UNAPEC
UNIVERSIDAD APEC

Escuela de Graduados

Monografia para Optar por el Título de:

Maestría en Gerencia y Productividad

"Implementación de un Sistema de Seguridad de Infraestructura Aplicado a Empresas del Sector Bancario del País Año 2013"

Sustentante:

Marcos Antonio Díaz Diloné **2011-2112**

Asesor(a):

Edda A. Freites Mejía, MBA

Distrito Nacional, República Dominicana.

Agosto, 2013.

RESUMEN

En estos momentos la privacidad de las redes de informaciones de las empresas se encuentra violentada constantemente por los hackers y piratas informáticos, en consecuencia a estas premisas, presentamos este proyecto de creación de un sistema o aplicación de seguridad de infraestructura, aplicable al proceso de recibo de pagos del exterior, lo que conocemos como Remesas. El objetivo de este sistema es garantizar la seguridad de las transacciones de las remesas recibidas del exterior de los clientes vía la aplicación de monitoreo. Esta propuesta de implementación, tiene como objetivo mostrar cómo funciona esta herramienta, donde detallaremos el alcance de la misma, su estandarización y controles. Dentro de los puntos que identificamos como vitales en esta propuesta de implementación, consideramos los siguientes: la elaboración de las políticas de seguridad tecnológica, los componentes básicos de infraestructura, que seleccionamos como parte de la implementación, la identificación de la vulnerabilidad que están expuestas las aplicaciones que manejan procesos críticos de la infraestructura de la empresa y el flujo de implementación de dicha aplicación. Para la realización de este proyecto, hemos utilizado una metodología descriptiva y práctica donde se detallan el proceso, flujo de trabajo y operatividad de la aplicación, así como su ejecución, seguimiento y costo operativo. La principal conclusión a la que hemos llegado, es que si las empresas que manejan procesos informáticos críticos, desean mantener protegida estas informaciones, deben invertir en las actualizaciones y creación de aplicaciones de seguridad que reguarden la integridad de sus procesos. Entendemos que el éxito de la misma depende del seguimiento y controles creados por la empresa, el monitoreo constante a las actualizaciones que realice el suplidor de la aplicación, así como invertir en la capacitación de los usuarios para el uso eficiente y exitoso de esta herramienta.

INDICE GENERAL

CAPITULO III

IMPLEMENTACION DEL SISTEMA DE SEGURIDAD INFRAESTRUCTURA

LISTA DE FIGURAS

Pág.

INTRODUCCION

El presente proyecto de investigación, es una muestra del proceso que realizaremos sobre los aspectos relevantes de la implementación de un sistema de seguridad de infraestructura aplicado a empresas del sector financiero de nuestro país.

La información crítica es el alma de toda organización, la manera en que lo creamos, lo consumimos y lo comunicamos ha cambiado radicalmente. Por esta razón se debe modificar la forma en la que las empresas protegen este tipo de información y sus componentes de riesgos. Basta con ver las amenazas actuales y los enormes desafíos que se presentan, los ataques son más sofisticados y dirigidos.

Como parte del marco teórico que abarcamos como sustento de esta investigación, daremos a conocer algunas conceptualizaciones de importancia para el estudio:

Hardware de cómputos, es el equipo físico utilizado para las actividades de entrada, procesamiento y salida de un sistema de información. Consta de lo siguiente: varios dispositivos de entrada, salida y almacenamiento, y medios físicos para enlazar los dispositivos.

Software. Es el conjunto de programas que ejecuta una computadora. Estos programas contienen instrucciones u órdenes, las cuales se encuentran codificadas en un lenguaje que la computadora puede comprender. Daniel Cohen y Enrique Asin (2005).

Esta tecnologías representan recursos que se pueden compartir a través de la organización y constituyen la Infraestructura de tecnología de la información (TI), esta da la base o la plataforma sobre la cual la empresa puede construir su sistemas específicos de información.

Sistema de Gestión de la seguridad de la Información (SGSI) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001. El término se denomina en inglés "Information Security Management System" (ISMS).[1]

"El concepto clave de un SGSI es para una organización del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información".[2]

Negocios en Línea. "Uso de la internet y la tecnología digital para ejecutar todos los procesos de negocios de las empresas. Incluye el comercio electrónico como un proceso para la administración de la empresa y para la coordinación con proveedores y otros socios de negocios".[3]

Comercio Electrónico. *Según Jeffrey Rayport*, el comercio electrónico se puede definir como intercambios mediados por la tecnología entre diversas partes (individuos, organizaciones, o ambos) así como actividades electrónicas dentro y entre organizaciones que facilitan esos intercambios.

Pirata, Hackers y Crackers. Estos son tres grandes grupos de individuos que actúan del lado oscuro de la tecnología, son considerados como criminales de alta tecnología aunque sus actividades son diferentes. La práctica de los hackers implica un reto intelectual, ya que su intención es introducirse en determinados sistema descifrando códigos y claves sin destruir alterar la información que se encuentra.

---

[1] Wikipedia, Enciclopedia Libre, http://es.wikipedia.org/wiki/Sistema_de_Gesti%C3%B3n_de_la_Seguridad_de_la_Informaci%C3%B3n

[2,3] *Laudon, K. & Laudon, J. 2004, Sistema de información Gerencial, editorial Pearson, Prenticel Hall, p. 399 y 448.*

"La existencia de estos personajes y su habilidad para introducirse en diversos sistemas es una preocupación constante de las compañías que de alguna manera están relacionadas con internet, pues de no contar con excelentes murallas de fuego (firewalls) y algoritmos de encriptación de datos, la información crítica se encuentra a merced de hackers y crackers. Por lo tanto, ha surgido un reto para los administradores de información. Contar con mecanismos de protección en contra de estos individuos que se dedican a cometer delitos tecnológicos." *Daniel Cohen y Enrique Asin (2005).*

La seguridad es un tema de suma importancia y actualmente de moda, sin embargo la Republica Dominicana aún se encuentra en dentro de la fase inicial de una pirámide de muchos peldaños. Las soluciones de seguridad tradicionales no son suficientes, por ejemplo en el 2010, los ataques sofisticados utilizaron tácticas combinadas para entrar en cientos de organizaciones.

Es conocido que las grandes potencias políticas y económicas del mundo están siendo atacadas por la vulnerabilidad que sufren sus sistemas de seguridad, por lo que es también una problemática que afecta a todas las instituciones que manejan información crítica, por lo que sus estructuras informáticas son blanco de ataques constantes.

El objetivo principal de esta propuesta de implementaciones consiste en conocer y analizar los componentes principales de los Sistemas de seguridad de infraestructura y mostrar el proceso de Implementación para ser aplicada a empresas del sector Bancario de nuestro país.

Los hallazgos de esta propuesta aportaran un valor agregado significativo, en el proceso de implementación de este tipo de ambiente tecnológico, ya que daremos a conocer algunas de las ventajas que aporta este tipo de sistema, además de servir de guía para el uso eficiente de estos, en este sector, como protección a sus más valiosas informaciones.

La limitante principal al elaborar esta propuesta, es que en el mercado bancario no encontramos fuentes sobre estudios posteriores sobre estos tipos de implementaciones, ya que las políticas que rigen la seguridad de la información en el sector bancario del país es hermética con relación a ofrecer datos al respecto. Esto por consiguiente es una de las limitantes que encontramos para realizar comparaciones precisas de estos sistemas.

En el desarrollo de esta investigación las informaciones están contenidas en tres capítulos:

En el capítulo I: Funcionalidad de los sistemas de infraestructura, se describe en qué consisten estos sistemas, sus componentes y funcionalidad.

En el capítulo II: Políticas generales de seguridad de infraestructura, se defines las políticas creadas para la aplicación, algunas amenazas que sufren estos sistemas y sus características.

En el capítulo II: Implementación del sistema de seguridad de Infraestructura, se describe el flujo y proceso de implementación de la aplicación.

La conclusión del proyecto explica que la importancia de estos sistema radica en el impacto de seguridad que proporcional a las herramientas de valor crítico para las empresas, su beneficio es incalculable en relación para aquellas no la poseen o cuyas aplicaciones son limitativas o pocos flexibles.

CAPITULO I

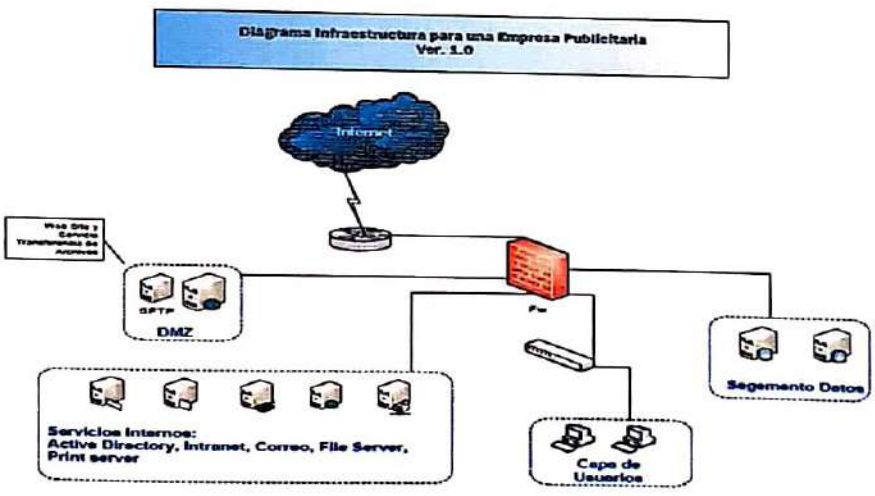
FUNCIONALIDAD DE LOS SISTEMAS DE INFRAESTRUCTURA

1.1. Sistema de Infraestructura

Tecnología de Información se define como el conjunto de dispositivos físicos y aplicaciones de Software que se requieren para operar toda la empresa. Sin embargo, la Infraestructura de TI también es un conjunto de servicios a lo largo y ancho de la empresa, presupuestados para la administración y que abarcan capacidades tanto humanas como técnicas. [4]

Las (TI) exigen continuas renovaciones en la infraestructura informática como consecuencia de las constantes innovaciones y mejoras que aparecen en el mercado. Por esta razón, existe el compromiso en las instituciones de actualizar sus soluciones a esa continua evolución.

Figura No 1. Modelo Infraestructura



Fuente: Autoría propia, 2013

[4] Laudon, K. & Laudon, J. 2004, *Sistema de información Gerencial, editorial Pearson, Prenticel Hall*

La infraestructura informática abarca elementos como: Redes, Líneas de comunicación, Telefonía, PCs, Servidores, Impresoras, Sistemas operativos, Servicios de correo, Web, Bases de datos, Mecanismos de seguridad informática esta a su vez esta segmentada por diversos procesos en los que podemos citar, Planificación, Proyectos de Mejora, Monitoreo, Gestión de Incidentes, Gestión de Problemas, Gestión de Cambios, Gestión de Configuración, Gestión de Parches, entre otros.

Un ejemplo donde se puede presentar la importancia de una infraestructura robusta, es el caso del gusano Stuxnet, fue la primera muestra de arma cibernética cuyo uso llegó al conocimiento del gran público. Los autores de Stuxnet abrieron la caja de Pandora, mostrando a todo el mundo cuan efectivos pueden ser los ataques contra las unidades vitales de infraestructura industrial. Ya podremos imaginar la consecuencia de un tipo de ataque de este nivel.

Después del descubrimiento de Stuxnet, se encontraron también otros programas similares: Duqu, Flame y Gauss. Todos estos programas tienen algunos rasgos en común, pero sus objetivos, funcionalidades y fecha de creación son diferentes.

Sin embargo, estos no son los únicos ejemplares conocidos de programas ciberespías y de ciber sabotaje. Las armas cibernéticas se han convertido en una triste realidad y han pasado a formar parte del arsenal de algunos países. Si antes los países, para defender sus intereses geopolíticos, hacían uso de medios diplomáticos, económicos y militares, ahora para realizar determinadas tareas, en vez de aviones, misiles, tanques o navíos pueden usar programas maliciosos especialmente diseñados. Su uso, en caso de que el ataque tenga éxito, permite lograr los mismos resultados, pero de una forma mucho más barata, silenciosa y anónima. El reciente caso de Wiper ha confirmado una vez más la efectividad de este método.

Hoy en día podemos decir que para conservar su soberanía, un país no sólo debe hacer respetar sus intereses socioeconómicos y políticos, sino también cuidar escrupulosamente su espacio informático. Y una de las tareas de primer plano es controlar los sistemas informáticos de importancia crítica para el estado.

1.2. Componentes de la Infraestructura tecnológica.

1.2.1 Equipo de Cómputo

Se entiende por éste a cualquier elemento de la infraestructura tecnológica e informática (hardware), software, accesorio, periférico, de telecomunicaciones y relacionado con cualquiera de estos.

