ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

IV PROMOCIÓN

PROYECTO

TEMA

"AUDITORÍA DE LA SEGURIDAD DE INFORMACIÓN AL SISTEMA ELECTRÓNICO BURSÁTIL (SEB) DE LA BOLSA DE VALORES DE GUAYAQUIL"

AUTORAS

MAYRA BENAVIDES RODRÍGUEZ
JULIA MACÍAS TULCÁN

AÑO

2011

AGRADECIMIENTO

A todos quienes nos formaron en esta nueva meta emprendida, compartiendo sus conocimientos y abriendo espacio hacia una nueva profesión que requiere de mucha honestidad y compromiso.

DEDICATORIA

A nuestras familias, a nosotras mismas, por el arduo trabajo y apoyo constante que como equipo nos hemos brindado.

Julia & Mayra

INDICE GENERAL

SECCIÓN 1: INFORME DEL PROYECTO

Capítulo 1: Objetivo del Proyecto

El objetivo de este Proyecto es desarrollar la AUDITORÍA DE LA SEGURIDAD DE INFORMACION AL SISTEMA ELECTRÓNICO BURSÁTIL (SEB) DE LA BOLSA DE VALORES DE GUAYAQUIL, de acuerdo a estándares internacionales de seguridad, para el Control de la Información en los Sistemas Informáticos.

Evaluar las vulnerabilidades a las que está expuesto su sistema transaccional y contribuir con un mejoramiento de sus controles, y sugerir la implementación de estrategias que cubran los procesos.

Capítulo 2: Justificación

Al ser, la Bolsa de Valores de Guayaquil una institución regulada por el Consejo Nacional de Valores y la Superintendencia de Mercados de Valores, requiere de una constante optimización de sus recursos tecnológicos de hardware y software, y para que esto se produzca, es importante que esta institución permita que su sistema transaccional más importante, se someta a una auditoria de seguridad de la información, de manera permanente.

Los riesgos, son uno de los principales problemas en la seguridad que debe enfrentar las TI, y para mitigar los daños que se puedan generar, se deben implementar medidas regulatorias, para evitar un impacto mayor de estos conflictos, de manera que tengamos a nuestra disposición un sistema informático en condiciones de brindar un servicio financiero, en condiciones seguras; aunque estas seguridades no proporcionen el 100% de tranquilidad a los usuarios, porque diariamente estamos expuestos a recibir ataques de diferente índole y origen, que ponen en peligro toda la información.

Capítulo 3: Alcance del Proyecto

El Alcance de este Proyecto, involucra la evaluación de la Seguridad de la Información que se maneja a través del Sistema Electrónico Bursátil, el cual incluye

actividades de análisis basado en estándares y pruebas de cumplimiento de los controles.

Se elaborará un informe final con los hallazgos y las debidas recomendaciones para contribuir con un mejoramiento de sus controles, y sugerir la implementación de estrategias que cubran el proceso soportado por el Sistema SEB.

Cabe indicar que en el trabajo desarrollado por el equipo no incluirá diseño ni implementación de estrategias y controles sugeridos.

Capítulo 4: Metodología, estándares y procedimientos

El desarrollo del proyecto se llevó a cabo en tres fases: la primera consistió en una investigación documental; la segunda en una investigación de campo y la tercera la conformó el análisis, evaluación y tratamiento de los riesgos de los activos de información. Siempre en el contexto de nuestra auditoria al SEB.

La investigación documental, permite conocer el tipo de Negocio al que se dedica la Bolsa de Valores y cuál es su estructura organizacional. También nos permite indagar sobre su cultura relacionada a los riegos de seguridad de la información.

La investigación de campo, se inició con el análisis sistemático del proceso que soporta al SEB, luego trabajamos con los instrumentos de recolección de la información, mediante la técnica de la entrevista, al personal que labora en las áreas de Operaciones, Sistemas y Centro de Cómputo; y finalmente una revisión del laboratorio informático para conocer la operatividad del sistema.

Se llevó a cabo el levantamiento de la información, con el resultado de las entrevistas semi-estructuradas, que se aplicaron y se realizaron visitas guiadas a las instalaciones.

Una vez obtenido los datos e información de los diferentes departamentos y personal involucrados, y corroborado con la visita al Centro de Computo de la Bolsa de Valores, se procedió a la revisión, análisis e interpretación de los mismos. Para ello

se emplearon métricas cuantitativas, pero en la mayoría se realizó usando la métrica cualitativa.

Los Estándares Internacionales para establecer las métricas de evaluación, consultados fueron:

- ISO/IEC 27002: Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
- ISO/IEC 27005: 2008: Gestión de Riesgos de la Seguridad de la Información
- Magerit versión 2 Metodología de análisis de Gestión de riesgo de los Sistemas Informáticos.
- ISO 15408: Common Criteria, con Criterios comunes para la Evaluación de la Seguridad de los Sistemas de Información TI
- COBIT 4.1: Marco de Trabajo para Alineación estratégica del negocio con TI
- COSO: Control Interno para la Gestión de Riesgos

Procedimientos:

- ✓ Revisión de documentación Normativas de la Bolsa de Valores de Guayaquil.
- ✓ Revisión de políticas y procedimientos relativos al uso y protección de la información.
- ✓ Revisión e identificación de riesgos en la seguridad de la información
- ✓ Desarrollo de pruebas de controles en la seguridad de la información
- ✓ Revisión e identificación de riesgos en la seguridad del sistema SEB
- ✓ Desarrollo de pruebas de controles en la seguridad de la información.

Capítulo 5: Equipo de Trabajo

EL equipo de trabajo está conformado por:

NOMBRES	TITULO ACADEMICO	CARGO
Julia Macías Tulcán	Ingeniera en Sistemas Computacionales	Representante del Equipo y Auditora
Mayra Benavides Rodriguez	Licenciada en Informática	Auditora

Capítulo 6: Plan General del Proyecto

Para el proyecto se establece una duración estimada de 240 días laborables desarrollados en las siguientes etapas:

- Encuestas.- Entrevista preliminar con el Director de Operaciones y Sistemas para conocer el ambiente informático en el cual se desenvolverá la auditoria. Encuesta con el personal de las áreas de Tecnologia, también entrevistas con el personal operativo del Área de Operaciones, Centro de Cómputo, Sistemas y O&M para recabar documentación que comprenda las normativas de la Bolsa de Valores, Políticas y Procedimientos relativos al uso y protección de la información.

- Diseño de "checklist" para revisiones: Diseñar Cuestionarios "check-list" con preguntas cerradas basados en las Normas ISO 270002:2005 para obtener información de campo referente al cumplimiento de las normativas, políticas y procedimientos.

- Revisiones. Se realizó revisiones de los documentos y registros que soportan el cumplimiento de las normativas, políticas y procedimientos, para verificar que cumplan con el propósito de precautelar la seguridad de la información.

- Evaluación de la información recabada.- Elaboración de matrices y gráficos, con los resultados de la evaluación de riesgo, realizada al proceso que es soportado por el SEB.

- Preparación de Informe de auditoria. Desarrollo del Informe del proyecto y el informe de la auditoria incluyendo hallazgos y resultado de la evaluación de riesgo que se realizo.

Capítulo 7: Observaciones Adicionales

Para el correcto avance del proyecto de la auditoria del sistema SEB se establece los siguientes requerimientos:

- Un coordinador que acepte el seguimiento del proyecto por parte de la Bolsa de Valores de Guayaquil.
- Disponibilidad para acceder a un ambiente de laboratorio del SEB.
- La autorización de los Directivos, para entrevistar a los responsables del sistema SEB.
- Los permisos correspondientes, para acceder al Centro de Cómputo para la revisión de los Servidores donde se aloja la información propia del sistema.
- Un área fisica para el trabajar en la revisión de la documentación y la información recabada.

SECCIÓN 2: INFORME DE AUDITORÍA

1. Investigación Preliminar

1.1. Antecedentes

Previo a la obtención del Título de Diplomado Superior en Auditoría Informática en el Centro de Educación Continua de la ESPOL; las profesionales integrantes del equipo de trabajo Licenciada Mayra Benavides Rodríguez e Ingeniera Julia Macías Tulcán, desarrollan el proyecto final con el Tema: AUDITORIA DE LA SEGURIDAD DE LA INFORMACION EN EL SISTEMA ELECTRÓNICO BURSÁTIL (SEB), para lo cual el Centro de Educación Continua Dirigido por la MAE. Julia Bravo mediante oficio CEC-A-081-2010 de fecha 08 de Julio, solicitó a la Corporación Civil Bolsa de Valores de Guayaquil, la aprobación del Tema y lugar con los objetivos y alcance del documento que se anexó.

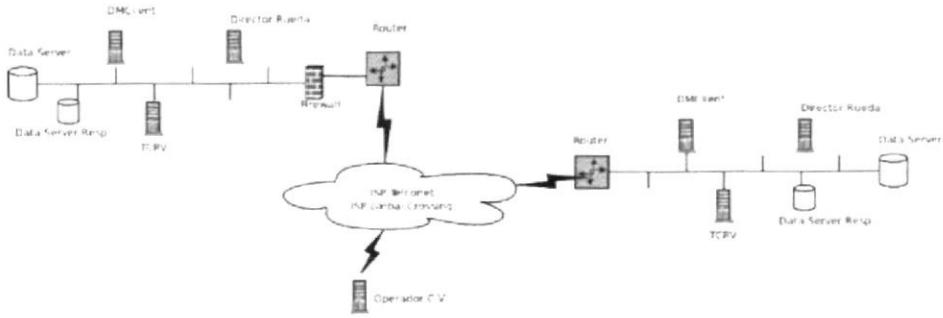
En virtud de lo solicitado, el Economista Arturo Bejarano Ycaza, Director General de la Bolsa de Valores de Guayaquil, autoriza mediante oficio DG.E.2010.0170 de fecha 20 de julio, el tema y lugar con los objetivos y alcance del documento, y designa al Ingeniero Luis Álvarez, como Coordinador del Proyecto y con quien debemos entrevistarnos para informar sobre las novedades y avance del Proyecto.

El SEB, Sistema Electrónico Bursátil versión 6.0.6.E; Diseñado por ICAP, es un Sistema de negociación electrónica, el cual permite la negociación entre participantes, así como la visualización de todas las demandas y ofertas del mercado.

El sistema incluye estadísticas y consultas para datos concurrentes e históricos.

Este sistema permite la exportación automática de información a Excel, así como el chat (comunicación) en línea con otros usuarios del sistema y una variedad de herramientas de operación.

La aplicación en el lado del cliente es actualizada en línea. Esto incluye los datos de la base de datos y la aplicación en si misma.



Esquema de funcionamiento del SEB

El sistema está compuesto por algunas aplicaciones que se ejecutan en el lado del cliente y del lado del servidor. La aplicación del lado del cliente se ejecuta en el sistema operativo Windows, mientras que las aplicaciones del lado del servidor se ejecutan en Red Hat Enterprise Linux (RHEL) del sistema operativo.

Las aplicaciones de servidor se pueden ejecutar en diferentes máquinas, pero por lo general se ejecutan en la misma.

La siguiente, son las aplicaciones básicas:

Data Server

Es un software de servidor que soporta conexiones de los clientes, así como de los demás servidores, envía la información que debe ser enviado a los clientes o las instituciones, configurado y autorizado. Permite conexiones con cifrado SSL para mayor seguridad. El uso o no de las conexiones SSL es configurable y depende de la red para ser utilizado y otros factores de seguridad que el administrador del sistema debe tener en cuenta.

Uno de sus principales funciones es recibir y distribuir la información generada en el sistema desde y hacia los distintos nodos conectados. Esta distribución de la información se realiza mediante listas de distribución entregado por la aplicación de servidor de gestión de datos.

Data Manager Server DMServer

Se trata de un software de servidor que mantiene y actualiza en línea la base de datos del sistema. Se verifica los permisos de acceso de los usuarios al sistema, los monitores de eventos determinados, como desconexiones, contraseñas erróneas. Se calcula y guarda las estadísticas del sistema, que se envían a los usuarios en tiempo real. Además, mantiene los datos históricos, que se envía a los usuarios de la demanda

Data Manager Cliente DMCliente

Se trata de una aplicación cliente (servidor) lateral que permite interactuar con el servidor de gestión de datos. Está dirigido a administradores de sistemas con el fin de que puedan gestionar la base de datos del sistema. Se utiliza para ver el estado de los usuarios en línea, la historia de las conexiones de usuario y desconexiones, la historia de las órdenes /operaciones, los gráficos de precios, montos transados y varias herramientas de administración como de los usuarios el control de versiones, las contraseñas y los usuarios los errores como archivo problemas de acceso.

Lenguaje de Programación

El DMClient la aplicación de los usuarios se desarrolla con un lenguaje propio especialmente diseñado para la implantación de sistemas transaccionales para los mercados financieros. Este lenguaje, llamado DFN, consiste en una fuente pre compilados para C/ C + +, adaptados y especializados para el tipo de software mencionado. Esta especialización del lenguaje mejora significativamente la cantidad de tiempo requerido para desarrollar un sistema.

Además, el sistema utiliza algunas bibliotecas de cálculo y de comunicación que por sus requisitos de alto rendimiento se han desarrollado utilizando Microsoft Visual C / C + +.

En el caso del DataServer es enteramente desarrollado en C / C + +.

Base de Datos

Cada cliente tiene en su máquina una estructura con los archivos necesarios para conectarse a los servidores. Para cada conexión el servidor enviará una copia fiel a la información pública. Cada cliente recibe también su información privada que también se almacena en los servidores, en caso de que un usuario pierda sus datos locales, puede utilizar uno nuevo para conectar con el sistema sin pérdida de información.

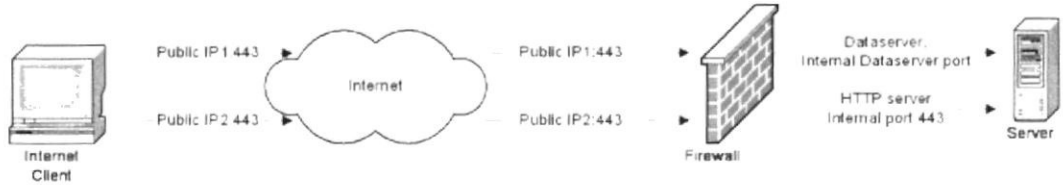
Esta configuración se utiliza en sistemas de tiempo real para proporcionar una mayor velocidad y capacidad en la respuesta a las consultas.

La información pública es la que está disponible para todos los participantes del mercado, tales como los precios y las cantidades de ofertas y demandas, y las veces que estas ofertas y demandas se hicieron (aunque no la identidad de los ofertantes y oferentes).

La información privada es la que está disponible sólo para una institución o rama, como el precio y la cantidad de operaciones donde fue la contraparte.

Se utiliza la base de datos + Ctree, distribuido por FairCom.

El DataServer se levanta diariamente: los Técnicos de Redeval que realizan funciones del Centro de Cómputo, acceden con el DDME (Administrador de Demonios en Linux) para levantar las aplicaciones Data Server, y DMServer en los Servidores de Quito y Guayaquil.



Esquema de intercambio de información del SEB

Este sistema fue evaluado en una Auditoría Externa realizada por la Escuela Superior Politécnica, en Septiembre del 2009, como parte del programa de trabajo que el

CNV pidió a las Bolsas de Valores de Guayaquil y Quito previo a dar una resolución sobre un proceso de unificación de los sistemas de negociación bursátil.

El CNV emitió una resolución final N° CNV-007-2011 del 05 de octubre del 2011 publicada en el R.O. N° 563 del 25 de octubre del 2011, en la que indica "Disponerse a las corporaciones civiles Bolsa de Valores de Quito y Bolsa de Valores de Guayaquil, la utilización de un solo sistema transaccional de negociación bursátil"

CARACTERÍSTICAS DE HARDWARE DEL SERVIDOR SEB

- Pentium IV
- Procesador Intel
- Velocidad 3 GHz
- Memoria Ram 2 GB
- Disco Duro 80 GB

CARACTERÍSTICAS DEL SOFTWARE

- Red HatEnterprice ES
- Linux Versión 3
- El Servidor SEB
- NO tiene Internet
- El Dmclient Si tiene acceso a Internet, pero para uso del usuario.
- El Director Si tiene acceso a Internet, pero para uso del Usuario.

