de Evaluación obteniéndose la Matriz de Evaluación Aplicada a Pacificard la misma que se puede ver completa en el Anexo 7. (Ver Anexo 7).

					RESULTADOS DE RIESGO			VULNERABILIDAD
					IMPACTO			
EMPRESA	COBIT	PESO TECNICO	PESO POLITICO	PESO TOTAL	I	C	D	
Evaluar y administrar los riesgos de TI	PO9	100	100	100	41,67	41,67	41,67	78,33
		100	100	100				78,33

					RESULTADOS DE RIESGO			VULNERABILIDAD
					IMPACTO			
EMPRESA	COBIT	PESO TECNICO	PESO POLITICO	PESO TOTAL	I	C	D	
Adquirir y mantener una infraestructura tecnológica	AI3	70	60	65	50,00	0,00	50,00	75,00
Administrar cambios	AI6	30	40	35	42,00	0,00	42,00	78,00
		100	100	100				76,50

Tabla 4.4 Matriz Resumen (PO9, AI3, AI6) de Evaluación aplicada a Pacificard
Fuente: Curso COBIT –CEC-Instructor: Ing. Mark Jaramillo
Elaborado por: autores

	RESULTADOS DE CONTROL				MADUREZ	
	EFECTIVIDAD	EFICIENC	CUMPLIM	CONFIABI	CALIF.	RESULT.
EMPRESA						%
Evaluar y administrar los riesgos de TI	80	80	80,00	83,33	3,5	70
						70,00
					3,5	

	RESULTADOS DE CONTROL				MADUREZ	
	EFECTIVIDAD	EFICACIA	CUMPLIM	CONFIABI	CALIF.	RESULT.
EMPRESA						%
Adquirir y mantener una infraestructura tecnológica	70	70	0,00	0,00	3,5	70
Administrar cambios	84	84	0,00	84,00	3,5	70
						70,00
					3,5	

Tabla 4.5 Continuación: Matriz Resumen (PO9, AI3, AI6) de Evaluación aplicada a Pacificard

Fuente: Curso COBIT –CEC-Instructor: Ing. Mark Jaramillo

Elaborado por: autores

					RESULTADOS DE RIESGO			VULNERABILIDAD
					IMPACTO			
EMPRESA	COBIT	PESO TECNICO	PESO POLITICO	PESO TOTAL	I	C	D	
Definir y administrar los niveles de servicio	DS1	10	25	17,5	41,67	41,67	41,67	76,67
Administrar los servicios de terceros	DS2	15	10	12,5	32,50	35,00	32,50	75,00
Administra el desempeño y la capacidad	DS3	15	20	17,5	0,00	0	42	82,00
Garantizar la continuidad del servicio	DS4	15	15	15	0	0	48	77,5
Garantizar la seguridad de los	DS5	10	10	10	43,6364	43,636	43,636	76,36364
Administración de datos	DS11	15	10	12,5	38,3333	0	0	81,66667
Administración del ambiente físico	DS12	20	10	15	50	0	50	78
		100	100	100				77,79

					RESULTADOS DE RIESGO			VULNERABILIDAD
					IMPACTO			
EMPRESA	COBIT	PESO TECNICO	PESO POLITICO	PESO TOTAL	I	C	D	
Garantizar el cumplimiento con	ME3	100	100	100	0,00	0,00	0,00	78,00
		100	100	100				78,00

Tabla 4.6 Matriz Resumen (DS, ME) de Evaluación aplicada a Pacificard
Fuente: Curso COBIT –CEC-Instructor: Ing. Mark Jaramillo
Elaborado por: autores

	RESULTADOS DE CONTROL				MADUREZ	
	EFECTIVID	EFICAC	CUMPLI	CONFIAB	CALIF.	RESULT.
EMPRESA						%
Definir y administrar los niveles de servicio	83,3333	83,33	86,67	83,33	3,5	70
Administrar los servicios de terceros	75,00	70,00	70,00	65,00	3,5	70
Administra el desempeño y la capacidad	84	84	0	0,00	3,5	70
Garantizar la continuidad del servicio	78	78	0	0	3,5	70
Garantizar la seguridad de los	0	0	87,27	87,273	4	80
Administración de datos	0	0	0	76,667	3	60
Administración del ambiente físico	0	0	0	0	3,5	70
						70,00
					3,5	