1.2.2 Sistema de Cómputo

Un Sistema de Cómputo es un conjunto de elementos electrónicos que están interactuando constantemente entre sí, (*hardware*) para procesar y almacenar información de acuerdo a una serie de instrucciones (*software*).

1.2.3 Red Local

Es una herramienta de tecnología soportada por diferentes medios de comunicación como fibra óptica, ondas de radio y cables de cobre (UTP), mismos que proveen diferentes anchos de banda para su funcionamiento. Junto con estos medios se cuenta con equipo de conectividad como Switches, convertidores de medios y puntos de acceso que deben contar con una correcta instalación y protección eléctrica para su operación continua.

A través de esta red se proveen diferentes servicios a la comunidad universitaria, tales como acceso a Internet, correo electrónico, sistemas institucionales, videoconferencias, entre otros.

1.2.4 Red Inalámbrica

Éste término suele utilizarse más para referirse a aquellas redes de telecomunicaciones en donde la interconexión entre nodos es implementada sin utilizar cables. Las redes inalámbricas de telecomunicaciones son generalmente implementadas con algún tipo de sistema de transmisión de información que usa ondas electromagnéticas, como las ondas de radio.

Las redes inalámbricas encuentran su definición en el conjunto de estándares basados en las especificaciones IEEE 802.11x, y son conocidas por diferentes nombres como WLAN (Wireless Local Area Network) o WIFI, Wi-fi, WiFi (Wireless Fidelity).

Este tipo de redes permiten conectar dispositivos electrónicos entre sí sin necesidad de utilizar un cable. La tecnología alámbrica es un medio que permite la conectividad con un rango de seguridad y velocidad mucho mejor, y las redes inalámbricas son dependientes de la primera.

1.3. Riesgos en Infraestructuras

1.3.1 Anatomía del ataque

Los blancos más peligrosos para los ataques cibernéticos son, en primer lugar, los Sistemas informáticos de infraestructuras críticas que controlan las unidades de importancia clave. El que estas unidades queden fuera de servicio, puede crear caos y catástrofes. Nuestras vidas dependen de una forma u otra de estos sistemas. Estos traen calefacción a nuestros hogares, abastecen el agua y la electricidad, brindan la señal de radio, dirigen el tráfico de vehículos, controlan la extracción de recursos y los procesos de producción en las fábricas y factorías.[5]

---

[5] Kaspersky Lab, 2012, http://www.viruslist.com/sp/analysis?pubid=207271189

Aparte de las unidades industriales, existe una gran cantidad de organizaciones para las cuales el acceso no autorizado a la información puede convertirse en un serio problema: bancos, instituciones médicas, centros de investigación y empresas.

En los Sistemas informáticos de infraestructuras críticas, para controlar las instalaciones se usan aplicaciones, que por desgracia no están libres de errores y vulnerabilidades.

Para que el ataque cibernético sea efectivo, es necesario que el enemigo tenga la comprensión completa de la estructura interna de la instalación a atacar. Por esta razón, los ataques suelen constar de varias etapas.

En la primera etapa de exploración se recopila información sobre la topología interna de la red, los equipos y aplicaciones utilizadas, porque al enemigo le interesan sus detalles y características.

En esta etapa, no suelen lanzarse ataques contra los blancos principales, sino contra las compañías subsidiarias encargadas de la automatización (integradores de sistemas) ya que éstas, por lo general, tienen una actitud menos responsable ante la seguridad informática, pero al mismo tiempo manejan datos valiosos. Además, estas compañías pueden tener acceso autorizado a la red tecnológica del destino del ataque final, que el enemigo puede utilizar en las posteriores etapas del ataque.

En la etapa de recopilación de información también se pueden lanzar ataques contra compañías de servicio, socios de negocio, proveedores de equipos, etc.

En la segunda etapa se usa la información recolectada para hacer un análisis minucioso y se elige el vector de ataque más efectivo. Una vez encontrado, se determina qué vulnerabilidades del software hay que utilizar para penetrar el sistema y qué funcionalidades debe tener el código malicioso para alcanzar el objetivo necesario.

Después, si es posible, se compran aplicaciones y equipos similares a los atacados para hacer pruebas reales de los programas maliciosos, y al fin, se busca la forma de infiltrar el software malicioso en las instalaciones atacadas. Aquí, el espectro de posibilidades va desde métodos relativamente simples de ingeniería social hasta formas ultra tecnológicas de penetrar en los canales de comunicación.

1.3.2 Características de los Sistemas de Control

En el campo de la seguridad de los sistemas de infraestructura informática, hay dos peligrosísimos problemas. Se trata de los defectos de los modelos de seguridad desarrollados para los sistemas empresariales y de los defectos de los entornos en los que se ejecutan estos modelos.

Hasta hace poco, durante la creación de modelos de seguridad informática para instalaciones de las empresas, se creía que el aislamiento físico de la instalación era suficiente para protegerla. Como regla, el modelo de seguridad de estas instalaciones se basa en los principios de "security by obscurity" (seguridad por oscuridad) y "air gap" (aislamiento físico). Sin embargo, el incidente de Stuxnet mostró que estos principios ya no funcionan, y que este enfoque de seguridad es irremediablemente obsoleto.

Los Sistemas informáticos de infraestructuras críticas se caracterizan por la heterogeneidad de sus aplicaciones y hardware. Una red típica suele constar de servidores SCADA bajo Windows o Linux, servidores de sistemas de gestión de bases de datos (SQL Server u Oracle), un conjunto de controladores lógicos programables (PLC) de diferentes marcas, paneles de operador (HMI), sensores intelectuales y un canal de comunicación con sistemas ERP. Al mismo tiempo, según los resultados de las últimas investigaciones de DHS, cada red tecnológica tiene un promedio de 11 puntos de conexión directa con la red corporativa. [6]

---

[6] Kaspersky Lab, 2012, http://www.viruslist.com/sp/analysis?pubid=207271189

1.3.3 Diagnósticos de las vulnerabilidades

Al hacer una apreciación de las vulnerabilidades de los Sistemas informáticos de infraestructuras críticas, es necesario tener en cuenta su tiempo de explotación, que es de decenas de años. Y que hasta mediados de los años 2000 ni siquiera existía el término de "vulnerabilidad de aplicaciones" y que los problemas de seguridad simplemente no se consideraban durante la fabricación de estos sistemas[1].

La mayor parte de los sistemas de control de procesos tecnológicos que funcionan en el presente fueron creados sin tomar en consideración la posibilidad de ataques cibernéticos. Por ejemplo, la mayoría de los protocolos de intercambio de datos usados por SCADA y PLC no contemplan ningún tipo de autentificación y autorización. Esto hace que cualquier aparato que se conecta a la red tecnológica sea capaz de recibir y enviar instrucciones de control a cualquier otro dispositivo.

Otro problema serio es que debido al largo ciclo de vida de los Sistemas informáticos de infraestructuras críticas, la documentación normativa prohíbe la actualización e instalación de nuevo software en el sistema, o supone grandes dificultades administrativas y tecnológicas. Durante mucho tiempo los Sistemas informáticos de infraestructuras críticas prácticamente no publicaron actualizaciones de software. Al mismo tiempo, es de dominio público una gran cantidad de información sobre las vulnerabilidades de los controladores y los sistemas SCADA, las vulnerabilidades de los sistemas operativos, las bases de datos e incluso de los sensores inteligentes.

Tampoco contribuyen a mejorar la situación de la seguridad cibernética las compañías que producen SCADA y PLC. El archivo de noticias de ICS-CERT es una prueba tangible de que los fabricantes no prestan la atención debida a sus soluciones, tanto de software como de hardware.

Los nombres de usuarios y contraseñas predeterminados grabados en los PLC, las llaves SSH y SSL, la posibilidad de hacer ataques mediante desbordamiento de buffer, la posibilidad de sustituir componentes del sistema por otros maliciosos y la realización de ataques Dos y XSS son las vulnerabilidades descubiertas con más frecuencia[1].

Además, la mayoría de los vendedores incluyen medios de administración remota en sus complejos software-hardware, pero delegan su configuración a los integradores.

Por su parte, los integradores pueden prestar poca importancia a estas configuraciones y como resultado los Sistemas informáticos de infraestructuras críticas con frecuencia están expuestos a Internet con el nombre de usuario y contraseña predeterminados. En la red global existen sistemas de búsqueda especializados capaces de descubrir dispositivos cuyo acceso es posible con el nombre de usuario y contraseña predeterminados, o que no tienen ninguna contraseña. Una vez obtenida esta información, cualquier persona tiene la posibilidad de controlar el sistema de forma remota.

Partiendo de lo expuesto, podemos afirmar que los componentes de los modernos Sistemas informáticos de infraestructuras críticas pueden ser comprometidos, infectados, funcionar incorrectamente y poner fuera de funcionamiento los equipos, dar información incorrecta al operador e inducirlo a tomar decisiones equivocadas, lo que puede resultar en situaciones peligrosas.

Por supuesto, en cada instalación existen sistemas de prevención de accidentes. Pero estos sistemas están destinados a evitar accidentes provocados por factores fortuitos y pueden resultar inútiles contra un ataque dirigido.

---

7. [1] http://www.viruslist.com/sp/viruses/analysis?pubid=207271189

Como si esto fuera poco, la aspiración de efectividad económica provoca que la producción de medios de protección contra averías se distribuya entre varias compañías subsidiarias. Y cada una de ellas tiene la posibilidad de incluir funcionalidades ocultas en varios niveles, desde el software de control hasta el chip del microprocesador.

Por tradición, los productores de equipos y software han concentrado sus esfuerzos en la estabilidad y la tolerancia contra fallas de sus soluciones. Hasta hace poco este enfoque, sin duda, estaba justificado, pero ahora ha llegado el momento de prestar una seria atención a la seguridad informática, invitando a colaborar y hacer peritajes de sus productos a compañías especializadas.

De esta manera, hemos llegado a una situación en que, por una parte, algunos países ya cuentan con armas cibernéticas y, por otra parte, los sistemas informáticos vitales de los estados están expuestos a los ataques. Dependiendo del nivel de desarrollo de las tecnologías informáticas en el país y el grado de automatización de las instalaciones industriales en particular, atacarlos puede ser más o menos fácil, pero el ciberataque siempre es posible.

1.3.4 Confianza en los sistemas de infraestructuras

En el presente, se ha hecho patente la necesidad de crear soluciones capaces de garantizar una protección fiable a las instalaciones industriales vitales y a las demás instalaciones y organizaciones sensibles a la penetración y la filtración de información. No obstante, sin importar cuan bien funcionen estos sistemas, el uso en los Sistemas informáticos de infraestructuras críticas de sistemas operativos y software vulnerables no permite a los fabricantes de medios de defensa garantizar la seguridad del sistema. En el caso de instalaciones de importancia vital, estas garantías son imprescindibles.

Pero no hay que contar con que todos los desarrolladores de sistemas clave de infraestructura informática se lancen de inmediato a realizar revisiones y actualizaciones totales de todo el software que utilizan, ni que los directores de las empresas actualicen en ese mismo momento las soluciones instaladas. Y si tomamos en cuenta que el ciclo vital de estos sistemas se cuenta en décadas, se hace evidente que, según un escenario de evolución, la implementación de Sistemas informáticos de infraestructuras críticas necesitará realmente mucho tiempo.

Sin embargo, la solución global del problema de las vulnerabilidades no es la única solución capaz de garantizar la seguridad del funcionamiento de las instalaciones empresariales.

Las vulnerabilidades son brechas que los programas maliciosos pueden utilizar para penetrar en los sistemas. Cualquier componente de los Sistemas informáticos de infraestructuras criticas se puede infectar. Y el componente infectado puede ejecutar en la red tecnológica acciones maliciosas que pueden conducir a catástrofes y al mismo tiempo desinformar al operador.

En estas situaciones, el operador de un sistema de importancia vital se ve obligado a administrar procesos tecnológicos sin ninguna garantía de que la información que usa para tomar decisiones sea correcta. En esencia, este es uno de los problemas claves de la seguridad de sistemas, porque el precio de los errores en este tipo de instalaciones puede ser muy alto.

1.3.5 Sistema operativo seguro

Qué requisitos tiene que cumplir un medio de control de la infraestructura informática completamente seguro. El sistema operativo no debe basarse en un código ya existente, por eso debe ser desarrollado desde cero.

Para garantizar la seguridad, no debe contener errores y vulnerabilidades en el núcleo que controla el resto de los módulos del sistema. Como consecuencia, el núcleo debe verificarse por medios que no permitan la existencia de vulnerabilidades o códigos de doble propósito.

Por la misma razón, el núcleo debe contener un mínimo crítico de código, y por lo tanto, la cantidad máxima de código, incluyendo los controladores, debe ser controlada por el núcleo y ser manejado con los privilegios restringidos. Y por último, en este medio debe estar presente un poderoso y fiable sistema de protección que admita diferentes modelos de seguridad.