La Red está protegida por un firewall - JUNIPER y lo controla La Empresa Global Crossing

1.2. Introducción a la Seguridad de la Información

Utilizar el término *seguridad de información*, no es otra cosa que la Protección de la Información y de los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada. Es importante, señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: La información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser hurtada, borrada o saboteada: Esto afecta su disponibilidad y la pone en riesgo. Además debemos considerar la información como un activo crítico de las organizaciones y como tal se debe preservar su integridad, confidencialidad y disponibilidad.

No obstante es preciso indicar que no es posible eliminar por completo los riesgos, sin embargo es posible reducirlos mediante la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar las amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo institucional, es decir, que contribuyan a proteger y salvaguardar, la información como los sistemas que la almacenan y administran.

Es importante que las empresas evalúen las vulnerabilidades, a las que están expuestos sus sistemas transaccionales y hagan un mejoramiento de sus controles, implementando estrategias que cubran todos los procesos.

Los riesgos son uno de los principales problemas en la seguridad que debe enfrentar TI, y para mitigar los daños que puedan generar, se deben adoptar medidas preventivas que eviten estos conflictos, y a la vez, disponer de un sistema en línea, que produzca con eficiencia, su actividad fundamental; aunque estas seguridades no brinden una cobertura total, por las amenazas diarias al sistema, deben generar un ambiente de confiabilidad y tranquilidad, por sus medidas implementadas.

1.3. Entorno Organizacional de la BVG

1.3.1. ORGANIZACIÓN INSTITUCIONAL

La Bolsa de Valores es un mercado en el que participan intermediarios (Operadores de Valores, representantes de Casas de Valores) debidamente autorizados con el propósito de realizar operaciones, por encargo de sus clientes, sean estas de compra o venta, de Títulos valores (acciones, pagarés, bonos, etc.) emitidos por empresas inscritas en ella (emisores).

El Objetivo principal de una Bolsa de Valores, es por lo tanto, brindar a sus miembros los servicios y mecanismos requeridos para la negociación de valores.

La Bolsa de Valores de Guayaquil, que nació como Compañía anónima en 1969, se transformó en Corporación Civil Sin Fines de Lucro el 4 de mayo de 1994, de acuerdo a la Ley de Mercadeo de Valores y se ubica bajo el control de la Superintendencia de Compañías. No obstante las bolsas tienen la capacidad de autorregularse, con la facultad de emitir las normas y reglamentos para controlar y supervisar las operaciones bursátiles.

De esta forma, la BVG provee el espacio físico, instalaciones, sistemas y toda la infraestructura institucional, para que las negociaciones de título valores, se desarrollen en forma ordenada, transparente y segura.

La BVG fue la primera bolsa del país en implementar el Sistema Electrónico Bursátil, conocido como Bolsa Electrónica, pionera en la automatización de la Rueda a Viva Voz para renta variable, así como en la utilización del Sistema de Compensación de Saldos Netos, que agilitó enormemente el pago de las operaciones de bolsa a través de transferencias de fondos en el Banco Central.

La Bolsa de Valores de Guayaquil, tiene un sistema de negociación electrónica el cual permite la negociación entre participantes, así como la visualización de todas las demandas y ofertas del mercado. Este sistema es vital para el servicio que brinda esta entidad a los miembros del Sector Financiero Bursátil y como tal debe mantener un nivel óptimo respecto a la seguridad de la información que procesa.

Presta los siguientes Servicios Transaccionales:

- Mecanismos de Negociación
- Tipos de Operaciones
- Sistemas de Liquidación
- Comisiones

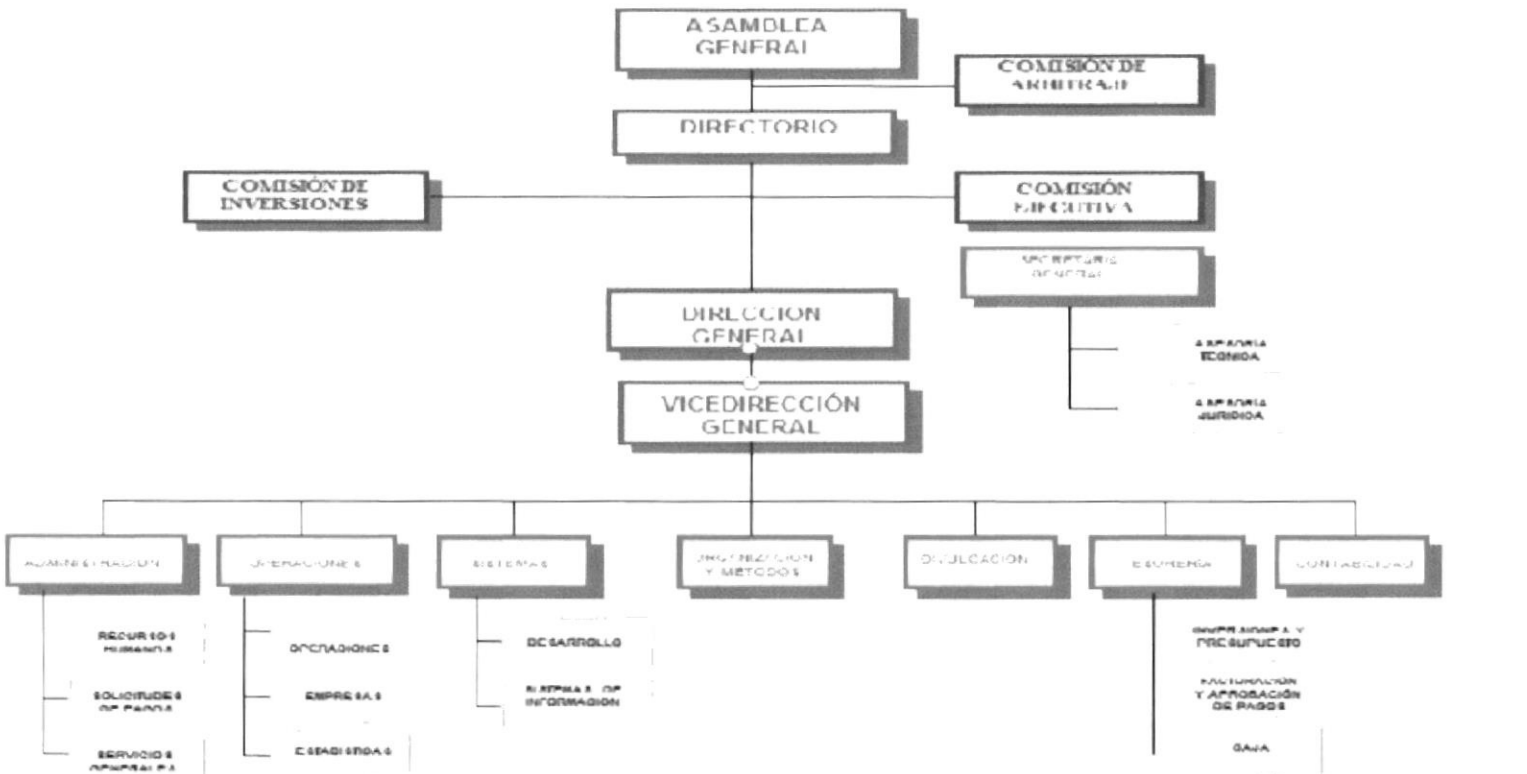
1.3.2. MISIÓN

Desarrollar el Mercado de Capitales del Ecuador sustentado en principios de transparencia, seguridad y sana competencia, generando servicios transaccionales y de información de constante innovación tecnológica. La Misión incluye impulsar el desarrollo de la cultura financiera en la sociedad y la inserción del Ecuador en los Mercados Financieros Internacionales.

1.3.3. VISIÓN

Crear medios necesarios para contribuir a lograr la distribución eficiente de la riqueza.

1.3.4. ESTRUCTURA ORGANIZACIONAL



DIRECTORIO DE LA BVG

PRINCIPALES

SECTOR EXTERNO

Ab. Rodolfo KronfleAkel - Presidente

Dr. Rómulo Gallegos Vallejo

Ing. Jorge García Torres

Dr. Juan Carlos Faidutti Estrada

SECTOR INTERNO

MAE. Paul Palacios Martínez

Sr. Víctor Abboud Fayad

Eco. Alfredo Barandearan Oyague

Ing. Xavier Neira Salazar

Dr. Jorge Andrade Avecillas

ALTERNOS

SECTOR EXTERNO

Ing. Francisco Ortega Gómez

Dr. Juan Trujillo Bustamante

Lcdo. Martín Fioravanti Villanueva

Ing. Markus Frey Keller

SECTOR INTERNO

Eco. Sergio Torassa Bertorino

Ing. Arturo Rodríguez Basurto

Lcda. Dora Lastra Guerrero

Lcdo. Germán Cobos Cajamarca

Ing. José Medina Serrano

DIRECTOR GENERAL

Eco. Arturo Bejarano Icaza

VICEDIRECTORA GENERAL

Anl. Oriana Rumbea Thomas

VICEDIRECTOR DE OPERACIONES Y SISTEMAS

Sr. Luis Álvarez Villamar

ASESORA INSTITUCIONAL

Srta. Carolina Márquez de la Plata

VICEDIRECTORA DE CONTABILIDAD

Eco. Silvia Guerrero

VICEDIRECTORA DE TESORERÍA

Ing. Noemi Moncayo

SECRETARIO GENERAL

Dr. Ricardo Gallegos

1.3.5. Políticas Institucionales

Los miembros de la Bolsa desarrollarán sus actuaciones profesionales de acuerdo con las normas, requisitos y procedimientos que rigen la formación y difusión de los precios de las operaciones que en ella se efectúan. A fin de conseguir el adecuado funcionamiento de este proceso de formación y difusión de precios.

Las Casas de Valores, adoptarán medidas de control adecuadas y suficientes, a fin de evitar que en la realización de sus operaciones puedan ser utilizadas, sin su conocimiento ni consentimiento, como

instrumentos para el ocultamiento, manejo, inversión o aprovechamiento en cualquier forma de dinero u otros bienes provenientes de actividades delictivas, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos vinculadas con las mismas.

Los miembros de la Bolsa introducirán los procedimientos operativos oportunos para identificar las operaciones efectuadas por sus empleados y personal y establecerán los registros y archivos que sean necesarios para conocer y seguir las operaciones que sus administradores, empleados y personal efectúen por cuenta propia sobre valores admitidos a negociación en esta Bolsa.

1.3.6. Políticas de Calidad

Nos comprometemos a generar continuamente productos y servicios transaccionales, de gestión, de control, de información e inscripción, de cumplimiento, sustentados en principios de transparencia, seguridad, eficiencia, equidad y confiabilidad; con sujeción al marco legal vigente y a nuestras normas de autorregulación, para impulsar el desarrollo del Mercado de Valores del Ecuador, procurar su inserción en los mercados internacionales, promover nuevas alternativas de financiamiento así como la cultura bursátil; y, estimular la distribución eficiente de la riqueza.

CAPÍTULO 2: Evaluación de riesgos

Es importante que las empresas evalúen los procesos de vulnerabilidades a los que están expuestos sus sistemas transaccionales, de manera que les permita implementar medidas estratégicas para mejorar los controles, y cubrir los desfases de seguridad.

Estos procesos de seguridad, brindaran a sus usuarios, un entorno bursátil coherente, con las políticas, de evitar riesgos innecesarios, en las diferentes fases de sus procesos financieros y de información.

CAPÍTULO 3: Objetivos de la Auditoria

1. Verificar la existencia y aplicación de planes, políticas y procedimientos relativos a la seguridad dentro de la organización.
2. Comprobar que los planes y políticas de seguridad y de recuperación, sean difundidos y conocidos por la alta dirección.
3. Evaluar el grado de compromiso por parte de la alta dirección, los departamentos usuarios y el personal de informática con el cumplimiento satisfactorio de los planes, políticas y procedimientos relativos a la seguridad.
4. Asegurar la disponibilidad y continuidad del equipo de cómputo el tiempo que requieran los usuarios para el procesamiento oportuno de sus aplicaciones
5. Asegurar que las políticas y procedimientos brinden confidencialidad a la información manejada en el medio de desarrollo, implantación, operación y mantenimiento.
6. Verificar que exista la seguridad requerida para el aseguramiento de la integridad de la información procesada en cuanto a totalidad y exactitud.
7. Constatar que se brinde la seguridad necesaria a los diferentes equipos de cómputo que existen en la organización.

8. Comprobar que existan los contratos de seguro necesarios para el hardware y software de la empresa (elementos requeridos para el funcionamiento continuo de las aplicaciones básicas).

9. Confirmar la presencia de una función responsable de la administración de la seguridad en:

    1. Recursos humanos, materiales y financieros relacionados con la tecnología de informática.

    2. Recursos tecnológicos de informática.

10. Evaluar las especificaciones para la seguridad del Sistema SEB

11. Verificar que los manuales de funcionalidad existan y se encuentren actualizados con las últimas versiones del SEB

12. Verificar que los procedimientos de instalación segura y puesta en marcha se encuentren documentados y aplicados.

13. Verificar que las versiones del SEB hayan sido correctamente tratadas.

14. Verificar que las pruebas de desarrollo y configuración del SEB se ejecuten y se haga un registro de ellas.

CAPÍTULO 4: Áreas o componentes a auditar

Las áreas, según la estructura organizacional, que se han considerado para la auditoria son:

- Dirección del Sistemas
- Sub-Dirección de Organización y Métodos.
- Sistemas
- Centro de Computo- Soporte de REDEVAL
- Proveedor de Sistemas ICAP.

CAPÍTULO 5: Alcance de la auditoria

El alcance la Auditoria comprende:

- Revisión de Politicas y Procedimientos relativos a la Seguridad de la Información que corresponden al proceso de Rueda Bursátil, a través del Sistema Electrónico Bursátil. Comprendiendo una revisión de documentación y registros obtenidos del proceso.
- Evaluación de controles implementados por el área de Tecnologia, para mitigar riesgos de seguridad de información en forma general.
- Evaluación del proceso de Desarrollo y/o adquisición de software.

CAPÍTULO 6: Criterios de auditoría a utilizarse

6.1 Sistemas de Gestión de la Seguridad de la Información

6.1.1 Estándares relacionados a la Seguridad de la Información

ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles o implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007.

Otros países donde también está publicada en español son, por ejemplo, Colombia, Venezuela y Argentina. El original en inglés y la traducción al francés pueden adquirirse en ISO.org.

• ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org

ISO 27005: Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en

la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.

MAGERIT – versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Cap. III: Guías de Técnicas. Son las técnicas utilizadas en los proyectos de análisis y gestión de riesgos.

COSO.- Factor identificado que podría afectar la consecución de un objetivo.

COBIT.- El potencial de que una amenaza dada explote las vulnerabilidades de un activo o grupo de activos, causando pérdida o daño a los mismos.

CAPÍTULO 7: Recursos de Personal

7.1 Por la Bolsa de Valores de Guayaquil

- Director de Operaciones y Sistemas
- Anl. del área de Sistemas
- Encargada de la administración del SEB por parte de REDEVAL
- Área de sistemas

CAPÍTULO 8: Herramientas y técnicas

8.1 Herramientas y Técnicas

8.1.1. Herramientas

- Cuestionarios basados en la Norma ISO 27001 y ISO 27002
- Cuestionarios basados en la Norma ISO 27005
- Cuadros de Resultados presentados en GráficosNormas ISO 27002

8.1.2. **Técnicas.**

- Elaboración de Check-list con preguntas cerradas (Si/No y No Aplica): Se elaboraron varios checklist con preguntas basados en los controles de la Norma ISO 27002 y la Norma ISO 15408 en las que los encuestados respondieron si o no, pero también tenia espacio para alguna observación importante que se quiera dar para acompañar a la respuesta.
- Elaboración de cuadros para Tasación: Utilizamos cuadros para solicitar al personal clave, que nos ayude haciendo una tasación de los Activos de Información.
- Técnicas especificas para el análisis y gestión de riesgos de la Metodología de Magerit version 2

  1. Uso de tablas para la obtención sencilla de resultados
  2. Técnicas algoritmicas para la obtención de resultados elaborados.