	RESULTADOS DE CONTROL				MADUREZ	
	EFECTIVID	EFICAC	CUMPLI	CONFIAB	CALIF.	RESULT.
EMPRESA						%
Garantizar el cumplimiento con	0	0	76,00	76,00	3,5	70
						70,00
					3,5	

Tabla 4.7 Continuación: Matriz Resumen (DS, ME) de Evaluación aplicada a Pacificard

Fuente: Curso COBIT –CEC-Instructor: Ing. Mark Jaramillo
Elaborado por: autores

Luego de aplicar la matriz se han obtenido los siguientes resultados:

En el dominio Planear y Organizar la calificación fue de 3.5 que es un nivel de madurez administrado y medido, lo cual indica que la visión y planificación de

Pacificard tienen un buen enfoque que contribuye a la visión estratégica del negocio.

En el dominio Adquirir e Implementar la calificación fue de 3.5 que es un nivel de madurez administrado y medido, lo cual indica que las soluciones son integradas de acuerdo a los objetivos de Pacificard, y se tiene un gran enfoque en la importancia de la mejora continua de la infraestructura de la empresa.

En el dominio Desarrollar e Implementar la calificación fue de 3.5 que es un nivel de madurez administrado y medido, lo cual que está correctamente gestionado y puede ser medido.

En el dominio Monitorear y Evaluar la calificación fue de 3.5 que es un nivel de madurez administrado y medido, lo cual garantiza que se tienen controles para garantizar que los procesos son gestionados y pueden ser medidos.

La calificación global de Pacificard es 3.5, lo que nos muestra que el proceso es administrado y medido, y se pueden tomar acciones de mejora continua si se considera necesario.

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Las Entidades Bancarias deben cumplir las leyes, políticas y reglamentos de la legislación nacional e internacional, para evitar pérdidas de dinero, multas, sanciones o un cierre definitivo del negocio.
- Es necesario garantizar el cumplimiento de políticas y procedimientos que determine la Entidad, con un adecuado monitoreo que permita optimizar recursos para llegar a los objetivos corporativos del negocio.
- Es posible mejorar la gestión de TI, con un marco de referencia eficaz que gestione políticas, controles internos y prácticas definidas, lo que ayuda a que cada persona tenga conocimiento de las funciones que debe realizar y el procedimiento para ejecutarlas, menor dependencia de expertos, menor cantidad de errores, incremento de la confianza de socios, clientes y entes reguladores.
- Los procesos de implantación requieren del apoyo de la dirección y los recursos suficientes.
- El proceso debe ser controlado y revisado, convirtiéndose en un proceso de mejora continua.
- La efectividad de las mejores prácticas depende de cómo se implementan y mantienen.
- Las mejores prácticas ayudan a mejorar el desempeño, transparencia y control de actividades de TI.
- Las mejores prácticas representan un enfoque común para un buen control de TI, que trata de unificar el lenguaje para las personas involucradas.

- Las mejores prácticas ayudan a gestionar adecuadamente los riesgos de TI, evitando: proyectos fallidos, inversiones perdidas, brechas de seguridad, fallas de los sistemas, fallas de proveedores para entender y satisfacer los requerimientos de los clientes.
- El utilizar mejores prácticas traza un camino desde una situación caótica hacia procesos definidos y gestionados de TI.
- Las Entidades Bancarias necesitan priorizar dónde y cómo utilizar las mejores prácticas, se requiere un plan de acción eficaz que se adapte a las circunstancias y necesidades particulares.
- Para el caso de Pacificard se pudo mostrar la aplicabilidad de la propuesta de gestión en aspectos: económico, técnico, operacional y legal.
- Pacificard cuenta con su Hot Site y su Plan de Recuperación de Desastres, sin embargo si se complementa con la propuesta de gestión, se puede alcanzar mejores resultados.
- En el Ecuador las Entidades Bancarias y Financieras, son supervisadas por la Superintendencia de Bancos con la finalidad de revisar la transparencia en todos los movimientos.
- El contar con una alternativa de recuperación radica en la necesidad de mantener en funcionamiento los procesos críticos aún en situaciones de desastre.
- Se ve la necesidad de realizar continuos análisis de riesgos, en base a los cuales se puede establecer procedimientos de contingencia y de mitigación.
- Para seleccionar una alternativa de recuperación es de mucha ayuda llevar a cabo un BIA, un RTO y un RPO.