De conformidad con esto, estamos creando un sistema operativo propio, cuya peculiaridad fundamental es la absoluta imposibilidad de ejecutar funciones no declaradas.

Sólo basándose en un sistema operativo como éste se puede construir una solución que permita al operador no sólo ver lo que en realidad ocurre en la producción, sino también controlarla. Y esto sin importar quienes sean los fabricantes de sistemas operativos, bases de datos, SQL, Oracle, en concreto, sin importar su grado de protección o de si tienen vulnerabilidades. Es más, sin importar su grado de infección.

De hecho, estamos hablando de un sistema de protección inteligente contra averías de nueva generación. Un sistema de protección que tome en cuenta todo el complejo de índices de la empresa al mismo tiempo. Un sistema de seguridad que no permita averías como consecuencia de acciones incorrectas del analista, ni de los errores del software del sistema clave de infraestructura informática, ni de los ataques cibernéticos. Además, el sistema puede complementar los medios tradicionales de protección contra averías, lo que permite hacer un seguimiento de escenarios más complejos.[8]

Esta solución deberá integrarse en los sistemas clave de infraestructura informática ya existentes para protegerlos y garantizar la monitorización fidedigna, o tomarse en cuenta durante el diseño de nuevos sistemas clave de infraestructura informática. En ambos casos, garantizando la aplicación de principios de seguridad modernos.

---

[8] Kaspersky Lab, 2012, http://www.viruslist.com/sp/analysis?pubid=207271189

CAPITULO II

POLITICAS GENERALES DE SEGURIDAD DE INFRAESTRUCTURA

2.1. Definición de Política de Seguridad de Informática

Todas las empresas, grandes y pequeñas, necesitan una política de información. Los datos de la empresa son un recurso importante, y a usted no le agradara que los demás hagan con ellos lo que se les antoje. Es necesario contar con reglas sobre la manera en que se organizarán y mantendrán los datos, y quien tendrá autorización para verlos o modificarlos.

Un política de información, especifica las reglas de la organización para compartir, distribuir, adquirir, estandarizar, clasificar e inventariar la información. Una política de información establece procedimientos y responsabilidades específicos, que identifican cuales usuarios y unidades de la organización pueden compartir información.

Las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.[9]

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

---

[9] Ciro Dussan, 2006, http://www.unilibrecali.edu.co/entramado/images/stories/pdf_articulos/volumen2/Politicas_de_seguridad_informtica.pdf

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

2.1.1. Políticas de Seguridad informática

La seguridad informática o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.[10]

---

[10] Wikipedia, Enciclopedia Libre, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Según Cohen, D. & Asin, E. (2005), los sistema de información se pueden definir técnicamente como un conjunto de componentes interrelacionados que funcionan con el fin de apoyar las actividades de una empresa o negocio.

Para estos autores, los sistemas de información no son más que solo computadoras. El uso eficiente de estos sistemas requiere entender los aspectos de organización, administración y tecnología de la información que les dan forma.[11]

Todos los sistemas de información se pueden describir como soluciones de organización y administración a los retos planteados por el entorno que ayudaran a crear valor para la empresa.

2.2. La amenaza informática del futuro

Si en un momento el objetivo de los ataques fue cambiar las plataformas tecnológicas ahora las tendencias cibercriminales indican que la nueva modalidad es manipular los certificados que contienen la información digital. El área semántica, era reservada para los humanos, se convirtió ahora en el núcleo de los ataques debido a la evolución de la Web 2.0 y las redes sociales, factores que llevaron al nacimiento de la generación 3.0.[12]

---

[11], Cohen, D. & Asin, E., 2005, Sistema de Información para Negocios, 4ta, edición, MacGrawHill, México., Pág. 6

[12] Wikipedia, Enciclopedia Libre, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

- Se puede afirmar que "la Web 3.0 otorga contenidos y significados de manera tal que pueden ser comprendidos por las computadoras, las cuales -por medio de técnicas de inteligencia artificial- son capaces de emular y mejorar la obtención de conocimiento, hasta el momento reservada a las personas".
- Es decir, se trata de dotar de significado a las páginas Web, y de ahí el nombre de Web semántica o Sociedad del Conocimiento, como evolución de la ya pasada Sociedad de la Información.

En este sentido, las amenazas informáticas que viene en el futuro ya no son con la inclusión de troyanos en los sistemas o softwares espías, sino con el hecho de que los ataques se han profesionalizado y manipulan el significado del contenido virtual.

- La Web 3.0, basada en conceptos como elaborar, compartir y significar, está representando un desafío para los hackers que ya no utilizan las plataformas convencionales de ataque, sino que optan por modificar los significados del contenido digital, provocando así la confusión lógica del usuario y permitiendo de este modo la intrusión en los sistemas, la amenaza ya no solicita la clave de homebanking del desprevenido usuario, sino que directamente modifica el balance de la cuenta, asustando al internauta y, a partir de allí, sí efectuar el robo del capital.

2.3. Políticas Generales de seguridad

Una política de seguridad para que sea efectiva, necesita contar con elementos indispensables que apoyen este proceso: La cultura organizacional, las herramientas y el monitoreo. Esto involucra la participación directa y comprometida de las personas, el diseño de planes de capacitación constante a los usuarios. La disponibilidad de recursos financieros, técnicos y tecnológicos es fundamental y sobre todo actividades de control y retroalimentación que diagnostiquen e identifiquen puntos débiles para fortalecerlos siguiendo las mejores prácticas.

Las organizaciones pueden definir unos ámbitos básicos o esenciales en donde empezar a implementar políticas de seguridad; entre los más comunes encontramos:

- Seguridad física: acceso físico, estructura del edificio, centro de datos.

- Seguridad de la red corporativa: configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, disciplina operativa, gestión de cambios, desarrollo de aplicaciones.

- Seguridad de usuarios: composición de claves, seguridad en estaciones de trabajo, formación y creación de conciencia.

- Seguridad de datos: criptografía, clasificación, privilegios, copias de seguridad y recuperación, antivirus, plan de contingencia.

- Auditoria de seguridad: análisis de riesgo, revisiones periódicas, visitas técnicas, monitoreo y auditoria. Aspectos legales: prácticas personales, contratos y acuerdos comerciales.[13]

2.3.1 Características Generales

a) Cuentas de Usuarios

Es la cuenta que constituye la principal vía de acceso a los sistemas de información que posee la empresa; estas cuentas aíslan al usuario del entorno, impidiendo que pueda dañar al sistema o a otros usuarios, y permitiendo a su vez que pueda personalizar su entorno sin que esto afecte a otros.

---

[13].http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT

Cada persona que acceda al sistema debe tener una sola cuenta de usuario. Esto permite realizar seguimiento y control, evita que interfieran las configuraciones de distintos usuarios o acceder al buzón de correo de otro usuario.

b) Detección de intrusos

Los sistemas computarizados y aplicaciones están en permanente evolución, por tal razón pueden surgir nuevos puntos vulnerables. A pesar de los avances en los sistemas de seguridad, los usuarios no autorizados con herramientas muy sofisticadas tienen grandes posibilidades de acceso a las redes, sistemas o sitios de las organizaciones e interrumpir sus operaciones.

Actualmente, existen más de 30.000 sitios en internet orientados a la piratería o intrusión de redes, los cuales ofrecen programas de fácil descarga y acceso que han dejados las puertas abiertas para nuevos ataques.

c) Privacidad en la Red

Las comunicaciones son la base de los negocios modernos, pues sin las mismas ninguna empresa podría sobrevivir. Por tal razón, es necesario que las organizaciones mantengan sus servidores, datos e instalaciones lejos de los hackers y piratas informáticos.

La temática de la privacidad de las redes ha ido cobrando, desde hace más de una década, un lugar bien importante en el entorno del desarrollo de la informática, ya que las empresas se sienten amenazadas por el crimen informático y busca incansablemente tecnologías que las protejan del mismo, para lo cual destinan partidas en sus presupuestos para fortalecer la seguridad de la información y de las comunicaciones.

d) Virus y Antivirus

Antes de profundizar en este tema, debemos aclarar que los virus de computadoras son simplemente programas, y como tales hechos por programadores. Son programas que debido a sus características particulares son especiales. Para hacer un virus de computadora no se requiere capacitación especial, ni una genialidad significativa, sino conocimientos de lenguajes de programación para el público en general y algunos conocimientos puntuales sobre el ambiente de programación y arquitectura de las PC's.

Un virus es simplemente un programa, una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco.

Un virus es una porción de código ejecutable, que tiene la habilidad única de reproducirse. Se adhieren a cualquier tipo de archivo y se diseminan con los archivos que se copian y envían de persona a persona.

2.3.2 Clasificación

A continuación esbozamos una clasificación que tiende a catalogar los virus actuales, sin intentar crear una clasificación académica, sino una orientación en cuanto a funcionalidad de los virus:

- **Virus de Macros/Código Fuente:** Se adjuntan a los programas fuente de los usuarios y, a las macros utilizadas por: Procesadores de Palabras (Word, Works, WordPerfect), Hoja de Cálculo (Excell, Quattro, Lotus).
- **Virus Mutantes:** Son los que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados (NATAS o SATÁN, Miguel Angel, por mencionar algunos).

- **Gusanos:** Son programas que se reproducen a sí mismo y no requieren de un anfitrión, pues se "arrastran" por todo el sistema sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posesionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borradas los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdidas de datos.
- **Caballos de Troya:** Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones.
- **Bomba de Tiempo:** Son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables con tipo COM o EXE. En espera de una fecha o una hora determinadas para "explotar".

Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que las contiene.

- **Autorreplicables:** Son los virus que realizan las funciones más parecidas a los virus biológicos, ya que se auto reproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u horas programadas o cada determinado tiempo, contado a partir de su última ejecución, o simplemente al "sentir" que se les trata de detectar. Un ejemplo de estos es el virus del viernes 13, que se ejecuta en esa fecha o se borra (junto con los programas infectados), evitando así ser detectado.
- **Infectores del área de carga inicial:** Infectan los diskettes o el disco duro, alojándose inmediatamente en el área de carga. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo.

- **Infectores del sistema:** Se introducen en los programas del sistema, por ejemplo COMMAND.COM y otros se alojan como residentes en memoria. Los comandos del Sistema Operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el Sistema Operativo y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver sus carpetas (también llamadas: folders, subdirectorios, directorios).
- **Infectores de programas ejecutables:** Estos son los virus más peligrosos porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de palabras). La infección se realiza al ejecutar el programa que contiene al virus, que en ese momento se posesiona en la memoria de la computadora y a partir de entonces infectará todos los programas cuyo tipo sea EXE o COM, en el instante de ejecutarlos, para invadirlos autocopiándose en ellos.[14]

[14]. http://codechoco.gov.co/files/POLITICAS_INFORMATICAS_CODECHOCO.pdf

CAPITULO III
IMPLEMENTACION DEL SISTEMA DE SEGURIDAD INFRAESTRUCTURA

3.1. Descripción del Sistema (Remesas)

Luego de ver evaluado los conceptos y las terminologías que contempla una infraestructura, podemos dar inicio a lo que será nuestro sistema de Monitoreo de los pagos recibidos del exterior (Remesas) Fuente: *Economy Weblog.*[15].

Se denominan remesas a los envíos de dinero que envían los emigrantes a sus países de origen. Lo normal es que este dinero proceda de los sueldos y salarios que cobran los emigrantes por su trabajo en el país de destino. Los envíos se originan, por tanto, como consecuencia de los lazos familiares, de obligación y afecto entre los inmigrantes y personas que han dejado en su país de origen.

La importancia de las remesas estriba en que se dirige a las capas pobres de los países pobres. Un reciente estudio sobre once países indica que la repercusión de las remesas en términos de reducir la pobreza de la población en su conjunto advierte que el 50% o más de las personas de los hogares receptores se encontrarían bajo la línea de pobreza si no contaran con el aporte de tales transferencias. Las remesas, con frecuencia, benefician a regiones y comunidades donde no llegan las inversiones extranjeras o los programas de ayuda oficial al desarrollo

En la actualidad los flujos mundiales de remesas casi duplican las cantidades que se pagan en concepto de ayuda al desarrollo y, equivalen a más de las tres cuartas partes de la inversión extranjera directa.

[15] *Economy Weblog.*

3.2. Aspectos generales de diseño

1. El desarrollo del requerimiento implica un módulo separado de Monitoring el cual tendrá sus propias estructuras (tablas de base de datos), adicional compartirá estructuras con el sistema del Core del banco cuando sea necesario.

2. La autenticación de la funcionalidad desarrollada a la medida será utilizando usuarios previamente creados en Monitoring. Lo anterior implica, que la administración de la seguridad será realizada Directory de la empresa.