CAPÍTULO 9: Plan de Comunicación

Comunicación Formal escrita

Para el efecto se han dispuesto las siguientes cuentas de correo electrónico

Auditoras:

Julia Macías: julyemacias@hotmail.com y julyemacias@deecvale.com

Mayra Benavidez: mayra_benavid2@hotmail.com

Por la BVG

Luis Álvarez: lalvarez@bvg.fin.ec y luisalvarez@deecvale.com

Heleg Egas: hegas@bvg.fin.ec

CAPÍTULO 10: Programa de auditoria

10.1 Análisis de Riesgo

10.1.1 Marco Teórico

SEGURIDAD DE LA INFORMACION

La seguridad de la información se caracteriza por la preservación de:

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

Evento de seguridad de la información. Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

[ISOIIEC TR 18044:2000]

Activos de información.- Se entiende al conjunto de elementos con valor informativo que son propiedad de una empresa, institución o individuo, y que reflejan su actividad.

Amenaza. Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

[NTC 5411-1:2006]

Análisis de riesgos. Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

[ISO/IEC Guía 73:2002]

Confidencialidad.- La información está protegida de personas no autorizadas.

Definición de riesgo según COSO

(Comitee of Sponsoring Organizations of the tread way commission – 1992)

Factor identificado que podría afectar la consecución de un objetivo.

Definición de riesgo según ISO

(Guidelines for the Management of It Security)

El potencial de que una amenaza dada explote las vulnerabilidades de un activo o grupo de activos, causando pérdida o daño a los mismos.

Disponibilidad.- Los usuarios tienen acceso a la información y a los activos asociados cuando lo requieran.

Integridad.- La información está como se pretende, sin modificaciones inapropiadas.

Política. Toda intención y directriz expresada formalmente por la Dirección.

Riesgo. Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC Guía 73:2002]

Vulnerabilidad. Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

[NTC 5411-1:2006]

Gobierno Corporativo.- Definición

Sistemas y procesos que una empresa pone en funcionamiento para proteger los derechos de sus "grupos de interés" (stakeholders).

- Accionistas
- Inversores
- Empleados
- Comunidad
- Clientes
- Proveedores
- Acreedores
- Estado

10.1.2 Análisis de Riesgo para la Bolsa de Valores

Se aplico la herramienta para Tasación de Activos recomendada por el Ing. Lenin Espinoza con las siguientes personas:

Director de Operaciones y Sistemas

Sub-Director de Operaciones

Analista de Sistemas

Jefe de Soporte del REDEVAL.

10.1.3 Objetivos del Análisis de Riesgo.

- Identificación de los procesos críticos de la Bolsa de Valores.
- Identificación de los activos de información de un proceso crítico ya seleccionado.
- Identificar Amenazas, Vulnerabilidades y riesgo de los activos de información.
- Sugerir controles basados en los Objetivos de Control de ISO 270002.

10.1.4 Identificación de Riesgos

Resumen de pruebas realizadas y hallazgos

REVISIÓN DE LAS RECOMENDACIONES DADAS POR LA ESPOL A BVG

Se hizo una revisión de la adopción que la Bolsa de Valores de Guayaquil, hizo a las recomendaciones sugeridas por los auditores externos en la Auditoría del SEB realizada en septiembre del 2009

PRUEBAS DE LABORATORIO

DMCLIENT

- Se constató que permite monitorear el estado de las posturas que han puesto los operadores de bolsa (usuarios del sistema), no tiene opciones para hacer modificaciones a estas posturas.
- Se constató que la aplicación muestra un log de las actividades de los usuarios y este tiene un histórico que está almacenado físicamente en el Server.

- Se constató que la aplicación tiene una ventana de monitoreo de sucesos importantes que alerta sobre errores de acceso de usuarios, intentos fallidos, y caídas de conexión de los usuarios.

- Se constató que el equipo donde está esta aplicación en producción, tiene habilitado el uso libre de navegación por internet y en toda la red ya que este equipo sirve también para administración de red.

DIRECTOR

- El Modulo de Director está en un equipo ubicado en el Dpto. de Operaciones, con sistema operativo Windows 2003 Server.

- Se constató que esta aplicación permite hacer configuraciones para que se inicie o finalicen las transacciones mercantiles diariamente.

- Se constató que este equipo está habilitado para que el usuario tenga navegación por internet, controlada por el firewall
  El firewall que utilizan es un Juniper que es administrado remotamente por el proveedor Global Crossing. Cualquier cambio en las políticas se debe solicitar mediante un ticket de requerimiento.

CONTROL DE ACCESO

- Se verificó que las claves de usuarios no son limitadas, pueden poner cualquier clave ej.: clave 123 (dentro de recomendaciones).

- En el Documento Titulado Política de Creación de Usuarios no se contempla esta parte.

- No es posible validar, que la persona que actúa con el usuario y clave, sea el Operador Autorizado de Bolsa. Pero la Política indica que solo este puede utilizar el usuario y clave.

- En el Control de cambios de versiones, no se lleva un control estricto del levantamiento de requerimientos, aunque existen los formatos y están los procedimientos. No se apegan a los lineamientos ya documentados.

- Existen formatos desactualizados en las revisiones de versiones nuevas.

- No hemos tenido acceso directo al archivo logs que están en el servidor, sino mediante una aplicación del data server.

AMBIENTE INFORMATICO

Las tareas de operatividad del SEB las realiza el personal de REDEVAL y también realizan tareas de soporte técnico.

Desarrollo de sistemas

1. Procedimientos de etapas de desarrollo

- Existe pero no lo utilizan para el SEB

- Se utiliza para solicitar a ICAP

- Existe una metodología pero no se lleva un control de las etapas de desarrollo del proveedor

2. Revisar respaldos y versiones

- Son guardados

- Se los baja x FTP

- En un Equipo de centro de cómputo, se almacenaran por espacio.

- Revisar formatos de requerimientos de usuario

- Revisar Formatos de Plan de pruebas
    - Control de requerimientos (se envía a jefes)
        - For 38
- Se verificó log de actualizaciones de antivirus
    - Las licencias están actualizadas

10.1.5 Evaluación de Riesgos

"Del buen entendimiento del proceso dependerá la identificación de riesgos y los controles que los mitigan. En la identificación de riesgos es importante que se consideren los factores que pueden incrementar los riesgos, tales como la calidad del personal, experiencias en la obtención de objetivos, complejidad de una actividad, distribución geográfica de las actividades, entre otras. La asociación"

Auditool.com

10.1.6 Ejecución de la evaluación de riesgo

ANALISIS Y EVALUACION DEL RIESGO PARA - TASACIÓN DE ACTIVOS DE INFORMACIÓN

EMPRESA: BOLSA DE VALORES DE GUAYAQUIL
PROCESO:OPERACIONES-

SUBPROCESO: RUEDA ELECTRONICA
Persona Encuestada: Luis Alvarez

SISTEMA: SISTEMA ELECTRONICO BURSATIL -SEB
Cargo: Director de Sistemas y Operaciones

Los activos de información identificados han sido tasados y se han ordenado de mayor a menor promedio de tasación

	ACTIVOS	TASACIÓN			
		NCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
	INFRAESTRUCTURA				
1	Servidor SEB Guayaquil	5	5	5	5
2	Servidor SEB Quito DATA SERVER	5	5	5	5
3	Servidor SEB Guayaquil-Respaldo	5	5	4	5
4	Servidor SEB Quito Respaldo	5	5	4	5
5	Equipo DMClient Guayaquil	5	5	4	5
6	Equipo Director (Guayaquil)	5	5	4	5
7	Firewall Juniper	3	4	4	4
	router Global Crossing	3	4	4	4
	router Telconet	3	4	4	4
	Sistema operativo Red Hat Enterprice ES Linux Version 3 de Servidor SEB Guayaquil y Quito	3	3	4	3
	Windows XP SP 3 en equipos PC	2	3	4	3
	RED intranet	2	4	3	3
	Balanceador de carga 3Com	2	4	3	3
	Equipo TCRV Impresión en Linea	2	3	3	3
	Servidor de Antivirus	2	2	2	2
	APLICACIONES				
	Data Server DS	4	5	5	5
	Data Manager Server DMS	4	5	5	5
	SEB-DMClient	4	4	5	4
	SEB-Director	4	5	5	5
	TCRV Impresion en linea envia los archivos planos a la	3	4	4	4
	Symantec Backup	3	4	3	3
	I.S.P. Telconet	3	3	4	3
	I.S.P. Global Crossing	3	3	4	3
	DDMW Administrador de Demonios para subir las aplicaciones y d	3	3	3	3
	Sophos version 9.5 Antivirus para Windows	1	3	3	2
	PERSONAS				
	Sub-Director de Operaciones	5	5	4	5
	Asistente de Operaciones	5	5	4	5
	Operador de Casa de valores	5	5	4	5
	Director de Operaciones	4	5	3	4
	Director de Sistemas	4	5	3	4
	Jefe de Soporte Técnico REDEVAL	4	3	3	3
	Técnico de REDEVAL en Centro de Computo Guayaquil	4	3	2	3
	Técnico de REDEVAL en Centro de Computo Quito	4	3	2	3
	BASE DE DATOS DE INFORMACION				
	CTREE+	5	5	5	5
	Respaldos de ultima version de la aplicación	4	5	4	4
	DATOS				
	INFORMACIÓN DE POSTURAS DE OFERTAS	5	5	5	5
	INFORMACIÓN DE RUEDAS	5	5	5	5
	INFORMACION DE POSTURAS DE DEMANDAS	5	5	5	5
	PRECIOS Y CANTIDADES DE LAS OPERACIONES	3	5	5	4
	INFORMACIÓN DE EMISORES DE TITULOS	3	4	5	4
	INFORMACION DE IDENTIDAD DE OFERTANTES Y DEMANDANTE	5	5	5	5
	DOCUMENTACION				
	REPORTES DE LIQUIDACIONES	3	5	4	4
	AUTORIZACIONES PARACREAR USUARIOS DE OPERADORES DE CASAS DE VALORES	3	3	4	3
	TITULOS VALORES QUE SE NEGOCIAN	2	4	4	3
	MANUALES DE USUARIO DEL SEB PARA OPERADORES DE CASAS DE VALORES	2	3	3	3