5.2 RECOMENDACIONES

- En el caso de aplicarse esta propuesta de gestión es necesario que se actualice periódicamente, de tal manera que se genere una base de conocimientos apropiada a la realidad de la Entidad Bancaria y con procedimientos en cada caso.
- Entre los especialistas que harán las revisiones de esta propuesta de gestión es importante contar con un asesor legal, debido a que las leyes siguen cambiando y es primordial cumplir con la normativa vigente.
- En el caso de Pacificard, si bien es cierto se cuenta con personal asignado a cada uno de los procesos a restaurar, se debería contar en cada paso con su respectivo punto de control, para garantizar el cumplimiento de los pasos requeridos.
- Realizar simulaciones para constatar que se van a obtener los procesos esperados, el simple hecho de realizar un restore de una Base de Datos puede indicarnos si los respaldos son funcionales.
- Considerar las recomendaciones que brinda la Superintendencia de Bancos (Ver Anexo 5).

BIBLIOGRAFÍA

[1] Superintendencia de Bancos y Seguros, Dirección Nacional de Estudios, Subdirección de Estadística y Estudios http://www.superban.gob.ec, último acceso, 15 de mayo 2011.

[2] IT GOVERNANCE INSTITUTE, OGC OFFICE OF GOVERNMENT COMMERCE; Alineando Cobit 4.1, ITIL V3 e ISO/IEC 27002 en beneficio del negocio, 2008.

[3] IT GOVERNANCE INSTITUTE, Mapping of NIST SP800-53 Rev 1 With COBIT 4.1, 2007.

[4] IT GOVERNANCE INSTITUTE, Mapping of ISO/IEC 17799:2005 With COBIT 4.0, 2006.

[5] IT GOVERNANCE INSTITUTE, Mapping of ITIL v3 With COBIT 4.1, 2008.

[6] ALVAREZ ÁLVAREZ GUSTAVO ALEXANDER, Universidad Nacional de Trujillo; NIST SP800-53 REV. 3 con COBIT 4.1, 2010.

[7] IT GOVERNANCE INSTITUTE, Mapping of NIST SP800-53 Rev 1 With COBIT 4.1, 2007.

[8] Alineando COBIT 4.1, ITIL V3 4.1, ITIL v3 e ISO/IEC 27002 en beneficio del Negocio, Reporte del ITGI y la OGC.

GLOSARIO DE TÉRMINOS

1. Efectividad: Precisión y plenitud con la que los usuarios alcanzan los objetivos especificados. Se encuentra normalmente basada en la relevancia de los documentos recuperados.
2. Eficiencia: Medida de los recursos empleados en relación con la precisión y plenitud con que los usuarios alcanzan los objetivos especificados. A esta idea se asocia la facilidad de aprendizaje.
3. Confidencialidad: La información únicamente será proporcionada a quien debe conocerla. La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
4. Integridad: La información permanece intacta. Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información.
5. Disponibilidad: La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
6. En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizada para protegerlo, y los canales

de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas operativos debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

7. Riesgo: Es cualquier situación que impida alcanzar el objetivo, lo que puede ser intencional o accidental. Es también la posibilidad de que se materialice una amenaza en un Activo, en un Dominio o en toda la Organización. Existen una serie de sinónimos relacionados al término tales como: peligro, inseguridad, trance, lance, conflicto, compromiso, apuro, alarma.
8. Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
9. Impacto: Es la medida de la consecuencia al materializarse una amenaza.
10. Vulnerabilidad: es la debilidad que posibilita la ocurrencia de la materialización de una amenaza sobre un Activo.
11. Ataque: Es un evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
12. Desastre o Contingencia: Es la interrupción de la capacidad de acceso y procesamiento de la información[70].
13. VeriSign: Es una empresa de seguridad informática famosa por ser una autoridad de certificación reconocida mundialmente. Emite certificados digitales RSA para su uso en las transmisiones seguras por SSL, principalmente para la protección de sitios en Internet en su acceso por http.
14. Verified by Visa: Es un sistema de autenticación en línea, que permite realizar compras en la Internet con la misma seguridad que existe en el mundo físico, de forma rápida y sencilla.

---

http://es.wikipedia.org/wiki/Seguridad_de_la_informacion

15. MasterCard SecureCode: Es un servicio de seguridad para protegerlo contra el uso no autorizado de la tarjeta MasterCard mientras se compra por Internet, en los comercios participantes.

ANEXOS