3. Se identificará el área de trabajo de un usuario según el grupo de trabajo al que esté identificado en la herramienta Monitoring. Si un usuario pertenece a todos los grupos de trabajo podrá completar, verificar y liberar transferencias.

4. Las búsquedas serán sobre los campos mapeados contra la trama de Monitoring.

5. La contingencia debe acordarse en conjunto con la empresa, la intención es, velar por la continuidad en los servicios.

3.3 Procedimiento de Ejecución

3.3.1. Captura de Archivos

a) proceso

1. Los archivos que contienen los mensajes Remesas entrantes pueden estar ubicados en varias carpetas fuentes, por lo tanto esto debe ser posible configurar N rutas fuente de archivos y por cada ruta fuente se debe configurar su ruta destino. Cada mensaje Remesas procesado de una carpeta fuente debe ser entregado en la carpeta destino configurada.

2. Los archivos que contienen los mensajes Remesas poseen una extensión específica por carpeta la cual es configurable y el proceso buscará los archivos únicamente con la extensión configurada en cada carpeta fuente.

3. Se asume que no existe ningún proceso concurrente el cual procese los archivos que contienen los mensajes Remesas y pueda ocasionar problemas con la lectura de los mismos.

4. Una vez procesados los mensajes Remesas contenidos en un archivo, este último debe eliminarse de la carpeta fuente y ser trasladado a la carpeta de archivos procesados. Esta carpeta debe ser configurable por carpeta fuente, al igual que se hace con la carpeta destino.

5. Los nombres de los archivos que se trasladan a la carpeta de "Archivos procesados" podría ser renombrados, esto debe ser configurable mediante el establecimiento de sufijos, prefijos y numeración consecutiva.

6. Cada vez que se leen los archivos se genera un log tipo bitácora donde se puedan dar seguimiento de las lecturas correctas y fallidas de los archivos.

7. Cuando un archivo no pueda ser leído se dejará en la carpeta fuente y se intentará leerlo N veces (configurable), luego de pasados los intentos se pasará el archivo a la carpeta de archivos fallidos, la cual es configurable por cada carpeta fuente.

3.3.2. Procesamiento de Archivos

1. El contenido del mensaje Remesas llegará completo a la Base de datos Intermedia, el mapeo de los datos que llegarán a la Base de datos de Monitoring será configurable.

2. Se asumirá que un mensaje Remesa está incompleto cuando el número de cuenta no exista en la base de datos del sistema Monitoring. En caso de que ocurra esto, el mensaje si se ingresará en la base de datos pero será marcado como incompleto.

3. Debe existir una interfaz de usuario donde se puedan consultar los mensajes incompletos y de manera manual permitir completar el número de cuenta por un usuario del área de cumplimiento, una vez completado el mensaje debe ser marcada como completo.

4. Para los mensajes en los que se determine que la cuenta está incompleta, permanecerán de forma indefinida esperando ser completados manualmente por el área de cumplimiento.

5. Solo las mensajes marcados como completos serán evaluados contra las lista OFAC y seguidamente contra las reglas configuradas en Monitoring para tal caso.

6. Los mensajes REMESAS se identificarán de manera única por medio del Tag 20 (Ejemplo: 20:007505327853) perteneciente al cuerpo de un mensaje REMESAS.

3.3.3. Verificación Lista OFAC

1. Una vez que los mensajes ingresan como transacciones en una base de datos intermedia y están completos se procederá primeramente a hacer la verificación con OFAC utilizando el nombre del cliente. El resultado que retorne OFAC será registrado en la base de datos.

2. El proceso se quedará esperando indefinidamente la respuesta de OFAC en caso de que el servicio Web no responda.

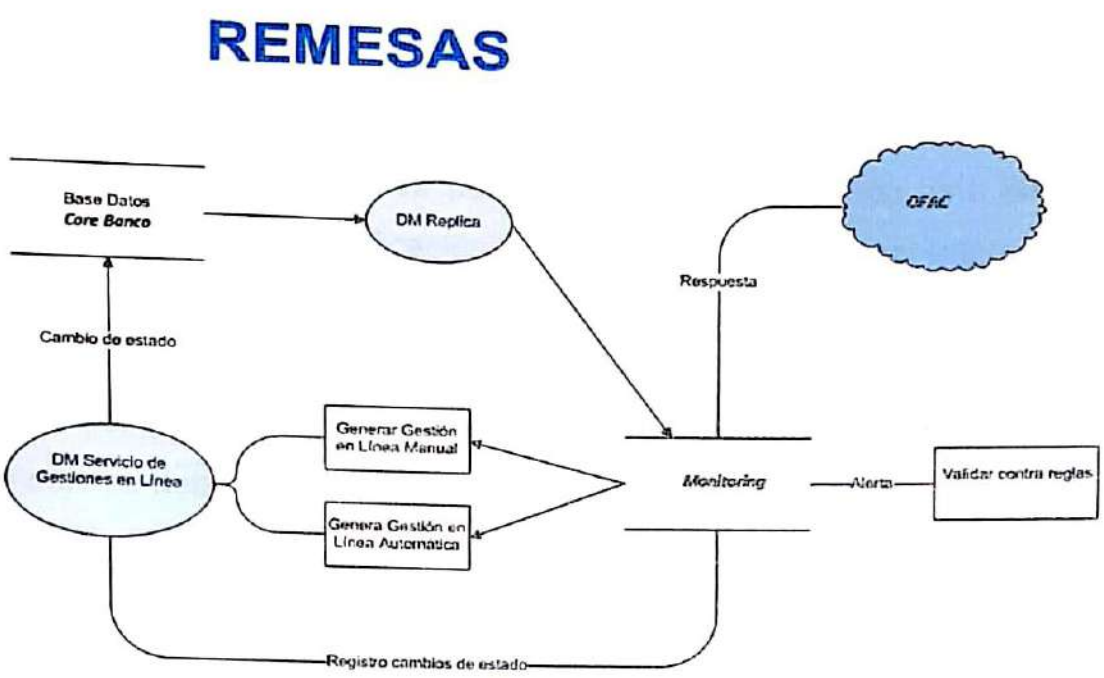
3. La verificación contra OFAC se realiza con las siguientes instrucciones:

    b. Crear el XML de consulta rellenando únicamente el valor de last_name con el nombre completo.

    c. Si el last_name está con el nombre completo el campo first_name deberá tener como valor "Null"

    d. Todos los demás campos del XML pueden quedar vacíos o no estar presentes en la consulta contra listas OFAC.

Figura No. 2. Esquema Proceso de Remesas



Fuente: *Autor 2013*

3.3.4. Evaluación de Transacciones

1. Para evaluar los mensajes Remesas una vez ingresados en Monitoring como transacciones el usuario debe crear estrategias, las cuales tendrán las reglas que se desean aplicar a los mensajes REMESAS.

2. Por cada carpeta definida como fuente debe existir la posibilidad de asignar una estrategia. Las reglas pertenecientes a estas estrategias serán las que se utilizarán para evaluar los mensajes pertenecientes a los archivos que existan en la carpeta.

3. Las transacciones que ingresen a Monitoring son evaluadas por todas las reglas configuradas.

4. Cuando una transacción está marcada como alertada por alguna de las reglas de la estrategia configurada para la carpeta fuente debe ser validada primeramente por el área de cumplimiento la cual determinará de manera manual si se libera o no.

5. Si la transacción es liberada por el área de investigación esta pasará a un segundo proceso de verificación por parte de usuarios de Internacional, los cuales deciden de manera manual si una transacción se debe liberar o no.

6. Debe existir una opción que permita enviar a imprimir un mensaje Remesas, el mensaje se debe imprimir tal y como se presenta en el archivo original.

7. Una transacción que es alertada y pasada a verificación por parte del área de cumplimiento permanece indefinidamente retenida hasta que se libere manualmente.

8. A través de configuración se indicará cuáles son los grupos de trabajo que tienen la funcionalidad de liberar o verificar las transacciones alertadas.

3.3.5. Entrega de Archivos

1. Una vez que las transacciones pasaron el proceso de verificación se debe generar el archivo con el/los mensaje(s) Remesas correspondientes.
2. El proceso verificará cuáles transacciones están listas para ser entregadas y creará un archivo con los mensajes REMESAS que encuentre. Un archivo podrá contener uno o más mensajes REMESAS liberados.
3. Los archivos entregados serán los archivos modificados y se crearán en la carpeta destino configurado. Cada mensaje REMESAS procesado proveniente de un archivo, se entregará en la carpeta destino configurada para su carpeta fuente.

4. El nombre de estos archivos entregados podrían contener un nombre y un consecutivo específico, el cual deberá ser configurable.
5. La entrega de los archivos de entrada deben cumplir con especificaciones del Core. Cada mensaje contenido en un archivo debe estar estructurado de esta forma: (***Hex 01*** + ***ACK*** + ***MensajeSWIFT*** + ***Hex 03*** + ***Blancos***,) donde cada valor tiene su significado como se muestra en la tabla siguiente:

Tabla No. 1. Especificaciones de Core.

CAMPO	DESCRIPCION
Hex 01	Hexadecimal 01
ACK	Mensajes de acuse de recibo
MensajeSWIFT	Contenido completo de un mensaje SWIFT
Hex03	Hexadecimal 03
Blanco en bloques fijos de bytes	Secuencia de espacio en blanco para completar el mensaje

Fuente: *Autoría Propia 2013*

El tamaño de los archivos varía dependiendo su tamaño, si es menor a 512 byte el archivo debe contener 512 byte, para saber el tamaño de cada mensaje, hay que mirar cuanto ocupa el mensaje (desde el carácter Hex 01 hasta el 03) y llevarlo al siguiente múltiplo de 512 bytes, si sobrepasa los 512 bytes lo llevamos a 1024 bytes, así sucesivamente incrementando siempre en 512 bytes.

Los archivos de entrada que se entregan en la carpeta fuente del componente desarrollado para la Institución por defecto contienen los caracteres especiales hexadecimal y los espacios en blanco para completar los bloques.

3.3.6. Mensajes 103 para remesas

A continuación se describe el procesamiento para aquellos mensajes SWIFT que deben ser interpretados como remesas.

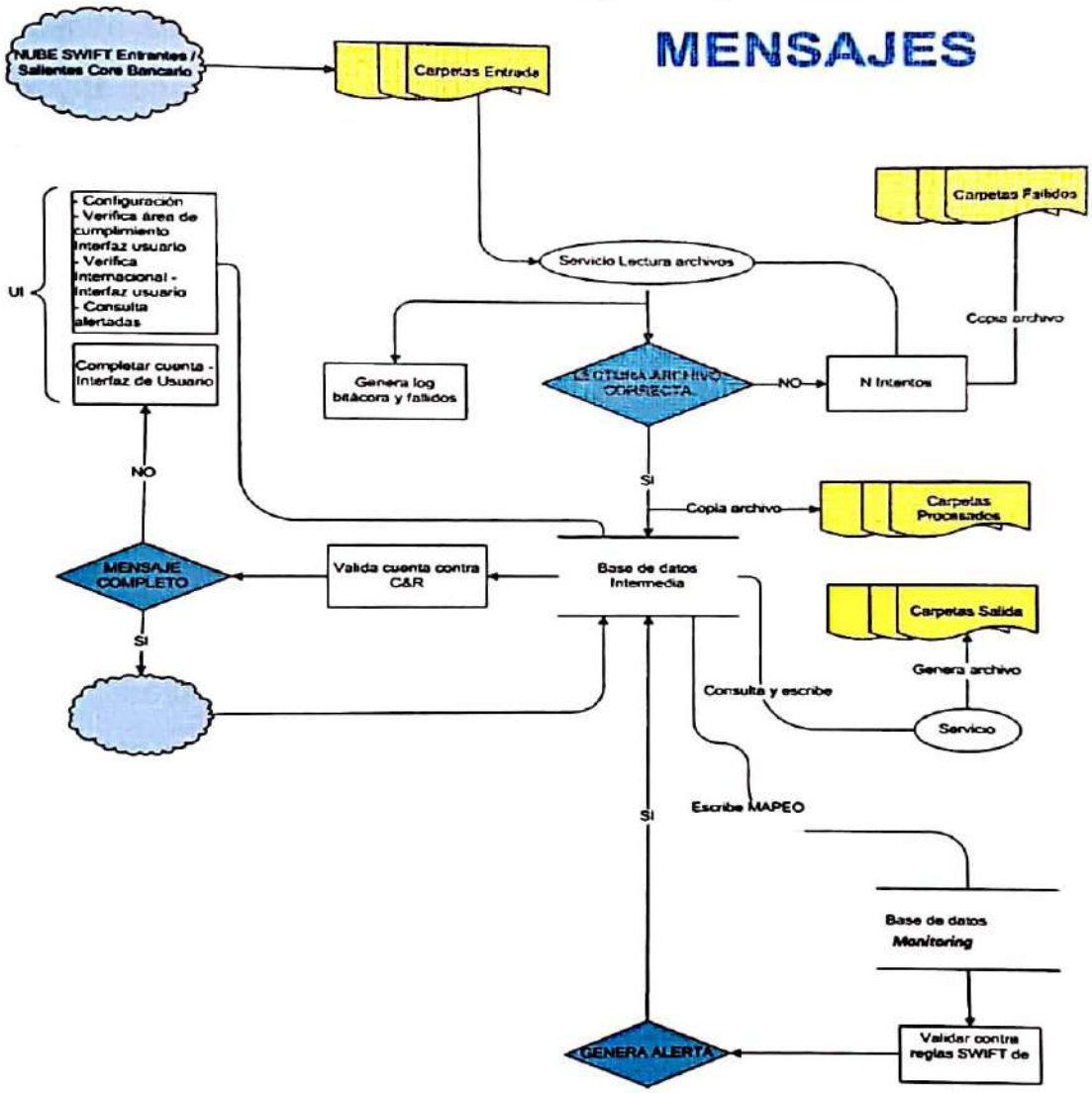
1. Toda remesa tiene en el tag 72 el string "*/REC/REMESAS /*' ó *"/TRABEX/*'.
2. Toda remesa debe validarse contra reglas y OFAC.
3. Si en el tag 59 surge del string "IDENT." Se asume que lo que sigue es una identificación por lo tanto no debe aplicarse validación de cuenta.
4. Si en el tag 59 no se encuentra en el string "IDENT." Se asume que lo que sigue es una cuenta por lo tanto debe aplicarse validación de cuenta siguiendo las instrucciones indicadas en el punto 5.
5. Solo aplica para mensajes 103 y 202
6. Debe existir parámetros de configuración en caso de que el servicio web de OFAC no responda. Un parámetro que permita desactivar la validación contra OFAC y otro parámetro que permita configurar el tiempo expresado en minutos que un mensaje SWIFT espera después de su primer verificación fallida contra OFAC para seguir su flujo normal. Es decir, si la validación contra OFAC falla en su primer intento el mensaje quedará N minutos intentando nuevamente obtener respuesta de OFAC, si después de transcurrido ese tiempo no recibe respuesta el mensaje sigue su flujo normal.
7. El nombre de los archivos no puede contener mensajes en blanco.
8. El nombre de los archivos no puede sobrepasar los 35 caracteres.
9. Una vez que las transacciones pasaron el proceso de verificación se debe generar el archivo con el/los mensaje(s) SWIFT correspondientes.