Tasación

Valor	Grado
5	Muy Alta
4	Alta
3	Medio Alta
2	Medio Baja
1	Baja

ANALISIS Y EVALUACIÓN DE RIESGO

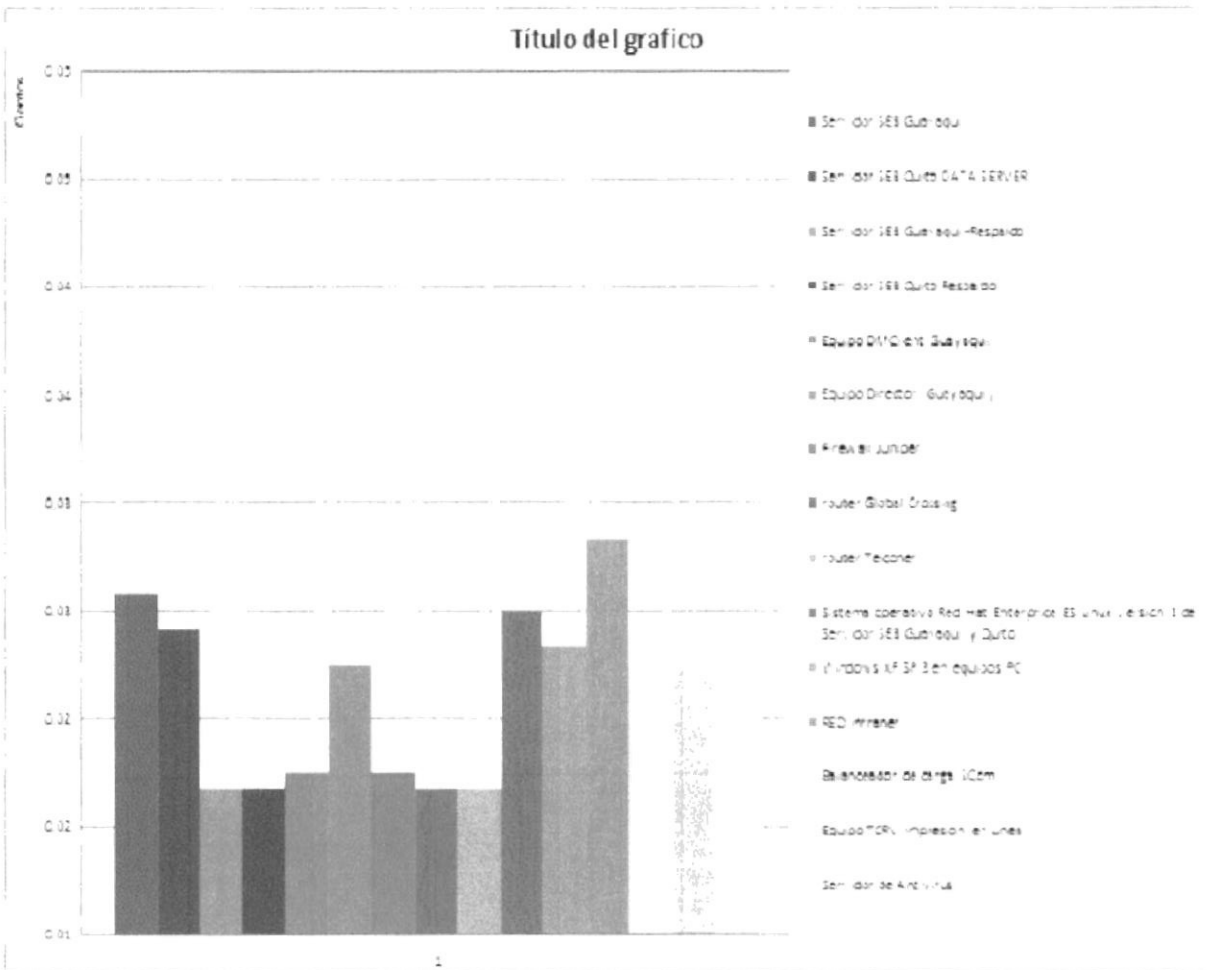
ANLALISIS Y EVALUACION DEL RIESGO
IDENTIFICACION DE YULNERABILIDADES

ACTIVOS		TASACIÓN				AMENAZAS				VULNERABILIDADES				RIESGO DE LA AMENAZA DE CARA A LA				CONTROLES
No.	Activo de Información	C	I	D	Tasación (Promedio)	Descripción	F	M	Calificación de Riesgo de Amenaza	Descripción	P	M1	Calificación de Riesgo de la Vulnerabil	Probabilidad	Impacto	Total de la Amen por el vulnerabilidad)	Total de amenaza por cada activo	Seleccion de Controles
1	Servidor SEB Guayaquil	5	5	5	5	Hacking de información	2	4	2	Utiliza enlaces públicos para tráfico de Internet	2	4	2,5	2,5	4	2,25		11.4.3 Identificación de equipos en las redes
						Virus en el Bios	1	3	2	El equipo ya tiene mas de 4 años en uso constante	2	3	2,5	1,5	3	2,25		9.2.4 Mantenimiento de
						Deterioro Físico	1	3	2		2	3	2,5	1,5	3	2,25	2,58	9.2.4 Mantenimiento de Eq
	Servidor SEB Quito DATA SERVER	5	5	5	5	Daño en Disco	2	3	2,5	Poco control del trabajo de mantenimiento contratado	3	3	3	2,5	3	2,75		9.2.4 Mantenimiento de Eq
						Daño en Tarjetas Controladoras de Disco	1	3	2		2	3	2,5	1,5	3	2,25		9.2.4 Mantenimiento de Eq
						Falla de Memoria	1	3	2		2	3	2,5	1,5	3	2,25	2,42	9.2.4 Mantenimiento de Eq
	Servidor SEB Guayaquil-Respaldo	5	5	4	5	Falta de espacio en el disco	3	3	3		1	1	1	2	2	2		9.2.2 Instalacion de suminis
						Obsolecencia de hardware	1	3	2		1	1	1	1	2	**1,5**		9.2.4 Mantenimiento de Eq
						Hacking de información	1	2	2		1	1	1	1	2	**1,5**	1,666666667	11.4.3 Identificación de
	Servidor SEB Quito Respaldo	5	5	4	5	Falta de espacio en el disco	3	3	3		1	1	1	2	2	2		
						Obsolecencia de hardware	1	3	2		1	1	1	1	2	**1,5**		
						Variaciones de voltaje	1	3	2		1	1	1	1	2	**1,5**	1,666666667	
	Equipo DMClient Guayaquil	5	5	4	5	Falta de espacio en el disco	2	3	2,5		1	1	1	1,5	2	1,75		
						Obsolecencia de hardware	2	3	2,5		1	1	1	1,5	2	1,75		
						Hacking de información	2	3	2,5		1	1	1	1,5	2	1,75	1,75	
	Equipo Director (Guayaquil)	5	5	4	5	Ataques de virus que se infectan por la red	4	4	4		1	1	1	2,5	2,5	2,5		
						Falla de Memoria por quedarse sin espacio	3	4	3,5		1	1	1	2	2,5	2,25		
						Falta de espacio en el disco	2	4	3		1	1	1	1,5	2,5	2	2,25	
	Firewall Juniper	3	4	4	4	Ataques de hacking black	1	3	2		1	1	1	1	2	**1,5**		10.6.1 Controles de red
						Saturación del trafico	2	4	3		1	1	1	1,5	2,5	2		10.6.2 Seguridad de los ser
						Deterioro propio por desgaste de hardware	1	4	2,5		1	1	1	1	2,5	1,75	1,75	7.1.1 Inventario de Activos
	router Global Crossing	3	4	4	4	Virus en el Spyware y ataques de intrusos	1	3	2		1	1	1	1	2	**1,5**		
						Saturacion de trafico de navegacion en internet	3	3	3		1	1	1	2	2	2		11.4.1 Política de uso de los servicios de la red
						Deterioro propio por desgaste de hardware	1	3	2		1	1	1	1	2	**1,5**	1,67	7.1.3 Uso aceptable de los activos
	router Telconet					Virus en el Spyware y ataques de intrusos	1	3	2		1	1	1	1	2	**1,5**		
						Saturacion de trafico de navegacion en internet	3	3	3		1	1	1	2	2	2		

TasActivo Contestado **INFRAESTRUCTURA** APLICACIONES PERSONAS BASE DE DATOS DATOS

Resumen

Servidor SEB Guayaquil	2,58
Servidor SEB Quito DATA SERVE	2,42
Servidor SEB Guayaquil-Respaldo	1,67
Servidor SEB Quito Respaldo	1,67
Equipo DMClient Guayacuil	1,75
Equipo Director (Guayaquil	2,25
Firewall Juniper	1,75
router Global Crossing	1,67
router Telconet	1,67
Sistema operativo Red Hat Enterp	2,50
Windows XP SP 3 en equipos PC	2,33
RED Intranet	2,83
Balanceador de carga 3Com	2,25
Equipo TCRV Impresión en Lines	2,25
Servidor de Antivirus	2,42

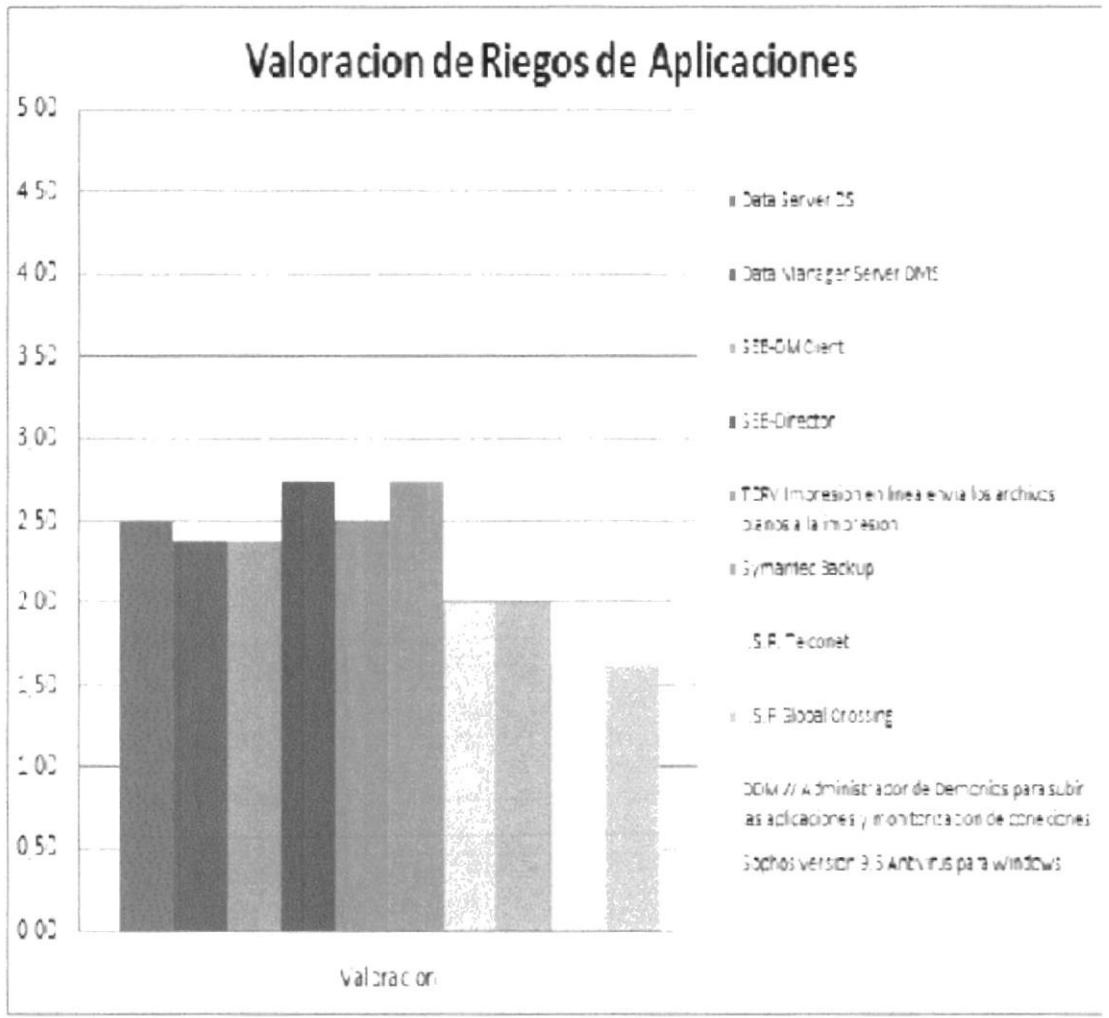


ANALISIS Y EVALUACION DEL RIESGO
IDENTIFICACION DE VULNERABILIDADES

ACTIVOS		TASACIÓN				AMENAZAS				VULNERABILIDADES				RIESGO DE LA AMENAZA DE CARA A LA VULNERABILIDAD				CONTROLES
No.	Activo de Información	C	I	D	Tasación (Promedio)	Descripción	F	M	Calificación de Riesgo de Amenaza	Descripción	F	M	Calificación de ...	Probabilidad	Impacto	Total de la Amenaza por vulnerabilidad	Total de amenazas por Activo	Selección de Controles
1	Data Server DS	4	5	5	5	Perdida de conexión con una de las nodos interconectados	1	5	3	Los nodos estan conectados mediante internet	1	3	2	1	4	2,50		12.6.1 Control de las vulnerabilidades técnicas
						Manejo inadecuado de datos criticos	1	5	3	La data es transportada a través de internet	1	3	2	1	4	2,50	2,50	12.4.1 Control de software de explotación
2	Data Manager Server DMS	4	3	3	3	Perdida de conexión	1	5	3	El equipo esta conectado a la misma red que todos los demas equipos	1	3	2	1	4	2,50		12.2.3 Integridad de los mensajes
						Errores de acceso de usuarios	2	4	3	Se utiliza un solo usuario para acceder	1	2	1,5	1,5	3	2,25	2,38	
3	SEB-DMClient	4	4	5	4	Perdida de conexión con el Servidor	1	5	3	El equipo esta conectado a la misma red que todos los demas equipos	1	2	1,5	1	3,5	2,25		12.2.1 Validacion de datos de entrada
						Errores de configuracion de parametros	2	5	3,5	No existe una politica definida en documentación de los parametros de configuración	1	2	1,5	1,5	3,5	2,50	2,38	
4	SEB-Director	4	5	5	5	Fallas en ingreso de datos	3	4	3,5	Existen Datos que no se controlan en el ingreso para que pueden ser erroneos Ej. El tipo de subasta	1	3	2	2	3,5	2,75		12.2.1 Validacion de datos de entrada
						Accesos no autorizados a la aplicación	2	5	3,5	El equipo tiene acceso a la navegación por internet con permisos dados por el proxy	1	3	2	1,5	4	2,75	2,75	12.3.2 Gestion de claves
	TCRV Impresion en linea envio los archivos planos a la impresión	3	4	4	4	Perdida de conexión con el Servidor	2	4	3	El equipo esta conectado a la misma red que todos los demas equipos	1	3	2	1,5	3,5	2,50		11.4.1 Politicas de uso de los servicios de red
						Error por desconfiguración de parametros	2	4	3	Los cambios en la configuración de parametros no se registran	1	3	2	1,5	3,5	2,50	2,50	11.6.1 Restriccion de acceso a la información
6	Symantec Backup	3	4	3	3	Ejecucion arbitraria de codigos	2	4	3	no valida la información de identidad enviada entre el servidor media y el agente remoto, que permite a los atacantes de hombre en medio (man in the middle) para ejecutar comandos NDMP a través de de vectores no especificados.	2	3	2,5	2	3,5	2,75		11.6.1 Restriccion de acceso a la información
						Accesos no autorizados a la aplicación	3	4	3,5		1	3	2	2	3,5	2,75	2,75	11.6.1 Restriccion de acceso a la información
7	I.S.P. Telconet	3	3	4	3	Falta de Disponibilidad	2	3	2,5	El SEB esta configurado para conectarse por Internet	1	1	1	1,5	2	1,75		12.2.2 Control de procesamiento interno
						Ataques de hacking	3	4	3,5	Equipos con IP publica no protegidos que pueden ser puertas abiertas	1	1	1	2	2,5	2,25	2,00	11.6.2 Aislamiento de los sistemas sensibles
[illegible]	I.S.P Global Crossing	2	2	4	2	Falta de Disponibilidad	2	3	2,5	El SEB esta configurado para conectarse por Internet	1	1	1	1,5	2	1,75		12.2.2 Control de procesamiento interno
						Ataques de hacking	3	4	3,5	Equipos con IP publica no protegidos que pueden ser puertas abiertas	1	1	1	2	2,5	2,25	2,00	11.6.2 Aislamiento de los sistemas sensibles
9	DDME Administrador de Demonios para subir las aplicaciones y monitorizacion de conexiones	3	3	3	3	Errores de configuracion de parametros	1	3	2	No existe una politica definida en documentación de los parametros de configuración	1	1	1	1	2	1,50		10.1.1 Documentacion de los procedimientos de operación
						Desconexion con el server	2	3	2,5	El equipo esta conectado a la misma red que todos los demas equipos	1	1	1	1,5	2	1,75	1,63	11.4.5 Segregación de redes 11.4.6 Control de la conexión a la red
10	Sophos version 9.5 Antivirus para Windows	1	3	3	2	Paso por alto spyware por desactualizacion	3	2	2,5	debilidad en el sistema de encriptación de firmas de antivirus,	1	1	1	2	1,5	1,75		10.4.1 Controles contra el codigo malicioso
						Los usuarios descargan informacion no autorizada en sus equipos	2	2	2	el mecanismo de almacenamiento de datos cifrados, ya que estos se guardan en un archivo de texto simple	1	1	1	1,5	1,5	1,50	1,63	10.4.2 Controles contra el codigo descargado en el cliente

TasActivo Contestado INFRAESTRUCTURA **APLICACIONES** PERSONAS BASE DE DATOS DATOS

Resumen	Valoracion
Data Server DS	2,50
Data Manager Server DMS	2,38
SEB-DM Client	2,38
SEB-Director	2,75
TCRV Impresion en linea envia los archivos planos a la impresion	2,50
Symantec Backup	2,75
I.S.P. Telconet	2,00
I.S.P. Global Crossing	2,00
DDMV Administrador de De	1,63
Sophos version 9.5 Antivirus para Windows	1,63



ANLALISIS Y EVALUACION DEL RIESGO
IDENTIFICACION DE VULNERABILIDADES

ACTIVOS		TASACION				AMENAZAS				VULNERABILIDADES				RIESGO DE LA AMENAZA DE CARA A LA				CONTROLES
No.	Activo de Información	C	I	D	Tasación (Promedio)	Descripción	F	M	Calificación de Riesgo de Amenaza	Descripción	P	Mt	Calificacion de Riesgo de la Vulnerabili	Probabilidad	Impacto	Total de la Amen por c/vulnerabilidad)	Total amenaza po Activo	Selección de Controles
1	Sub-Director de Operaciones	5	5	4	5	Divulgacion de información confidencial de terceros	1	3	2	Poco conocimiento del concepto de sigilo bursatil	1	2	1,5	1	2,5	1,75	2,333333	
						Alterar el proceso ordinario de formación de precios	2	3	2,5	El proceso de formación de precios es de cambios constantes	1	3	2	1,5	3	2,25		8.2.2 Concienciación,formación y capacitacion en seguridad de la informacion
						Falta de control de la transparencia de las negociaciones efectuadas en las ruedas bursatiles	3	4	3,5	El conocimiento de las herramientas de control del sistema puede ser complejo	2	3	2,5	2,5	3,5	3		8.1.1 Funciones y responsabilidades
	Asistente de Operaciones	5	5	4	5	Transmision de claves por telefono	3	3	3	La presura de cerrar una negociación puede resultar apremiante	3	3	3	3	3	3	2,67	8.1.1 Funciones y responsabilidades
						Falta a la confidencialidad o imprudencias en dar informacion confidencial	3	3	3	El codigo de conducta no especifica situaciones de este tipo por lo tanto no se incluyen sanciones	3	3	3	3	3	3		6.1.1 Acuerdos de Confidencialidad 8.1.3 Terminos y condiciones de Contratación
						Venta de información bursatil	1	3	2	Poca cultura de seguridad	1	3	2	1	3	2		8.2.2 Concienciación,formación y capacitacion en seguridad de la informacion
	Operador de Casa de Valores	5	5	4	5	Fallas Operativas	4	4	4	No es frecuente que se audite los procedimientos para disminuir errores	4	4	4	4	4	4	3,25	10.10.1 Registro de auditorias
						Sustracción o utilización de información de terceros sin autorización	2	4	3	Poca cultura bursatil del publico comun	1	4	2,5	1,5	4	2,75		
						Fraude al utilizar valores de terceros sin autorización de	2	4	3	Crisis economica del pais	2	4	3	2	4	3		8.2.3 Proceso Disciplinario
	Director de Operaciones	4	5	3	4	Autorizar que se proceda a correcciones de negociaciones cerradas	2	3	2,5	Las negociaciones se conforman de mucha información	2	3	2,5	2	3	2,5	2,75	
						Conflictos de intereses	4	3	3,5	Las personas suelen tener intereses economicos	3	3	3	3,5	3	3,25		8.1.2 Investigacion y antecedentes
						Olvido o negligencia para cumplir con regulaciones establecidas para su cargo	2	3	2,5	La presión por cumplir con las responsabilidades del cargo de director de operaciones y sistemas	2	3	2,5	2	3	2,5		8.2.1 Responsabilidades de la direccion
						Autorizar la implatacion de Sistemas con errores	3	5	4	La presión por cumplir con las responsabilidades del cargo de director de operaciones y sistemas	2	4	3	2,5	4,5	3,5		8.2.1 Responsabilidades de la direccion

TasActivo Contestado INFRAESTRUCTURA APLICACIONES **PERSONAS** BASE DE DATOS DATOS

Leyenda en la página 43

7		4	5	3	4	Olvido o negligencia para cumplir con regulaciones establecidas para su cargo	2	3	2,5	La presión por cumplir con las responsabilidades del cargo de director de operaciones y sistemas	2	3	2,5	2	3	3,5	2,75	8.2.1 Responsabilidades de la dirección
8	Director de Sistemas					Autorizar la implantación de Sistemas con errores	3	5	4	La presión por cumplir con las responsabilidades del cargo de director de operaciones y sistemas	2	4	3	2,5	4,5	3,5		8.2. Responsabilidades de la dirección
9						No cumplir los plazos de los proyectos de tecnología	4	4	4	Poco conocimiento de administración de proyectos	3	4	3,5	3,5	4	3,75		10.2.1 Responsabilidades y
10		4	5	3	4	Incumplimiento de competencias establecidas	3	3	3	No se supervisa sus actividades	3	3	3	3	3	3	3,416667	
11	Jefe de Soporte Técnico REDEVAL					Hacker, cliker de información	4	3	3,5	Dependencia de una sola persona quien conoce completamente la herramienta tecnológica	1	3	2	2,5	3	2,75		
12						Acceso de personas no autorizadas	3	4	3,5	Solo el centro de computo tiene control de acceso mediante medios magnéticos	1	3	2	2	3,5	2,75		
13		4	3	3	3	Falta de capacidad para instruir a su personal a cargo	3	3	3	Muy poca preocupación por capacitarse en manejo de personal	1	3	2	2	3	2,5	2,67	
14	Técnico de REDEVAL en Centro de Computo Guayaquil					Desprolijidad en el tratamiento de los equipos	4	4	4	Falta de supervision de las actividades que desarrolla los técnicos	2	4	3	3	4	3,5		
15						Profesionales sin conocimiento previo de tipo de negocio	4	3	3,5	El tipo de negocio de la institución no es muy difundido	5	5	5	4,5	4	4,25		
16		4	3	2	3	Intrusiones de personas no autorizadas	3	3	3	Solo el centro de computo tiene control de acceso mediante medios magnéticos	4	4	4	3,5	3,5	3,5	3,75	11.2.4 Revision de acceso de usuarios
17	Técnico de REDEVAL en Centro de Computo Quito					Exceso de atribuciones o confianza ciega del personal	3	3	3	Poca difusión de las políticas internas al personal	4	4	4	3,5	3,5	3,5		
18						Profesionales sin conocimiento previo de tipo negocio	3	3	3	El tipo de negocio de la institución no es muy difundido	3	4	3,5	3	3,5	3,25		8.1.2 Investigación de antecedentes
19		4	3	2	3	Rotacion de Personal	2	4	3	La contratación del personal no esta definida correctamente y su remuneración economica no esta conforme	2	4	3	2	4	3	3,25	8.1.3 Terminos y condiciones de Contratacion

Factores de Calificacion de Activo
I Integridad
C Confidencialidad
D Disponibilidad

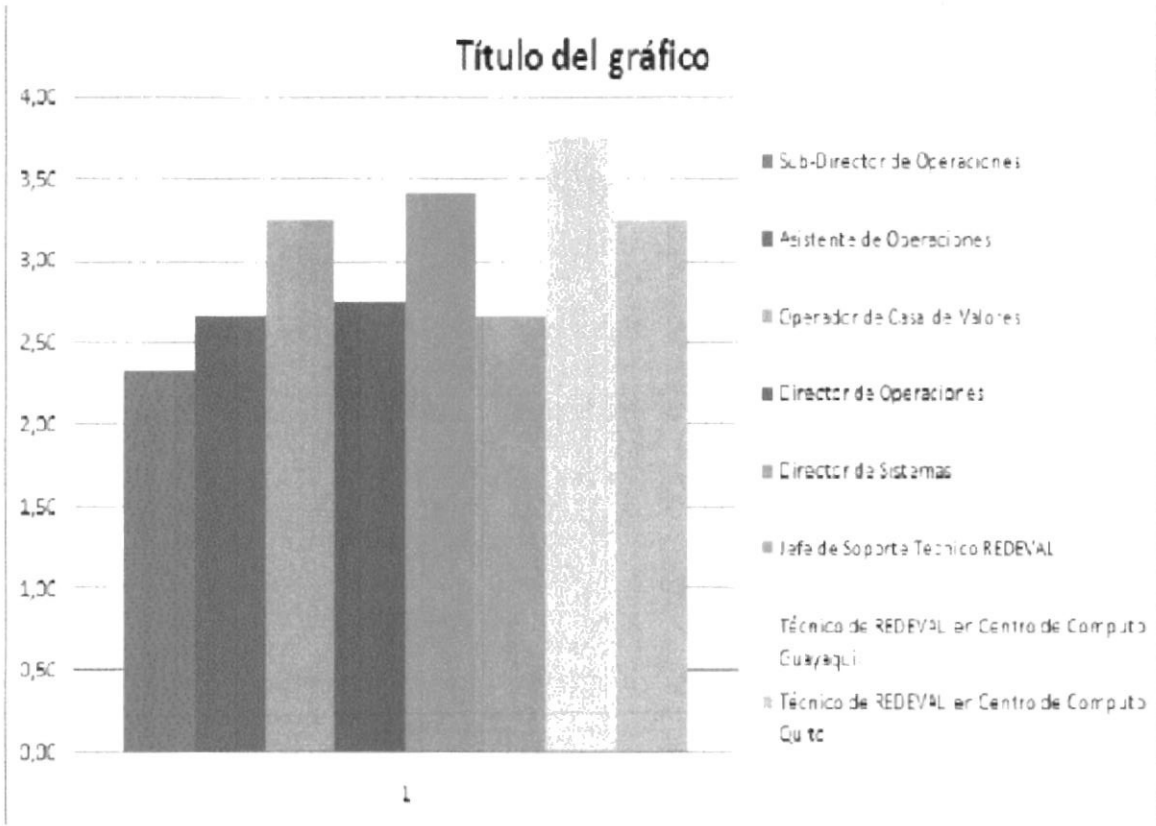
Factores de Calificacion de Riesgo de Amenaza

F	probabilidad de Ocurrencia de la amenaza [Frecuencia]
M	Impacto si se Materializa la Amenaza

Factores de Calificacion de Vulnerabilidad

P	Probabilidad que amenaza explote Vulnerabilidades
M1	Impacto material para la Amenaza a causa de la vulnerabilidad

Resumen	
Sub-Director de Operaciones	2.33
Asistente de Operaciones	2.67
Operador de Casa de Valores	3.25
Director de Operaciones	2.75
Director de Sistemas	3.42
Jefe de Soporte Técnico REDEVAL	2.67
Técnico de REDEVAL en Centro de Computo Guayaquil	3.75
Técnico de REDEVAL en Centro de Computo Quito	3.25



ANLALISIS Y EVALUACION DEL RIESGO
IDENTIFICACION DE VULNERABILIDADES

ACTIVOS		TASACIÓN				AMENAZAS				VULNERABILIDADES				RIESGO DE LA AMENAZA DE CADA A LA				CONTROLES
No.	Activo de Información	C	I	D	Tasación (Promedio)	Descripción	F	M	Calificación de Riesgo de Amenaza	Descripción	P	M'	Calificación de Riesgo de la Vulnerabilidad	Probabilidad	Impacto	Total de la Amenaza por c/vulnerabilidad	Total de todas amenazas	Selección de Controles
						Falta de soporte	4	4	4	Se requiere personal	4	4	4	4	4	4,00		[illegible] Control de los activos
	CTREE+					Obsolecencia y [illegible]	4	4	4	personal de Tecnología de la organización vive	4	4	4	4	4	4,00		
1		5	5	5	5	Complejidad de	4	2	[illegible]	únicamente por la	4	3	3,5	4	2,5	3,25	3,75	
	Respaldos de última versión de la aplicación					Daño físico de las cintas	4	4	4	No existe un plan de	[illegible]	1	1	2,5	2,5	2,50		10.5.1 Copias de seguridad de la información
						Descontinuidad	4	3	3,5	verificación de los	[illegible]	1	1	2,5	2	2,25		
2		1	5	4	4				0	respaldos porque no lo [illegible]	[illegible]	1	1	1	1	1,00	1,92	

Factores de Calificación de Activo
I Integridad
C Confidencialidad
D Disponibilidad

Factores de Calificación de Riesgo de Amenaza

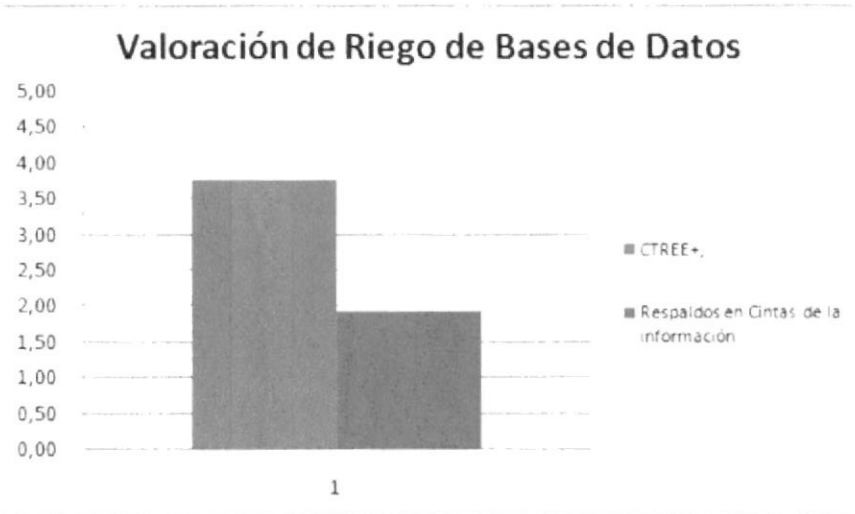
F	probabilidad de Ocurrencia de la amenaza (Frecuencia)
M	Impacto si se Materializa la Amenaza

Factores de Calificación de Vulnerabilidad

P	Probabilidad que amenaza explote Vulnerabilidades
M'	Impacto materialización Amenaza a causa de la vulnerabilidad

TasActivo | Contestado | INFRAESTRUCTURA | APLICACIONES | PERSONAS | **BASE DE DATOS** | DATOS

Resumen	
CTREE+.	3.75
Respaldos en Cintas de la informac	1.92



ANLALISIS Y EVALUACION DEL RIESGO
IDENTIFICACION DE VULNERABILIDADES

ACTIVOS		TASACIÓN				AMENAZAS				VULNERABILIDADES				RIESGO DE LA AMENAZA DE CARA A LA				CONTROLES
No.	Activo de Información	C	I	D	Tasación (Promedio)	Descripción	F	M	Calificación de Riesgo de Amenaza	Descripción	P	M1	Calificacion de Riesgo de la Vulnerabili	Probabilidad	Impacto	Total de la Amen por el/vulnerabilidad)	Total de toda la amenaza	Selección de Controles
1	INFORMACIÓN DE POSTURAS DE OFERTAS	5	5	5	5	Destrucción	2	4	3	Se los maneja como archivos planos no encriptados	2	4	3	2	4	3,00		7.2.1 Directrices y
						Corrupcion de integridad	3	4	3,5		3	4	3,5	3	4	3,50		7.2.2 Etiquetado y
						Desactualizacion	3	4	3,5		3	4	3,5	3	4	3,50	3,33	
	INFORMACIÓN DE RUEDAS	5	5	5	5	Destrucción	2	4	3	Se los maneja como archivos planos no encriptados	2	4	3	2	4	3,00		7.2.1 Directrices y clasificacion
						Corrupcion de integridad	3	4	3,5		3	4	3,5	3	4	3,50		7.2.2 Etiquetado y
						Desactualizacion	3	4	3,5		3	4	3,5	3	4	3,50	3,33	
	INFORMACION DE POSTURAS DE DEMANDAS	5	5	5	5	Destrucción	2	4	3	Se los maneja como archivos planos no encriptados	2	4	3	2	4	3,00		
						Corrupcion de integridad	3	4	3,5		3	4	3,5	3	4	3,50		
						Desactualizacion	3	4	3,5		3	4	3,5	3	4	3,50	3,33	
	PRECIOS Y CANTIDADES DE LAS OP	3	5	5	4	Destrucción	2	4	3	Se los maneja como archivos planos no encriptados	2	4	3	2	4	3,00		
						Corrupcion de integridad	2	4	3		2	4	3	2	4	3,00		
						Desactualizacion	2	4	3		2	4	3	2	4	3,00	3,00	
	INFORMACIÓN DE LOS TITULOS	3	4	5	4	Destrucción	3	4	3,5	Los respaldos de los datos no se comentan a pruebas o simulaciones de recuperación	3	4	3,5	3	4	3,50		
						Corrupcion de integridad	3	4	3,5		3	4	3,5	3	4	3,50		
						Desactualizacion	3	4	3,5		3	4	3,5	3	4	3,50	3,50	
	INFORMACION DE IDENTIDAD DE OFERTANTES Y DEMANDANTES	5	5	5	5	Utilización indebida	3	4	3,5	No se han implementado mecanismos de validación de identidad s más de la	4	4	4	3,5	4	3,75		11.2.3 Gestion de contraseñas de usuario
						Corrupcion de integridad	3	4	3,5	No se constato un procedimiento para creación y administración de claves	4	4	4	3,5	4	3,75		11.2.3 Gestion de contraseñas de usuario
						Desactualizacion	3	4	3,5		4	4	4	3,5	4	3,75	3,75	

Factores de Calificacion de Activo
I Integridad
C Confidencialidad
D Disponibilidad

Factores de Calificacion de Riesgo de Amenaza

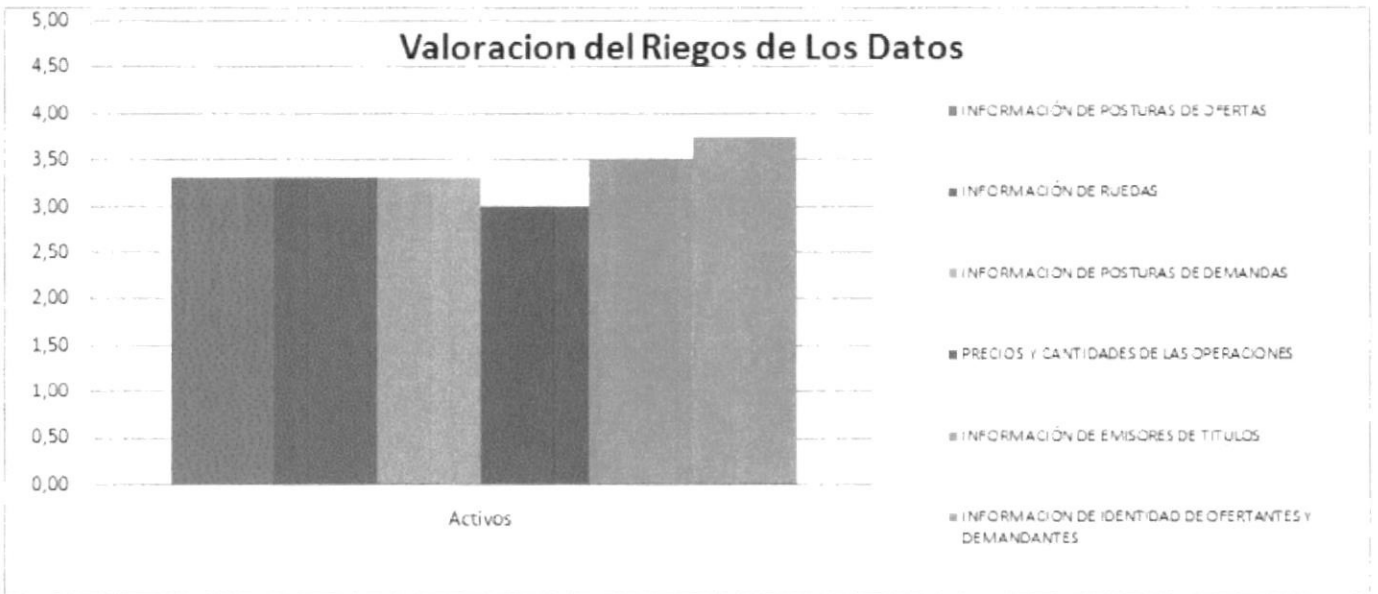
F	probabilidad de Ocurrencia de la amenaza (Frecuencia)
M	Impacto si se Materializa la Amenaza