10. El proceso verificará cuáles transacciones están listas para ser entregadas y creará un archivo con los mensajes SWIFT que encuentre.

11. Los archivos entregados serán los archivos modificados y se crearán en la carpeta destino configurado. Cada mensaje SWIFT procesado proveniente de un archivo, se entregará en la carpeta destino configurada para su carpeta fuente.

Este procedimiento lo podemos observar en la figura No. 2 que mostramos a continuación.

Figura No. 3. Flujo de procesos Mensajes 103 para remesas



Fuente: *Autoría Propia 2013*

3.3.7. Factores de Riesgos

La definición de los puntajes en el "Riesgo de Transacciones" es algo dependiente a cada banco. Es decir, cada banco puede generar su propia tabla de "riesgo" en la que dependiendo de sus propios conocimientos y experiencia, pueden calificar una transacción.

Por ejemplo pueden decidir que las transacciones con montos en dólares mayores a 200 son de "alto riesgo", por tanto, pueden definir una condición para que cuando se realice una transacción con un Monto_Dolar superior a los $200, se le asigne un puntaje de "50 puntos" a la transacción. Si por otro lado, saben que una transacción realizada tiene un valor de entre $150 y $200 no representa un riego tan alto como el anterior, pueden definir una condición para ese campo con un puntaje de "30 puntos" y así con los demás campos de la transacción que deseen. Al final, Monitoring desplegará en el campo "Score" la sumatoria de estos puntajes para cada transacción.

Una recomendación o mejor prácticas es realizar una tabla que tenga un valor de puntaje máximo, siendo este valor el nivel de más alto riesgo que puede tener una transacción.

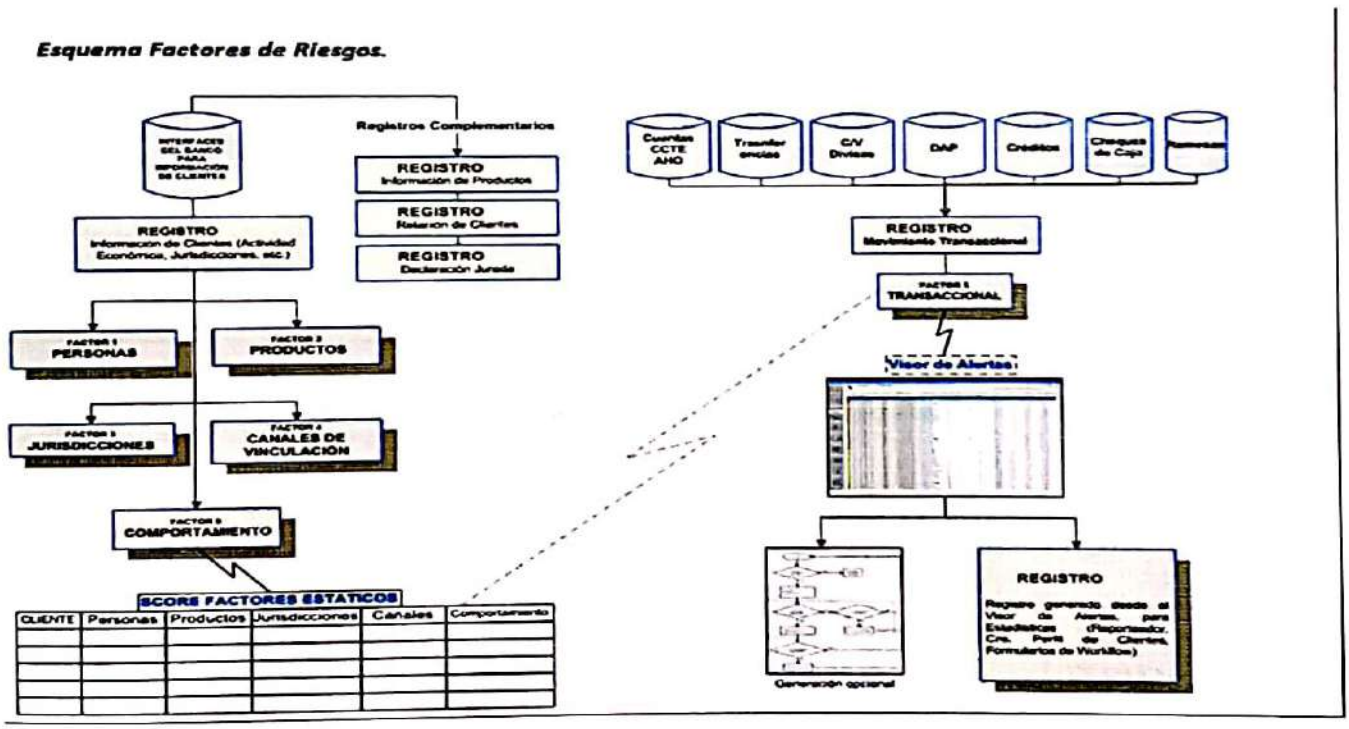
Es decir, si una transacción tiene un "Score" por ejemplo de 100 puntos, significa que esta transacción es del más alto riesgo (si éste es el puntaje máximo), y para llegar a tener este valor de 100 puntos, sería porque la transacción calificó en cada uno de los parámetros establecidos.

A manera de ejemplo:

Una transacción realizada con un Codigo_Transaccion = '416', con Punto de Entrada = '510', su Forma_Pago es '152', y el Monto_Dolar de la transacción fue de '1300' y se tienen definidas las siguientes condiciones para el "Riesgo de Transacciones" :

- Codigo_Transaccion	=	'416'	40 puntos
- Punto_Entrada	=	'510'	20 puntos
- Forma_Pago	>	'150'	20 puntos
- Monto_Dolar	>=	'1000'	20 puntos
TOTAL:			**100 puntos**

Figura. No. 4. Esquema Factores de Riesgos



Fuente: *Monitor 2013*

Tabla No. 2. Mapeo de campos de la remesa con Monitoring.

Consecutivo	Nombre Campo	Tipo y tamaño	Descripción	Atributo Campo
1	Id_Transaccion	numeric(18,0)	Identificador de la transacción	
2	Codigo_Transaccion	varchar(10)	Código de la transacción	TIPO_TRANSACCION
3	Fecha_Hora	datetime(8)	Fecha y hora en que se realiza la transacción	FECHA_INSERCION
4	Numero_Cliente	varchar(20)	Número identificador del cliente	COD_CLIENTE_ORDENANTE
5	Numero_Documento	varchar(50)	Número de referencia de la transacción	NUMERO_REMESA
6	Referencia	varchar(50)	Referencia complementaria de la transacción	CODIGO_REMESADOR
7	Monto_Local	float(8)	Monto de la transacción en moneda local	MONTO_REMESA
8	Pais_Originador	varchar(50)	País originador de la transacción	PAIS_ORDENANTE
9	Beneficiario	varchar(50)	Persona o cuenta beneficiaria de la transacción	NOMBRE_BENEFICIARIO
10	Pais	varchar(10)	País en el que se origina la transacciones	PAIS_BENEFICIARIO
11	Codigo_Sucursal	varchar(10)	Código de la sucursal en la que se realiza la transacción	SUCURSAL
12	Detalle_Transaccion	varchar(500)	Detalle de la transacción	NOTA
13	Id_Cajero	varchar(10)	Identificador del Cajero que procesa la transacción	TERMINAL_CAJERO

Fuente: *Autoría Propia, 2013*

Tabla No. 3. Descripción De Hardware y Software.

COMPONENTES	DESCRIPCION	
Rack Mount Server: **Modelos:** **DELL PE-R710** **HP DL380 G6,**	General	Servidor Tipo Rack Mount.
	Procesadores .	2 - Quad-Core Intel Xeon X5570 Processors.
	Memoria	12GB RAM, (6 X 2GB), DDR3 Dual Rank 1333Mhz.
	Discos	5 Discos 146GB SAS 15K 2.5" (2 en Raid 1, 3 en Raid 5).
	Bahías para Discos	1 - Cage 8 x 2.5" Hard Drive Option.
	Controladora RAID	SAS RAID (RAID1,5) Controller 2x4 Connectors, Internal, PCIe 512MB Cache.
	Interface de Red	1 - Cuatro Puertos Integrados Gigabit Ethernet NIC con failover y load balancing; TOE (TCPIP Offload Engine)
	Administración	Incluir Puerto de Administración.
	Ventiladores	Full Redundantes.
	Fuente de Alimentación	Full Redundante.
	Unidad Óptica	1 - DVD +/-RW, SATA, Interno.
	Tamaño	2U Rack Server with mounting rails included.
	2 HBA 8GB	Qlogic QLA 2640, 1P-PCI-X 4GB FC
	2 DAT 140	DAT 140 con un enclosure externo de 1U
	Garantía y Soporte	

Fuente: *Autoría Propia, 2013*

Tabla No. 4. Descripción Servidor Base de Datos.