Factores de Calificacion de Vulnerabilidad

P	Probabilidad que amenaza explote Vulnerabilidades
M1	Impacto materializarse la Amenaza : causa de la vulnerabbelidad

TasActivo | Contestado | INFRAESTRUCTURA | APLICACIONES | PERSONAS | BASE DE DATOS | DATOS

Activos	Valoración
INFORMACION DE POSTURAS DE OFERTAS	3,33
INFORMACIÓN DE RUEDAS	3,33
INFORMACION DE POSTURAS DE DEMANDAS	3,33
PRECIOS Y CANTIDADES DE LAS OPERACIONES	3,00
INFORMACIÓN DE EMISORES DE TITULOS	3,50
INFORMACION DE IDENTIDAD DE OFERTANTES Y DEMAN	3,75



ACTIVOS						AMENAZAS				VULNERABILIDADES				RIESGO DE LA AMENAZA DE CARA A LA				CONTROLES
N.c.	Activo de información	C	I	D	Tasación (Promedio)	Descripción	F	M	Calificación de Riesgo de Amenaza	Descripción	P	M1	Calificación de Riesgo de la Vulnerabilidad	Probabilidad	Impacto	Total de la Amenaza por Vulnerabilidad	Total de esta la amenaza	Selección de Controles
1	REPORTES DE LIQUIDACIONES	3	5	1	4	Acuteracion	2	4	3	No tiene ningun sistema de validacion como un codigo de Barra solo un numero	3	4	3,5	2,5	4	3,25		10.8.1 Políticas y procedimientos de intercambio de
						Perdida	4	4	4		4	4	4	4	4	4		10.8.2 Acuerdo de intercambio
						Errores de impresión	1	3	3,5	Requiere de un Proceso de ingreso ó verificTORY	4	3	3,5	4	3	3,5	3,58	15.1.3 Protección de los documentos de la
	AUTORIZACIONES PARA CREAR USUARIOS DE OPERADORES DE CASAS DE VALORES	3	3	4	3	Falsificacion	2	3	2,5	Son documentos manejados fisicamente para no ser protegidos	2	3	2,5	2	3	2,5		
						Acuteración	2	3	2,5		2	3	2,5	2	3	2,5		
						desactualizacion	3	3	3		3	3	3	3	3	3	2,67	
	TITULOS VALORES QUE SE NEGOCIAN	2	4	4	3	Robo o perdida	3	5	4	Alga de la de incertidumbre	3	5	4	3	5	4		
						Falsificación	2	5	3,5	Muchos Titulos Valores son al portador	3	5	4	2,5	5	3,75		
						Deterro	4	3	3,5	No existe una política que obligue a utilizar un papel isotermico tipo Moneda	4	4	4	4	3,5	3,75	3,83	
	MANUALES DE USUARIO DEL SEB PARA OPERADORES DE CASAS DE VALORES	2	3	3	3	Desactualización	1	3	3,5	Falta de control de actualizaciones	4	3	3,5	4	3	3,5		
						Obsolescencia	1	3	3,5		4	3	3,5	4	3	3,5		
						Complejidad de uso	3	3	3		3	3	3	3	3	3	3,33	

Factores de Calificación de Activo

I Integridad

C Confidencialidad

D Disponibilidad

Factores de Calificación de Riesgos Amenaza

F probabilidad de Ocurrencia de la amenaza (frecuencia)

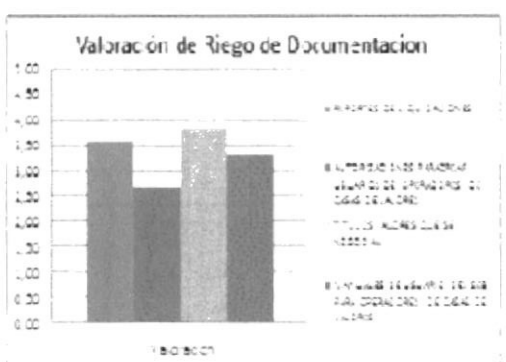
M Impacto si se Materializa la Amenaza

Factores de Calificación de Vulnerabilidad

P Probabilidad que amenaza explote Vulnerabilidad

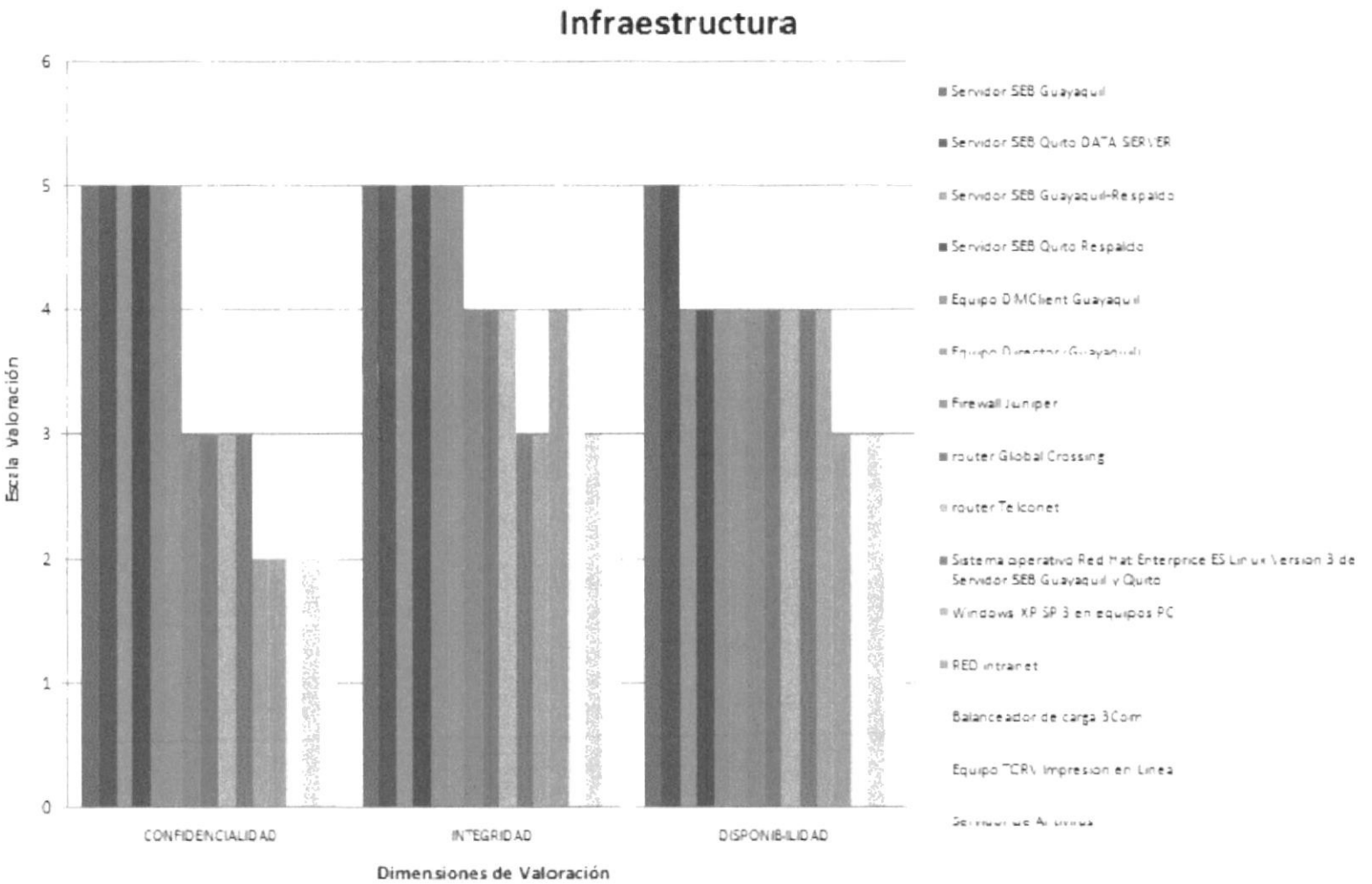
M1 Impacto materializarse la Amenaza a causa de la vulnerabilidad

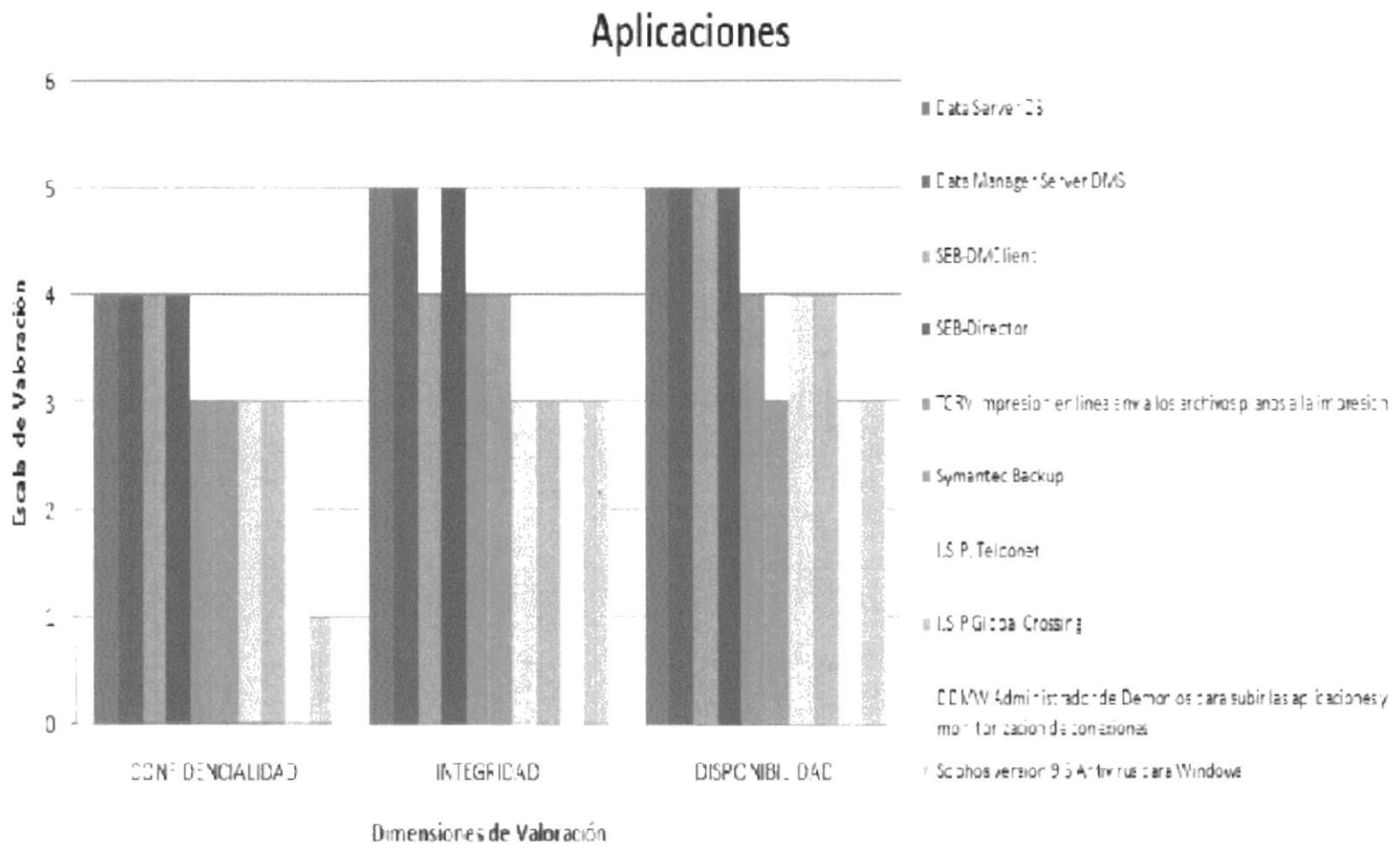
	Valoración
REPORTES DE LIQUIDACIONES	3,58
AUTORIZACIONES PARA CREAR USUARIOS DE OPERADORES DE CASAS DE VALORES	2,67
TITULOS VALORES QUE SE NEGOCIAN	3,83
MANUALES DE USUARIO DEL SEB PARA OPERADORES DE CASAS DE VALORES	3,33