COMPONENTES	
Hardware	
Procesador	2 Intel Xeon Quad Core 2.0 GHz o superior, 64 bits
Memoria RAM	32 GB
Almacenamiento	Se recomienda cada unidad sobre discos independientes, así como redundancia
70 GB: Sistema operativo, software y bases de datos del sistema SQL Server	
70 GB: logs bases de datos	
70 GB: Datos 1	
140 GB: Datos 2	
140 GB: Datos 3	
280 GB: Datos 4	
Conexión a red	100 Mbps
Software	
Sistema operativo	Microsoft Windows® Server 2008 Enterprise
Motor base de datos	SQL Server 2008
.Net Framework	2.0 y 3.5
Servidor de Aplicaciones	
Hardware	
Procesador	1 Intel Xeon Dual Core 2.0 GHz o superior, x86
Memoria RAM	6 GB
Almacenamiento	70 GB: sistema operativo y software
Conexión a red	100 Mbps: se recomienda ubicar este servidor en el mismo segmento de red que el servidor de base de datos
Software	
Sistema operativo	Microsoft Windows® Server 2003 Enterprise

Tabla 4. Continuación

COMPONENTES	
.Net Framework	2.0 y 3.5
Terminales	
Hardware	
Procesador	Intel Pentium 4 o superior
Memoria RAM	2 GB
Espacio en disco duro	100 Mbps
Conexión a red	10/100 Mbps
Software	
Sistema operativo	Microsoft Windows® XP Professional SP2 o superior
Net Framework	2.0y 3.5

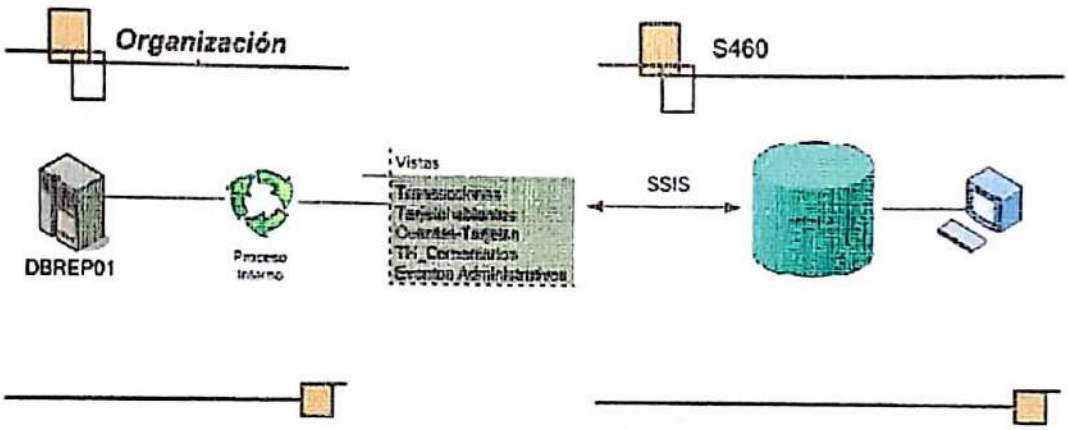
Fuente: *Autoria Propia 2013*

3.4 Documentación Técnica

Esquema General

A continuación se muestra el esquema de réplicas y de operación del servidor S460-SENTPREV01, definido entre la organización y el desarrollo para la correspondiente carga de información.

Figura No. 5. Esquema General del servidor



Fuente: *Autoría Propia, 2013*

A continuación la descripción del esquema general:

- Se cuenta con la fuente de datos en plataforma Oracle, el cual provee la información que es replicada al sistema Monitoring.
- La información de tarjetahabientes es cargada una vez por día.
- La información de transacciones es cargada cada diez segundos.
- La información de cuentas y tarjetas es cargada una vez por día.
- La información de TH_Comentarios es cargada cada dos minutos.
- La información de eventos administrativos es cargada cada minuto.

3.5. Procesos de Replicas Intergration Services

A continuación los *Integration Services* que se utilizan para obtener la información en la Bases de Datos Monitoring del core.

Estos procesos se desarrollaron utilizando la herramienta *"SQL Server Business Intelligence Development Studio 2008"*.

a) Proceso SSIS_Catalogos.dtsx

Este proceso carga los datos correspondientes a los catálogos de MCCs, Monedas, Paises Adquirentes, Bines, y Puntos de Entrada mediante varios Data Flow Task y Execute SQL Task. Este solo se ejecuta una única vez como carga inicial.

b) Proceso SSIS_FA_Cuenta_Tarjeta.dtsx

Este proceso carga los datos correspondientes a las cuentas y tarjetas mediante varios Execute SQL Task y Data Flow Task. Este proceso se ejecuta una vez al día.

c) Proceso SSIS_Tarjeta_Habiente_Credito.dtsx

Este proceso carga los datos correspondientes a los tarjetahabientes para la UEN de crédito mediante varios Execute SQL Task y Data Flow Task. Este proceso se ejecuta una vez al día.

d) Proceso SSIS_Tarjetahabiente_Debito.dtsx

Este proceso carga los datos correspondientes a los tarjetahabientes para la UEN de débito mediante varios Execute SQL Task y Data Flow Task. Este proceso se ejecuta una vez al día.

e) Proceso SSIS_TH_Comentarios.dtsx

Este proceso carga los datos correspondientes a comentarios sobre los tarjetahabientes mediante un Data Flow Task con varios Data Flow Transformations. Este proceso se ejecuta cada dos minutos.

f) Proceso SSIS_Trans_Admin.dtsx

Este proceso carga los datos correspondientes a los eventos administrativos mediante varios Execute SQL Task, Script Task, Data Flow Task y Data Flow Transformations. Este proceso se ejecuta cada 10 segundos.

g) Proceso SSIS_Trans_Credito.dtsx

Este proceso carga los datos correspondientes a las transacciones de crédito mediante varios Execute SQL Task, Script Task, Data Flow Task y Data Flow Transformations. Este proceso se ejecuta cada 10 segundos.

h) Proceso SSIS_Trans_Debito.dtsx

Este proceso carga los datos correspondientes a las transacciones de débito mediante varios Execute SQL Task, Script Task, Data Flow Task y Data Flow Transformations. Este proceso se ejecuta cada 10 segundos.

i) Proceso SSIS_Trans_Debito_TrxRetrazo.dtsx

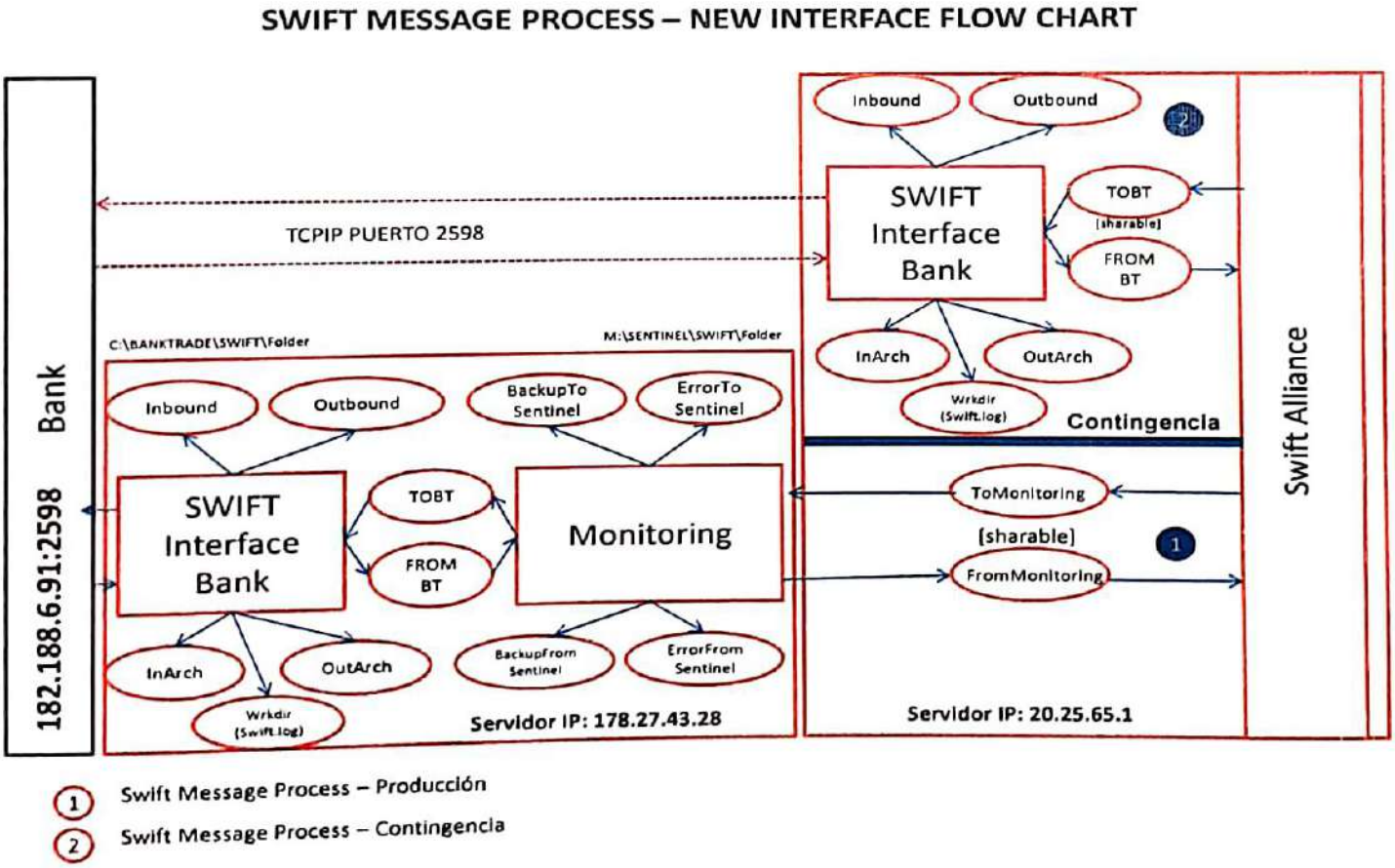
Este proceso carga los datos correspondientes a las transacciones de débito que llegan con retrasos mediante varios Execute SQL Task, Data Flow Task y Data Flow Transformations. Este proceso se ejecuta cada treinta minutos.

3.5.1 Descripción de paquetes SSIS (Integration Services)

Los paquetes IS son los procesos encargados de realizar cargas entre base de datos o en una misma base de datos. En Monitoring también se utilizan para dar mantenimiento a algunas tablas de información histórica de la base de datos Monitoring_Prevention.

Se encuentran almacenados en la siguiente ruta "D:\Program Files\Microsoft SQL Server\Integration_Services\Monitoring_SSIS\IS_Replicas\IS_Interface". En el servidor "C860-SENPMREB01" con dirección IP 182.150.0.48.

Figura No. 6. Proceso Mensajes Swift.



Fuente: *Autoría Propia 2013*

3.6. Jobs

a. Lista de Jobs

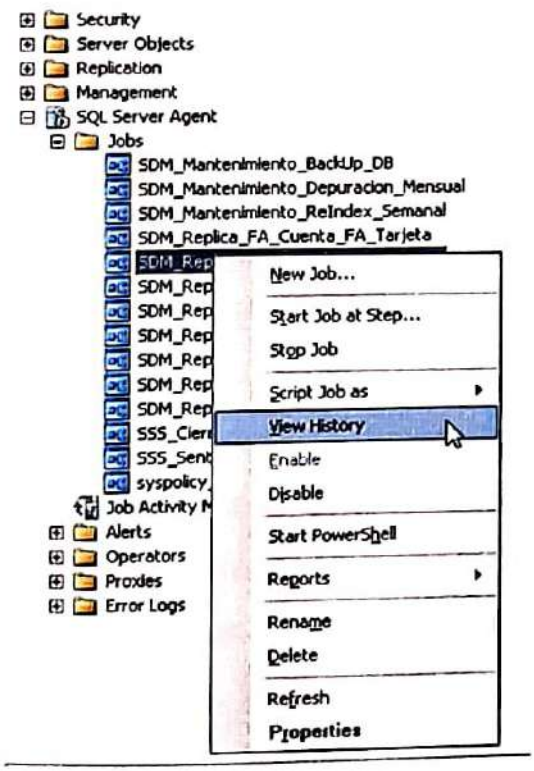
El detalle de los jobs y su calendarización de los procesos de réplica de Monitoring_Prevention se encuentran en el documento adjunto con nombre ***"Calendarización de Procesos, BanReservas.doc"***

b. Errores de ejecución en Jobs

Los procesos automáticos se ejecutan a través de "Jobs", para determinar el error en la ejecución de los mismos, existen dos mecanismos:

Visualizando el histórico de ejecuciones en el SQL Server Agent, como muestra las siguientes imágenes:

Figura No. 7. Vista SQL Server Management Studio



Fuente: *Server Producción sistema Monitoring, 2013*

3.7. Usuarios del sistema

A continuación se describen los usuarios que están utilizando en Monitoring en todos los procesos relacionados al sistema.

Base de datos:

- **Sa**: usuario administrador de la base de datos, no se utiliza por Monitoring.
- **SysMonitoring**: usuario interno de Monitoring, la contraseña es segura y no se debe cambiar.
- **Sdmin**: usuario de aplicación, se puede cambiar la clave en cualquier momento desde el sistema.
- **UtilitarioODBC:** Usuario creado para crear el ODBC que será configurado en las computadoras cliente.
- **UtilitarioACL:** Para hacer consultas de lectura externas a las diferentes tablas del sistema.
- **UtilitarioIS:** Usuario creado para la calendarización y ejecución de los jobs. La contraseña es segura y no se debe cambiar.
- **UtilitarioList:** Usuario creado para la cargar la lista que contiene los tarjetahabientes VIP. La contraseña es segura y no se debe cambiar.
- **Usuario y xusuario:** Son login de base de datos creados por el sistema Monitoring al momento de crear un usuario, por cada usuario es creado el usuario y su respectivo xusuario, a nivel de base de datos no se debe eliminar ninguno de los dos, es importante indicar que un usuario del sistema Monitoring solo puede acceder desde la aplicación y no a nivel de base de datos, si una contraseña es cambiada desde la base de datos dicho usuario no podrá ingresar desde la aplicación clientes

3.8 Plan de Pruebas Aplicación Monitoring.

Tabla No. 5. Plan de pruebas

INFORMACIÓN GENERAL ACERCA DE LAS PRUEBAS	
Dominio:	Interfaz Mensajes
Elemento(s):	Aplicación Monitoring
Tipo de Pruebas:	Pruebas Integrales
Coordinación:	Consultor - Dirección Seguridad Bancaria
Participantes:	**Consultores:**
Fecha Inicio:	21-09-2013
Fecha Fin:	00-00-00
Horario de Trabajo:	08:30 am a 5:00 pm
Lugar de Trabajo:	N/A
Req.(s) Incluidos(s):	N/A

Fuente: *Autoría Propia 2013*

Tabla No. 6. Proceso implementación Monitoring

Implementación Aplicación Monitoring	Resultado Esperado	Res.	Impacto
Preliminares			
1. Instalación Aplicación Monitoring	N/A		
2. Creación de Base de Datos.	N/A		
3. Instalación Interfaz Core.	N/A		
4. Apertura de Trafico.	N/A		
5. Configuración de Ambiente (Folders y Parámetros).	N/A		
6. Configuración Puertas de Entrada y Salida en Swift.	N/A		
7. Actualización Base de Datos de Cuentas.	N/A		
8. Limpieza de BD de Mensajes de Monitoring.	N/A		
9. Preparar Mensajes de Entrada y Salida para pruebas.	N/A		
Mensajes Entrantes			
10. Colocar y Cuantificar cantidad de mensajes en carpeta C:/Monitoring/Swift/TOMONITORING (149 archivos, 647 mensajes.)	Cuantos mensajes contienen los archivos, que los mismos sean procesados por la aplicación y pasen por las reglas y validaciones correspondientes, dejando una copia de cada archivo en el folder de respaldo y dejar folder vacío.		
11. Verificar y Cuantificar cantidad de mensajes procesados en carpeta C:/Server/SWIFT/TOBT	Verificar que se crearon la misma cantidad de archivo de mensajes procesados.		
12. Tomar tiempo de procesamiento de cada mensaje.	Que los mensajes se procesen en un periodo de tiempo prudente.		
13. Cuadrar cantidad de mensajes colocados contra cantidad de mensajes procesados, Incompletos, fallidos, etc.	Que la cantidad de mensajes procesados, incompletos, fallidos, insertados sea igual a la cantidad de mensajes colocados en la carpeta origen.		

Tabla No. 6. Continuación

Mensajes Entrantes	Resultado Esperado	Re	Impacto
14. Verificar contenido del mensaje.	Que el contenido del mensaje de entrada sea igual al contenido del mensaje de salida, salvo en los casos que el mensaje haya sido modificado en Monitoring por el usuario.		
15. Identificar y verificar mensajes MT103, MT202	Confirmar que solo los mensajes MT103, MT202 son validados por la aplicación.		
16. Verificar las carpetas: C:/MONITORING/Swift/BACKUPTOMONITORING, C:/MONITORING/Swift/ERRORTOMONITORING	Que las copias de mensajes se encuentren en el folders C:/MONITORING/Swift/BACKUPTOMONITORING y que los fallidos en C:/MONITORING/Swift/ERRORTOMONITORING		
17. Verificar nombre de archivos.	El nombre no puede contener espacios en blanco, no puede pasar de 35 caracteres.		
18. Verificar log mensajes fallidos.	De existir un mensaje fallido que el mismo tenga el mensaje de error correspondiente en el log.		
19. Identificar y verificar mensajes con cuentas validas de 15 posiciones sin caracteres. :20:F01227706BC401 :59:/200023500004866	Comprobar que las cuentas con este formato son procesadas correctamente.		
20. Identificar y verificar mensajes con cuentas validas de 15 posiciones con caracteres.:20:F61003 057942000 :59:/200-02-330-000401-3	Comprobar que las cuentas con este formato son procesadas correctamente.		
21. Identificar y verificar mensajes con cuentas validas de 10 posiciones sin caracteres. :20:F01227706C4C01 :59:/0801325454	Comprobar que las cuentas con este formato son procesadas correctamente.		

Tabla No. 6. Continuación

Mensajes Entrantes	Resultado Esperado		Impacto
32. Posibilidad de declinar mensajes con cuentas incompletas.	Que una vez seleccionada esta acción el mensaje sale de la bandeja de incompletos y deja un rastro de que existió.		
33. Definir regla de cumplimiento.	Confirmar que los mensajes se detienen conforme a la regla establecida.		
34. Verificar y liberar mensajes detenidos por las reglas de cumplimiento.	Que una vez liberada la transacción el mensaje sigue el flujo establecido.		
35. Verificar criterios de búsqueda de la aplicación.	Obtener consultas de mensajes acordes a las búsquedas solicitadas.		
36. Verificación Contra World Check.	Que los mensajes son verificados por World Check.		
37. Imprimir Mensajes.	Obtener salida de mensajes.		
38. Crear grupo de trabajo entrante.			
Mensajes Salientes			
39. Colocar y Cuantificar cantidad de mensajes en carpeta C:/Banktrade/Swift/FROMBT 20 archivos con 48 mensajes	Cuantos mensajes contienen los archivos, que los mismos sean procesados por la aplicación y pasen por las reglas y validaciones correspondientes, dejando una copia de cada archivo en el folder de respaldo y dejar folder vacío.		
40. Verificar y Cuantificar cantidad de mensajes procesados en carpetaC:/MONITORING/Swift/FROMMONITORING	Verificar que se crearon la misma cantidad de archivo de mensajes procesados.		
43. Tomar tiempo de procesamiento de cada mensaje.	Que los mensajes se procesen en un periodo de tiempo prudente.		
Cuadrar cantidad de mensajes colocados contra cantidad de mensajes procesados, Incompletos, fallidos, etc.	Que la cantidad de mensajes procesados, incompletos, fallidos, insertados sea igual a la cantidad de mensajes colocados en la carpeta origen.		
Verificar los mensajes incompletos	Que los mensajes incompletos respondan a los criterios establecidos. No deberían quedar incompletos por cuentas.		

Tabla No. 6. Continuación

Mensajes Salientes			
41. Actualizar Nombre en Monitoring	Que una vez modificado el nombre el mismo se graba correctamente en la base de datos y en el mensaje.		
42. Definir regla de cumplimiento.	Confirmar que los mensajes se detienen conforme a la regla establecida.		
43. Verificar y liberar mensajes detenidos por las reglas de cumplimiento.	Que una vez liberada la transacción el mensaje sigue el flujo establecido.		
44. Verificar criterios de búsqueda de la aplicación.	Obtener consultas de mensajes acordes a las búsquedas solicitadas.		
45. Verificación Contra OFAC.	Que los mensajes son verificados por OFAC.		
46. Imprimir Mensajes.	Obtener salida de mensajes.		
47. Verificar log mensajes fallidos.	De existir un mensaje fallido que el mismo tenga el mensaje de error correspondiente en el log.		
48. Verificar contenido del mensaje.	Que el contenido del mensaje de entrada sea igual al contenido del mensaje de salida, salvo en los casos que el mensaje haya sido modificado en Monitoring por el usuario.		
49. Identificar y verificar mensajes MT103, MT202	Confirmar que solo los mensajes MT103, MT202 son validados por la aplicación.		
50. Verificar las carpetas: C:/MONITORING/Swift/BACKUPFROMMONITORING C:/MONITORING/Swift/ERRORFROMMONITORING	Que las copias de mensajes se encuentren en el folders C:/MONITORING/Swift/BACKUPFROMMONITORING. y que los fallidos en C:/MONITORING/Swift/ERRORFROMMONITORING		
PROMEDIO DE AVANCE		%	
1. Comentarios Resultados			**Estatus**
			<Reportado >

Fuente: *Autoría Propia 2013*

Tabla No. 7. Propuesta Implementación

Licencias		**US$ 93,000.00**
Contrato de Mantenimiento y Soporte		**US$ 0.00**
Implementación		**US$ 64,000.00**
Instalación ambiente desarrollo y mapeos	US$ 7,200.00	3 semanas 1 consultor
Réplicas		
Procesos de alimentación desde tablas Oracle.	US$ 4,800.00	2 semanas 1 consultor
Apoyo en certificación: actividad en sitio	US$ 7,200.00	3 semanas 1 consultor
Verificación posterior aplicación ajustes	US$ 7,200.00	3 semanas 1 consultor
Piloto productivo	US$ 9,600.00	4 semanas 1 consultor
Desarrollo matriz de riesgo	US$ 4,800.00	2 semanas 1 consultor
Swift		
Cargas	US$ 9,600.00	4 semanas 1 consultor
Aplicación operativa	US$ 7,200.00	3 semanas 1 consultor
Integración con OFAC	US$ 4,800.00	2 semanas 1 consultor
Capacitación	US$ 4,800.00	2 semanas 1 consultor
Pase a producción y documentación	US$ 7,200.00	3 semanas 1 consultor
Seguimiento		
Usuarios	US$ 7,200.00	3 semanas 1 consultor
Técnico	US$ 2,400.00	1 semana 1 consultor
US$ 157,000.00		
Los viáticos estimados para este proyecto son US$41,660.		

Fuente: *Autoría Propia 2013*

3.9. Actividades y Supuestos

A continuación se detallan algunas de las actividades y se exponen los supuestos que las soportan (cuando aplican).

Instalación ambiente desarrollo y mapeos: en esta tarea se instala el ambiente de desarrollo y conjuntamente se realizan los mapeos de todas las fuentes de las cuales se van a alimentar los datos hacia Monitoring. Es requisito para realizar esta tarea tener listo el ambiente de desarrollo y disponibilidad de las personas con conocimiento de las diferentes fuentes de datos.

Réplicas: en esta tarea se desarrollan y certifican los procesos encargados de cargar los datos a Monitoring. El alcance de esta propuesta contempla una participación activa por parte del suplidor en esta actividad.

Los tiempos estimados en esta actividad se basan en el supuesto de que la institución se hará cargo de la mayor parte de esta actividad, encargándose de generar tablas en Oracle con la estructura y los datos definidos en los mapeos. El suplidor leerá dichas tablas, cargará hacia la base de datos de Monitoring y apoyará en la certificación. Es importante tener en cuenta que el suplidor se verá eximido de agregar validaciones o transformaciones. Adicionalmente cada tabla que se creará en Oracle deberá tener un consecutivo de registro que permita controlar los registros que se han procesado.

Piloto productivo: el piloto productivo consiste en instalar el sistema en el ambiente productivo, pasar los procesos de réplicas de datos a dicho ambiente y conectarlos contra el ambiente productivo del Core Banking. Adicionalmente en esta etapa se debe realizar la configuración del sistema y el inicio de la operación en forma parcial. Operación parcial implica que se trabaja con un subconjunto de herramientas y no necesariamente se involucra a todos los usuarios.

Desarrollo matriz de riesgo: se definen los factores que componen la matriz de riesgos y sus pesos. Dicha matriz se debe configurar en el sistema y se hace la primera calificación. No se contempla agregar datos adicionales para la matriz, es decir, se utilizarán los datos replicados en la primera etapa.

Pase a producción y documentación: durante esta etapa se terminan de definir y crear las herramientas requeridas, se instalan las estaciones de trabajo faltantes y se involucra a todas las personas en los diferentes procesos. En este punto se detiene el sistema actual.

Apoyo:

- *Usuarios:* apoyo en el uso del sistema y ajuste a los cambios en la forma de trabajar.

- *Técnico:* apoyo a los encargados del sistema desde el punto de vista técnico. En esta etapa se hace la entrega formal del sistema y se apoya en la configuración de respaldos y otros procesos administrativos.

Tabla No. 8 .Términos y Condiciones de Pago

La forma de pago será la siguiente: Licencias:	50% a la firma del contrato. 50% contra la instalación del Sistema de Software.
Mantenimiento Anual:	Se pagará contra la instalación del Sistema de Software y luego anualmente por adelantado en la fecha de aniversario del primer pago.
Implementación y Capacitación:	40% a la firma del contrato. 40% contra el inicio de la implementación. 20% contra el fin de la implementación.
Viáticos:	20% a la firma del contrato. 80% contra el inicio de la implementación.
Impuestos / Tasas:	Los precios y costos no incluyen ningún tipo de impuesto ni retención, en caso de haberlos serán pagados por la institución.

Fuente: *Autoría propia 2013*

3.10. Condiciones Generales

3.10.1. Licencia Inicial

La Licencia del Sistema de Software será no exclusiva, no transferible y usada en el Sitio Autorizado, en el ambiente de la institución. El original y cualquier copia del Sistema de Software o partes de ella, serán siempre propiedad del suplidor.

3.10.2. Servicios de Implementación y Capacitación:

La implementación y capacitación del Sistema de Software se regirá según nuestra metodología de implementación y plan de capacitación.