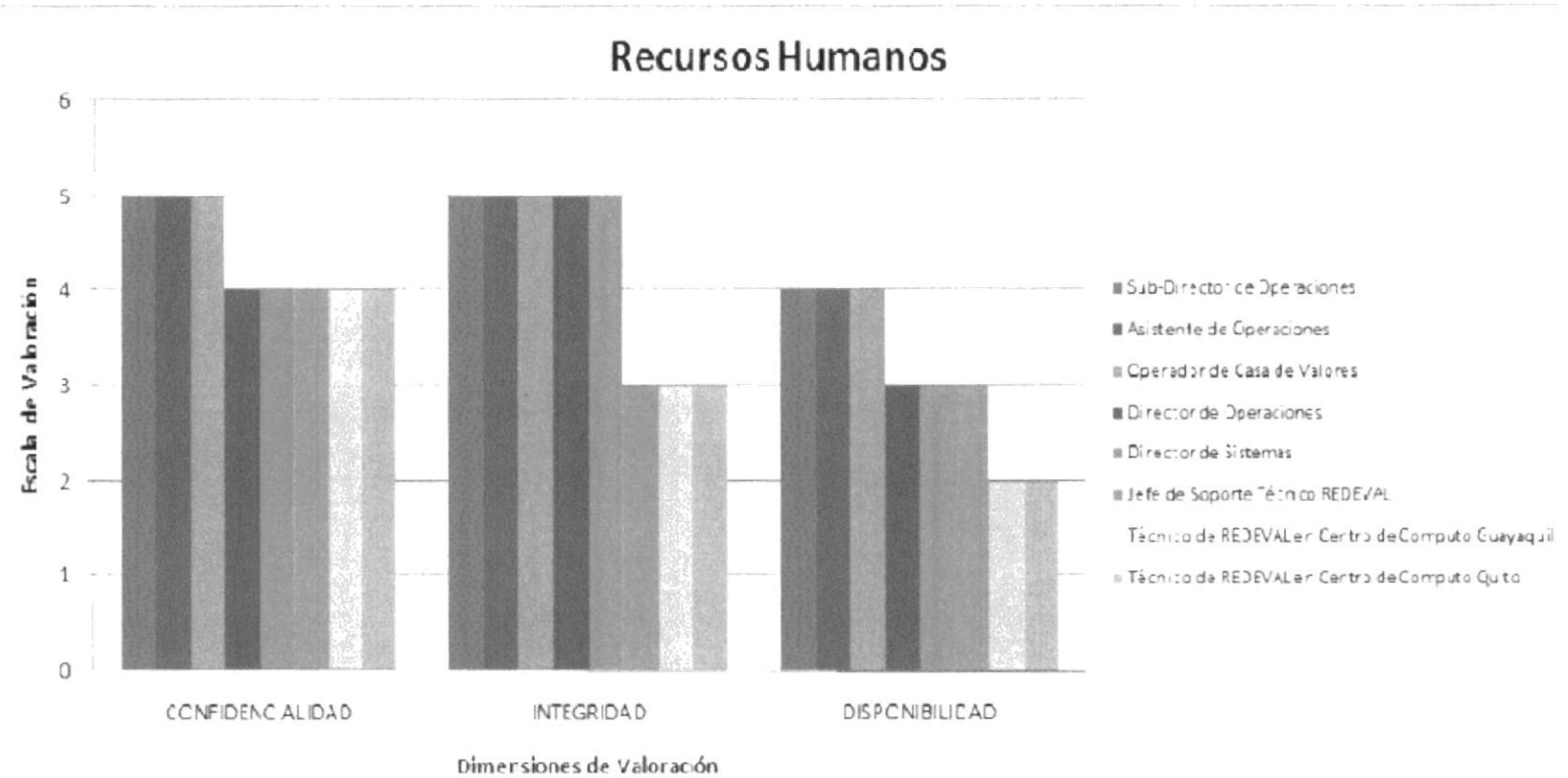


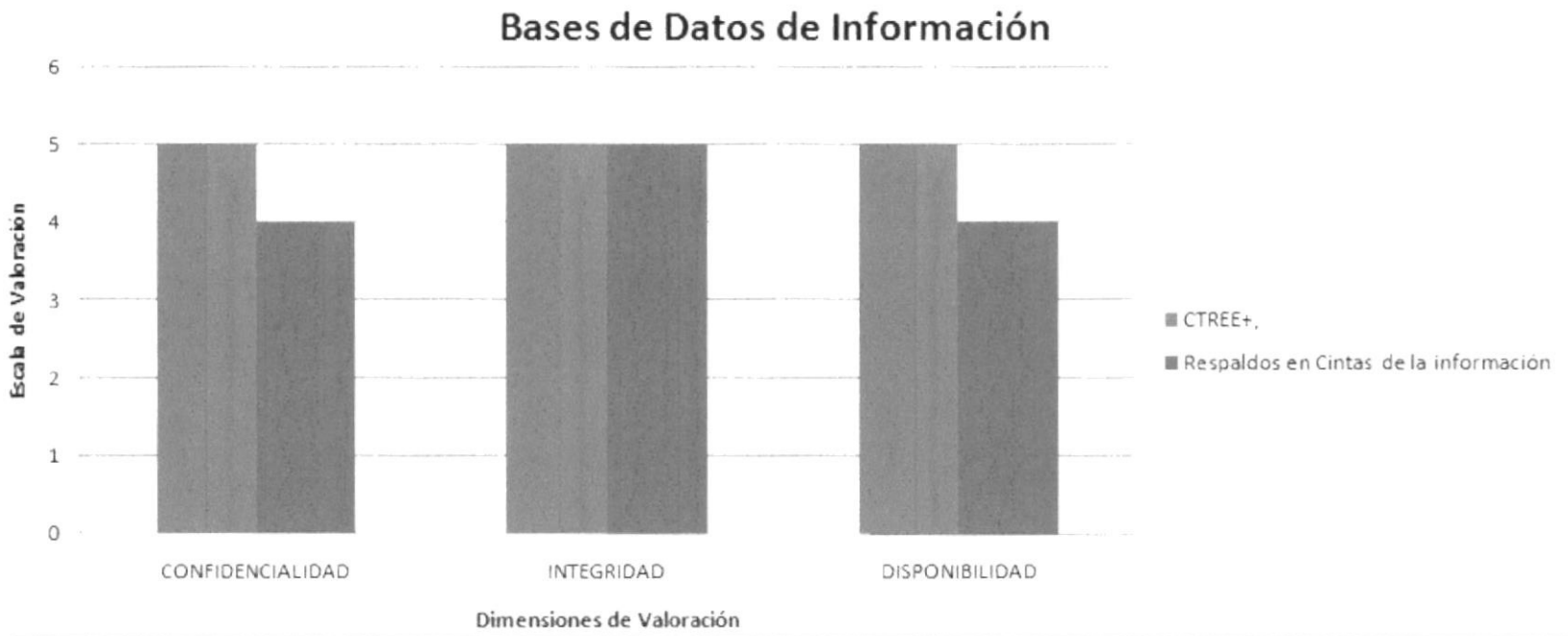
APLICACIONES PERSONAS BASE DE DATOS DATOS **DOCUMENTACION** Graficos de Tasacion

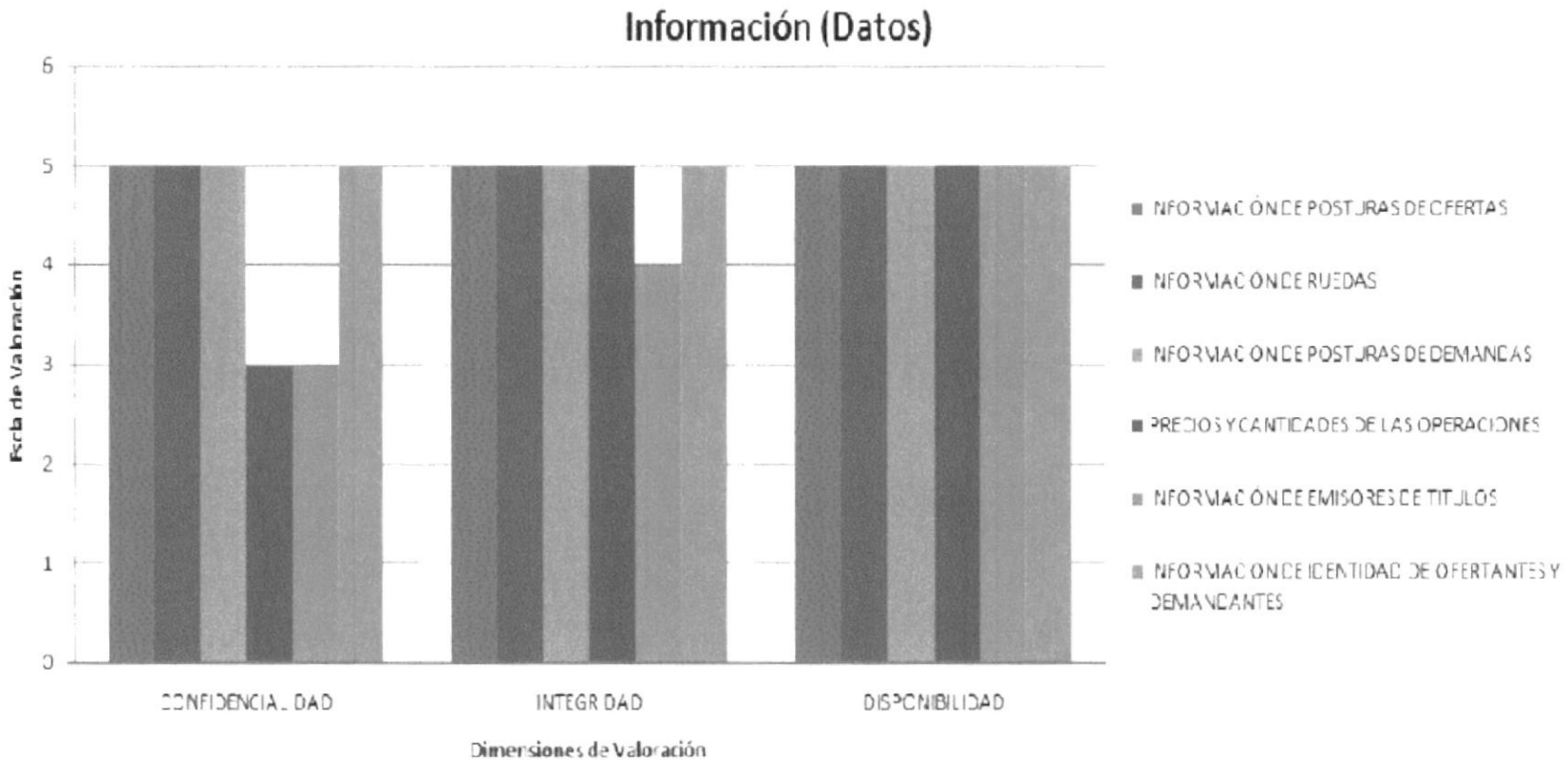
TASACION DE CRITICIDAD DE LOS ACTIVOS

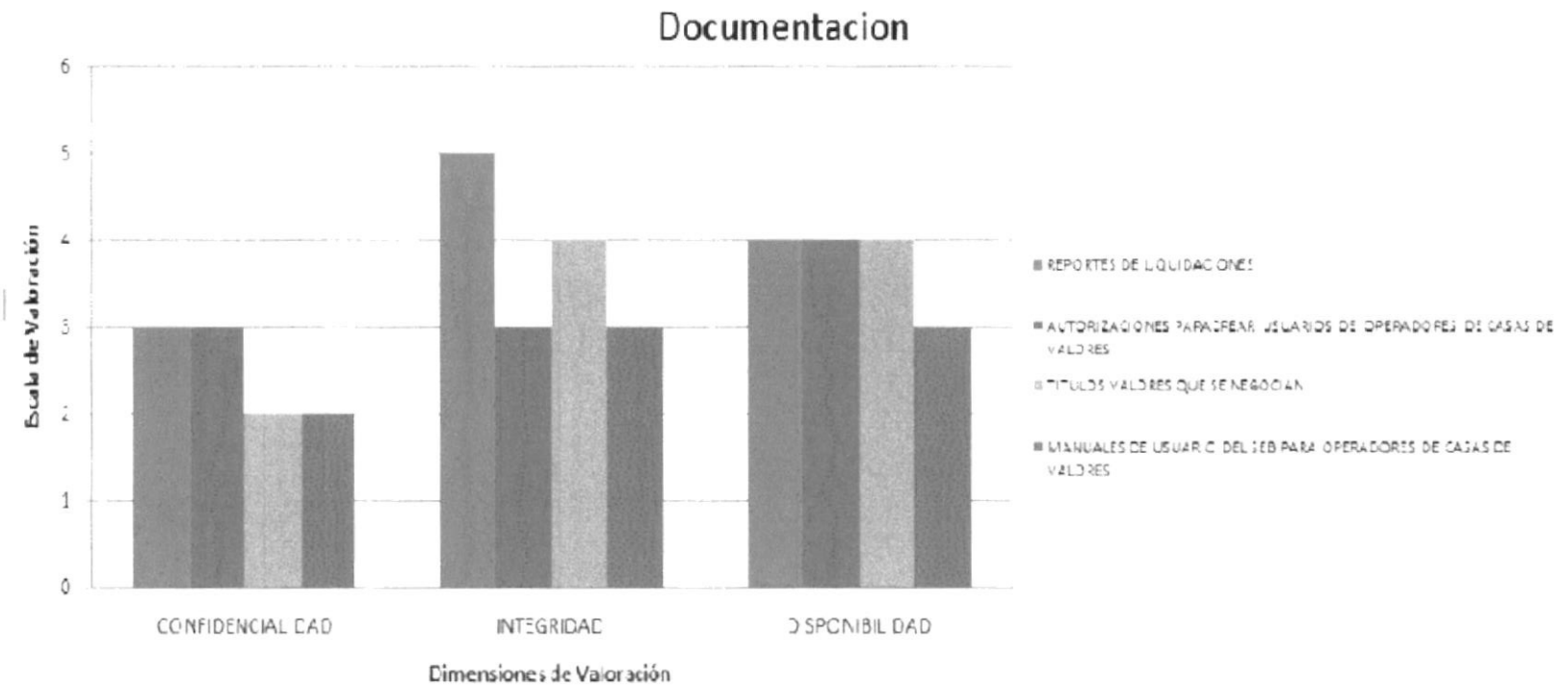

Infraestructura
Escala Valoración
6
5
4
3
2
1
0
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
Servidor SEB Guayaquil
Servidor SEB Quito DATA SERVER
Servidor SEB Guayaquil-Respaldo
Servidor SEB Quito Respaldo
Equipo DMClient Guayaquil
Firewall Juniper
router Global Crossing
router Telconet
Sistema operativo Red Hat Enterprice ES Linux Version 3 de Servidor SEB Guayaquil y Quito
Windows XP SP 3 en equipos PC
RED intranet
Balanceador de carga 3Com
Equipo TCRV Impresion en Linea


Aplicaciones
Escala de Valoración
6
5
4
3
2
1
0
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
Data Server DB
Data Manager Server DMS
SEB-DMClient
SEB-Director
TCP/Impresion en linea envia los archivos planos a la impresion
Symantec Backup
I.S.P. Telconet
I.S.P Global Crossing
DDMW Administrador de Demonios para subir las aplicaciones y monitorizacion de conexiones
Sophos version 9.5 Antivirus para Windows

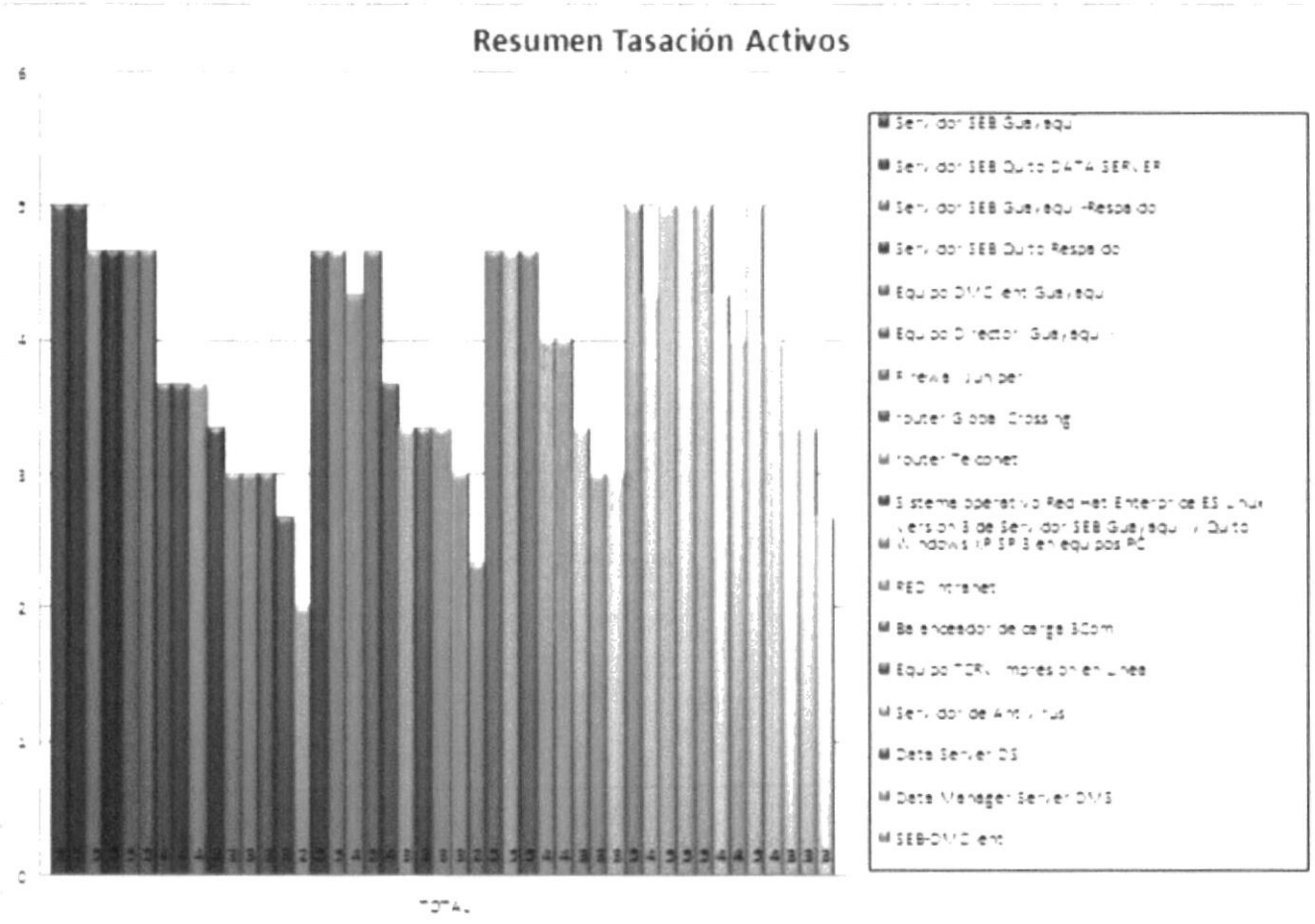

Recursos Humanos
Escala de Valoración
6
5
4
3
2
1
0
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
Sub-Director de Operaciones
Asistente de Operaciones
Operador de Casa de Valores
Director de Operaciones
Director de Sistemas
Jefe de Soporte Técnico REDEVAL
Técnico de REDEVAL en Centro de Computo Guayaquil
Técnico de REDEVAL en Centro de Computo Quito