A nivel general es importante recalcar que:

- El número de días de implementación señalados en la propuesta económica, corresponde al tiempo estándar estimado de acuerdo a nuestra metodología. Dependiendo de aspectos técnicos de la infraestructura de la institución y de sus procesos, el esfuerzo de implementación puede requerir ajustes.

- Este proceso de puesta en marcha incluye la instalación de cada producto, la capacitación a usuarios y la implementación de las diferentes herramientas del sistema (por ejemplo, definición de reglas, perfiles, indicadores, etc.).

- Las actividades que se realicen en las instalaciones de la organización, como por ejemplo Capacitación, Carga y Puesta en Marcha/Apoyo en Uso, se realizan en jornadas completas de 8 horas diarias.

- Si las actividades requieren más o menos tiempo de lo planteado, por causa de uso parcial del horario diario en las actividades con los usuarios de la institución y/o por tiempos adicionales relativos al proyecto (y no por causa del suplidor.), o lo contrario, por disminución de los tiempos previstos, los costos de Implementación se ajustarán proporcionalmente.

El costo por semana de implementación corresponde a US$ 2,400.00 (dos mil cuatrocientos dólares de los Estados Unidos de América) y será facturado quincenalmente.

- Los gastos de viaje son cubiertos por la institución y se consideran utilizando los siguientes rubros: viáticos diarios US$ 60.00, hotel diario US$ 120.00, impuestos y taxi aeropuerto US$ 120.00. Los costos de tiquetes aéreos se definirán de acuerdo al precio que brinde la aerolínea.

- La posibilidad de carga de datos antiguos dependerá de la calidad y estandarización de los datos a migrar. Los tiempos de carga deben ser confirmados una vez se analice la realidad de los datos a migrar y su volumen y diversidad.

- Si se involucra a él suplidor en la revisión, depuración de la data vía programación o borrado selectivo de información, estas actividades adicionales serán cotizadas, en proporción a los valores señalados para un mes de implementación, según sea el tiempo necesario para esta actividad. Esta actividad adicional no implicará responsabilidad final del Suplidor sobre la calidad de los datos y su certificación final debe estar a cargo del institución.

- De requerirse interfaces con otros sistemas, un consultor de la Monitoring. Será asignado a esas tareas y una vez definidas en detalle las interfaces requeridas, estas serán elaboradas. Se evaluarán las tareas necesarias y se establecerá los costos proporcionales en base a los valores señalados en esta oferta.

- El precio estimado en la propuesta está basado en la información disponible en el momento de preparar la misma, por lo tanto pueden existir variaciones dependiendo de requerimientos no visualizados en un inicio.

- Los valores señalados respecto del software y hardware serán pagados mediante transferencia a la cuenta que señale el Suplidor y son valores netos.

3.11. Análisis Costo Beneficios

Las mejores prácticas de negocios de nuestros clientes son incluidas en el sistema a través del mantenimiento anual, que les brinda acceso a todas las mejoras y nuevas funcionalidades que se le incluyen a Monitoring, además de soporte técnico remoto.

Esto asegura que la inversión en el sistema no se vuelva obsoleta desde el punto de vista funcional y técnico, en el mediano o largo plazo y se adapte a los giros del negocio.

Los siguientes son los beneficios de nuestro contrato de actualización y soporte remoto:

a) Entrega de las versiones del producto, actualmente en formato de disco compacto (CD).

b) Derecho a recibir sin costo las versiones de mantenimiento o menores y versiones mayores de los productos.

c) Cada versión mayor incluye manuales de usuario actualizados del producto en medio magnético.

d) Consultas de soporte técnico a través de nuestro Centro de Soporte Internacional, por teléfono, fax, correo electrónico o conexión remota, sobre consultas, problemas, errores o mejoras de los productos adquiridos.

e) Nuestra tecnología de comunicaciones nos permite conectarnos directamente a los computadores o servidores del cliente desde nuestras oficinas, para revisar o solucionar cualquier problema, sin ningún requisito especial de hardware o

software del cliente, solo manteniendo una conexión por Internet. Esto nos evita traslados y permite ganar tiempo en la revisión de cualquier situación.

f) Posibilidad de solicitar mejoras y que estas sean analizadas por el Comité de Administración de la Configuración de Monitoring.

g) Monitoring provee soporte técnico en sitio por solicitud del cliente a las tarifas estándares por hora.

CONCLUSIONES

1. La demanda de protección de los sistemas de seguridad informática de la empresa obligo a invertir y actualizar las aplicaciones necesarias para mantener el resguardo de las informaciones críticas que estos sistemas operan.

2. Diseñar y e implementar esta aplicación permitió asegurar el monitoreo de las transacciones del exterior con un grado mayor de seguridad.

3. Se establecieron parámetros de seguridad que abalan, clasifican y dan seguimiento a todas las transacciones de Remesas.

4. Se definieron políticas claras de seguridad en otros procesos que están directamente relaciones a esta aplicación y otras aplicaciones de seguridad informática de la institución.

5. Determinar la importancia y la vulnerabilidad del proceso de remesas propicio que se invirtiera en la puesta en funcionamiento de esta herramienta, y en su mejora continua.

6. Por ser un sistema nuevo para el área que dirige estas operaciones, su funcionabilidad se ha concebido de forma rápida y ágil por parte de los usuarios y administradores, sin embargo a largo plazo podría ser necesario la aplicación de mejoras y nuevos módulos con el fin de ampliar su capacidad.

7. La aplicación le permite al área de seguridad mantener un histórico eficiente de los eventos y errores relevantes de la aplicación.

8. Las aplicaciones que implican procesos vulnerables necesitan la atención prioritaria por parte de la área responsable, para asegurar que funcionen con las condiciones esperadas y aporten el grado de confianza necesaria, esto es vital para todo proceso de evaluación de la una implementación eficiente.

RECOMENDACIONES

1. Adecuar el módulo de remesas para que opere con mayor viabilidad con la nueva aplicación de monitoreo.

2. Actualizar las políticas establecidas para los usuarios y adecuarla con las mejoras que se realicen.

3. Realizar un programa de seguimiento estandarizado por el área administradora de la aplicación, para asegurar el resguardo de los datos.

LISTAS DE REFERENCIAS

Ben, Laurie, (2005). *Software libre, php y mysql .Tecnologías para el desarrollo de aplicaciones web.* Ediciones Díaz de Santos. España

Bell, Douglas, (2007).*Diagramas de clases para elaborar sistemas* [Documento en línea]. Disponible en http://www.monografias.com/diagramas de clase/lenguaje-modelado-sistemas.

Chohen D., K. & Asin Lares E. (2005). *Sistema de Información para los negocios.* México. MacGrawHill.

Charles Cresson Wood. *Políticas de Seguridad Informática*, 9th Mejores Prácticas Internacionales.

Hernández, R. Fernández, C. y Baptista, Pila (2009). *Metodología de la investigación.* Segunda Edición. Editorial McGraw-Hill. México.

Hurtado de Barrera, J., (2000). *Metodología de la investigación* holística (2da. ed.) Caracas, Venezuela: Fundación Sypal

James A. Senn, (2008), *Análisis y Diseño de Sistemas de Información.* Editorial Mc Graw Hill. Segunda edición. Colombia.

Laudon, K., & Laudon J. (2004). *Sistemas de información gerencial:* Administración de la empresa digital. México: Pearson Prentice Hall.

Marcelo, J. Riesgo y Seguridad de los sistemas de información. Universidad Politécnica de Valencia

Morant, Ribagorda, *Sancho*. *Seguridad y Protección de la información.* Editorial Centro de Estudios Ramón Areces. 1994

Montilva C, Jonas, (2008), *Gray Watch. Método de desarrollo de software para aplicaciones empresariales.* Mérida –Venezuela

Pastor Franco, J.; Sarasa López, M.A. *Criptografía digital. Fundamentos y aplicaciones.* Prensa Universitaria de Zaragoza, 1998

Shon Harris, (2002), *CISSP Certification*, fourth edition, McGraw-Hill/Osborne.

William, Stallings, *Comunicaciones y Redes de Computadoras*, 6ta Edición - Editorial McGraw-Hill. México.

http://es.wikipedia.org/wiki/Sistema_de_Gesti%C3%B3n_de_la_Seguridad_de_la_Informaci%C3%B3n *(Consultado en fecha 09/02/2013)*

http://www.revista-ays.com/DocsNum09/PersEmpresarial/scana.pdf *(Consultado en fecha 05/04/2013)*

http://www.unilibrecali.edu.co/entramado/images/stories/pdf_articulos/volumen2/Politicas_de_seguridad_informtica.pdf *(Consultado en fecha 06/04/2013)*

http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#POLIT *(Consultado en fecha 12/04/2013)*

http://codechoco.gov.co/files/POLITICAS_INFORMATICAS_CODECHOCO.pdf *(Consultado en fecha 22/04/2013)*

http://www.acatlan.unam.mx/cedetec/3179 *(Consultado en fecha 05/05/2013)*

http://www.viruslist.com/sp/analysis?pubid=207271189 *(Consultado en fecha 05/06/2013)*

http://www.viruslist.com/sp/viruses/analysis?pubid=207271189 *(Consultado en fecha 09/06/2013)*

ANEXOS

Glosarios de Termino:

Datos: Puede ser un número, una palabra, una imagen, son la materia prima para producción información.

Información: son datos que dentro del contexto dado tienen un significado para alguien.

Sistemas: Es el mecanismo por el cual se genera información.

Tecnología de Información: este concepto hace referencia a todas aquellas tecnologías que permiten y dan soporte a la construcción y operación de los sistemas de información, los cuales pueden ser tecnología de hardware, software, tecnología de almacenamiento y tecnología de almacenamiento.

Usuario: es quien accesa a la base de datos por medio de un lenguaje de consulta o de programas de aplicación.

Lenguaje de programación: es un conjunto de reglas y estándares para escribir un programa.

Interfaz del usuario: es cualquier situación donde el usuario recibe algo del sistema de información o da instrucciones al sistema computacional.

Archivo. Es un elemento de almacenamiento de información que consiste en una serie de registros, cada uno de los cuales contiene información similar.

Programación: consiste en elaborar los programas considerados en el diseño para cumplir con lo especificado por el usuario.

Implantación: consiste en instalar el sistema en el ambiente en que operara y en realizar los procesos necesarios para que opere correctamente.

Pruebas del sistema: Este proceso se realiza con el fin de asegurar que el sistema esté libre de errores y debe realizarse durante todo el proceso y no en la fase final.

Mantenimiento: es el proceso mediante el cual se realizan mejoras a un sistema para que tenga una vida útil más larga.

Remesas: son fondos que los emigrantes envían a su país de origen, normalmente a sus familiares.

SQL (Structure Query Language): es un lenguaje de consulta, que sirve para extraer información de la base de datos. Este lenguaje permite al usuario hacer requisiciones de datos sin tener que escribir un programa.

Gestión de incidentes: El servicio de gestión de incidentes de seguridad de RedIRIS (IRIS-CERT) tiene como objetivo coordinar la respuesta ante incidentes de seguridad informática que afecten a la seguridad de las redes de las instituciones afiliadas, como ataques de denegación de servicio, virus, gusanos, troyanos, etc. y realizar una labor preventiva avisando con tiempo a dichos centros de problemas potenciales, ofreciéndoles asesoramiento y facilitándoles soporte complementario.

Gestión de configuración: Se denomina Gestión de la Configuración al conjunto de procesos destinados a asegurar la calidad de todo producto obtenido durante cualquiera de las etapas del desarrollo de un Sistema de Información (S.I.), a través del estricto control de los cambios realizados sobre los mismos y de la disponibilidad constante de una versión estable de cada elemento para toda persona involucrada en el citado desarrollo

Gestión de parches: La gestión de parches implica aplicar parches y actualizaciones de software a un sistema. Es posible que la gestión de parches también implique eliminar parches no deseados o defectuosos. La eliminación de parches también se denomina **efectuar copias de seguridad** de parches.

Sistema ERP: Los **sistemas de planificación de recursos empresariales**, o **ERP** (por sus siglas en inglés, *Enterprise Resource Planning*) son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios.

Sistema SCADA: (Supervisory Control And Data Acquisition (Supervisión, Control y Adquisición de Datos) es un software para ordenadores que permite controlar y supervisar procesos industriales a distancia. Facilita retroalimentación en tiempo real con los dispositivos de campo (sensores y actuadores) y controlando el proceso automáticamente. Provee de toda la información que se genera en el proceso

productivo (supervisión, control calidad, control de producción, almacenamiento de datos, etc.) y permite su gestión e intervención.

PLC(controlador lógico programable) más conocido por sus siglas en inglés ***PLC*** *(Programmable Logic Controller)*, es una computadora utilizada en la ingeniería automática o automatización industrial, para automatizar procesos electromecánicos, tales como el control de la maquinaria de la fábrica en líneas de montaje o atracciones mecánicas.