Bases de Datos de Información
6
5
4
3
2
1
0
Escala de Valoracion
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
CTREE+,
Respaldos en Cintas de la informacion

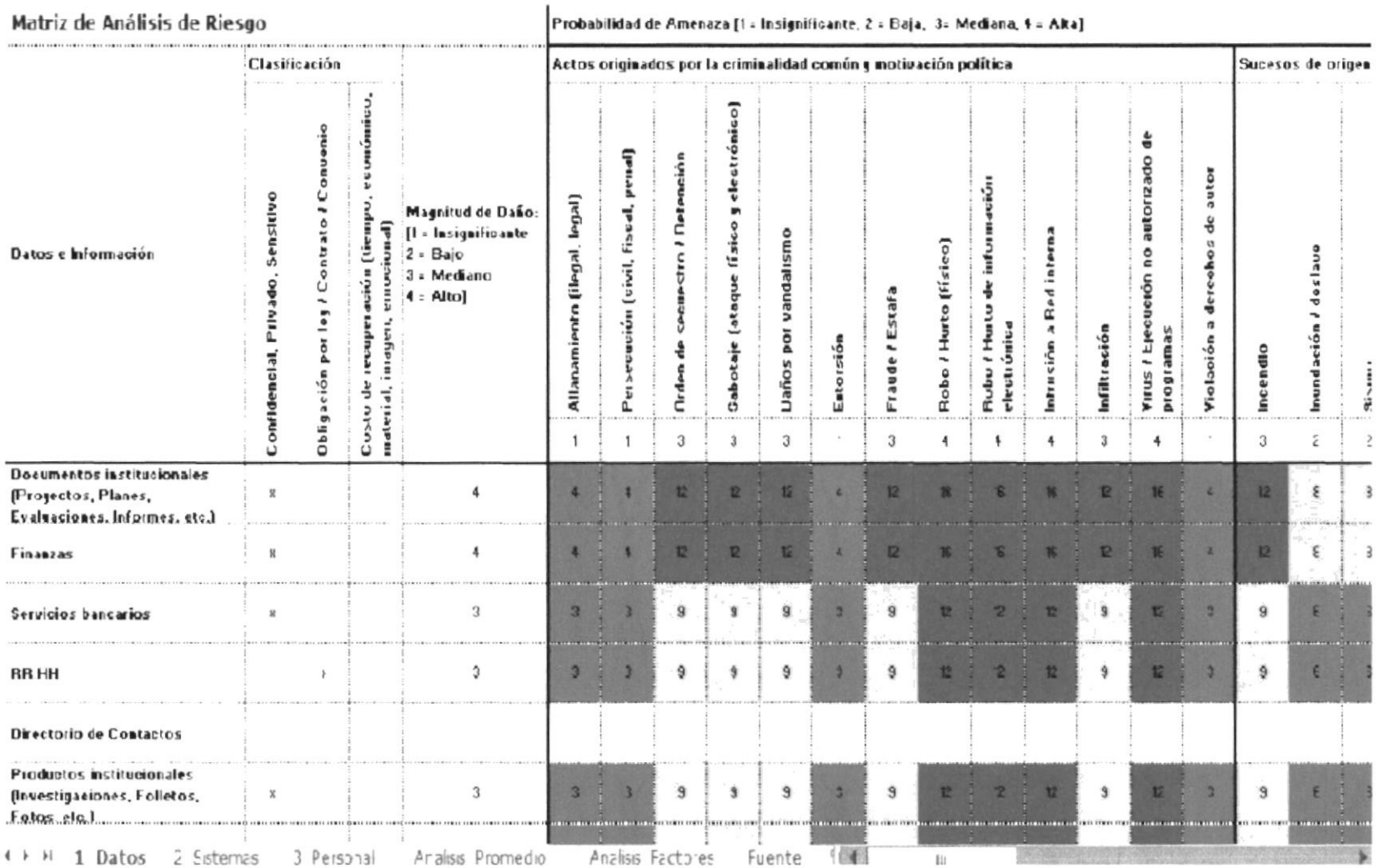

Información (Datos)
6
5
4
3
2
1
0
Escala de Valoración
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
INFORMACIÓN DE POSTURAS DE OFERTAS
INFORMACIÓN DE RUEDAS
INFORMACIÓN DE POSTURAS DE DEMANDAS
PRECIOS Y CANTIDADES DE LAS OPERACIONES
INFORMACIÓN DE EMISORES DE TITULOS
INFORMACIÓN DE IDENTIDAD DE OFERTANTES Y DEMANDANTES


Documentacion
6
5
4
3
2
1
0
Escala de Valoración
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
REPORTES DE LIQUIDACIONES
AUTORIZACIONES PARA CREAR USUARIOS DE OPERADORES DE CASAS DE VALORES
TITULOS VALORES QUE SE NEGOCIAN
MANUALES DE USUARIO DEL SEB PARA OPERADORES DE CASAS DE VALORES

RESUMEN DE TASACIÓN DE ACTIVOS

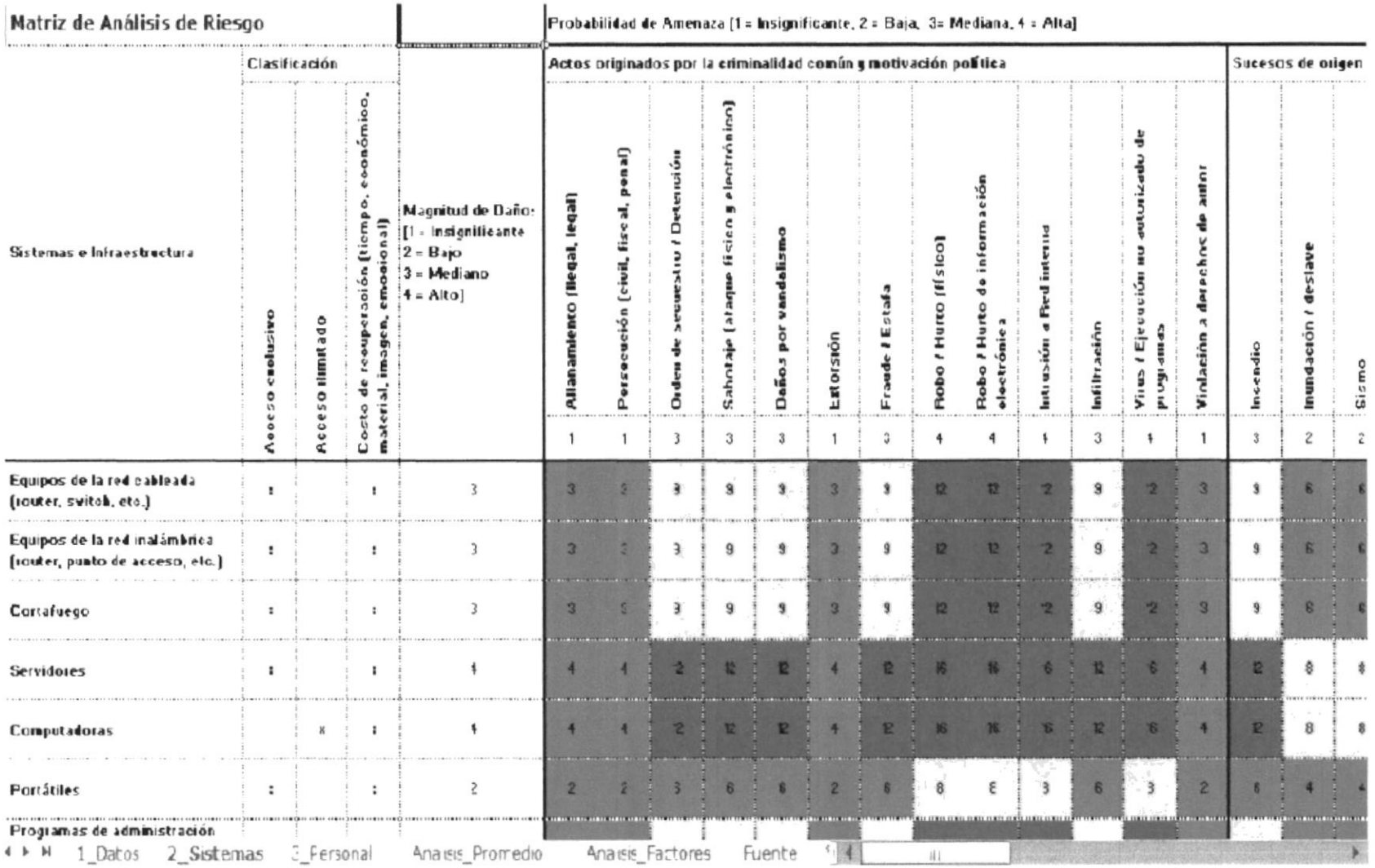

Resumen Tasación Activos
6
5
4
3
2
1
0
TOTAL
Servidor SEB Guayaquil
Servidor SEB Quito DATA SERVER
Servidor SEB Guayaquil Respaldo
Servidor SEB Quito Respaldo
Equipo DVD client Guayaquil
Equipo Director Guayaquil
Firewall Juniper
Router Global Crossing
Router Telconet
Sistema operativo Red Hat Enterprise ES Linux version 3 de Servidor SEB Guayaquil y Quito
Windows XP SP3 en equipos PC
RED Intranet
Balanceador de carga 3Com
Equipo TCR Impresoras en Línea
Servidor de Antivirus
Data Server DS
Data Manager Server DVS
SEB-DVD Client

MATRIZ ANÁLISIS DE RIESGO



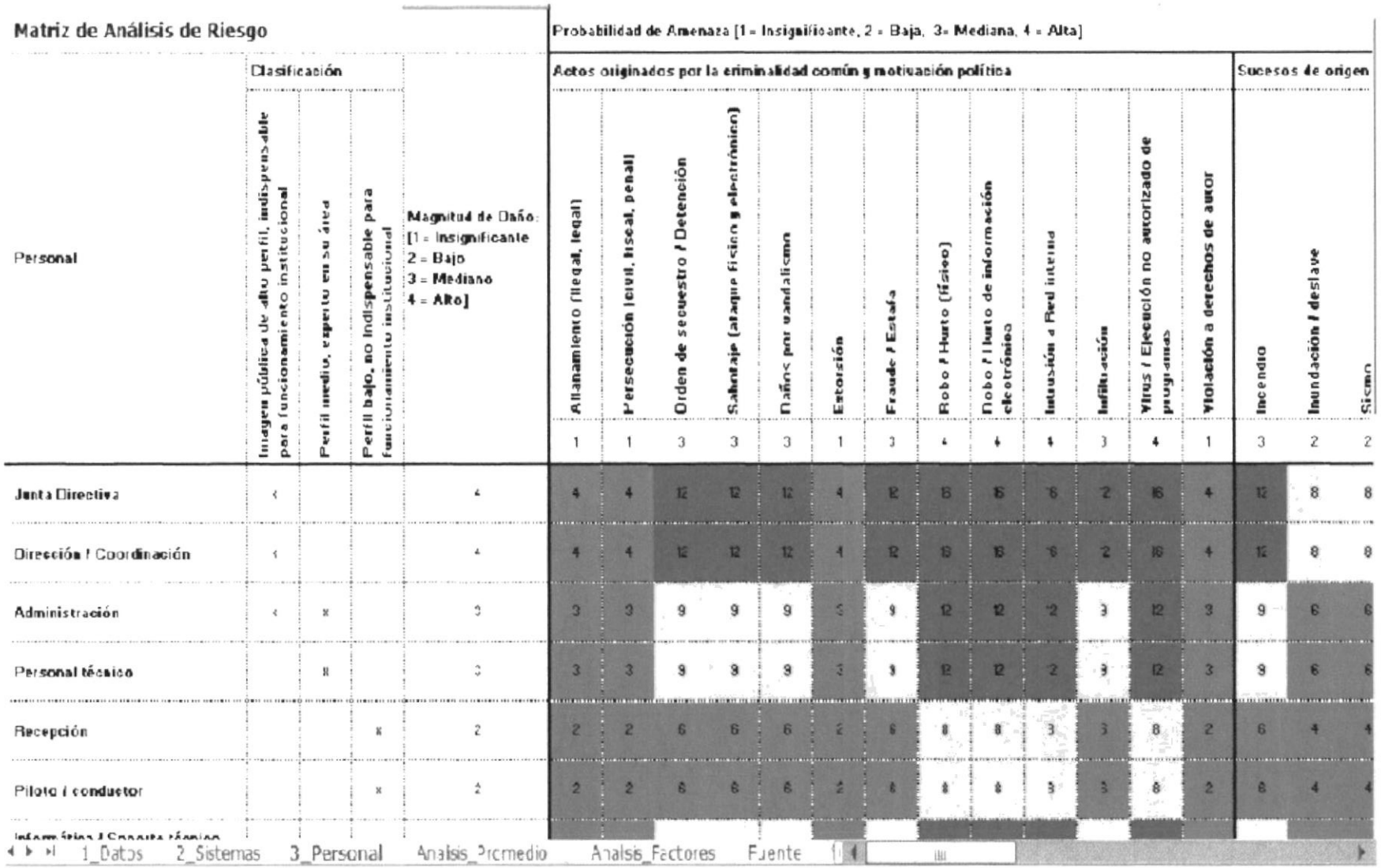
Matriz de Análisis de Riesgo	Clasificación				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]														
					Actos originados por la criminalidad común y motivación política												Sucesos de origen		
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Ordenes de comparecencia / Retención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / daño	Sismo
					1	1	3	3	3	1	3	4	4	4	3	4	1	3	2	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x			4	4	4	12	12	12	4	12	16	16	16	12	16	4	12	8	8
Finanzas	x			4	4	4	12	12	12	4	12	16	16	16	12	16	4	12	8	8
Servicios bancarios	x			3	3	3	9	9	9	3	9	12	12	12	9	12	3	9	6	6
RR HH		x		3	3	3	9	9	9	3	9	12	12	12	9	12	3	9	6	6
Directorio de Contactos																				
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)	x			3	3	3	9	9	9	3	9	12	12	12	9	12	3	9	6	6

1 Datos 2 Sistemas 3 Personal Analisis Promedio Analisis Factores Fuente



Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]														
	Clasificación				Actos originados por la criminalidad común y motivación política													Sucesos de origen	
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Ordenes de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizada de programas	Violación a derechos de autor	Incendio	Inundación / desfase	Sismo
					1	1	3	3	3	1	3	4	4	1	3	1	1	3	2	2
Equipos de la red cableada (router, switch, etc.)	x		x	3	3	3	9	9	9	3	9	12	12	2	9	2	3	9	6	6
Equipos de la red inalámbrica (router, punto de acceso, etc.)	x		x	3	3	3	9	9	9	3	9	12	12	2	9	2	3	9	6	6
Cortafuego	x		x	3	3	3	9	9	9	3	9	12	12	2	9	2	3	9	6	6
Servidores	x		x	4	4	4	12	12	12	4	12	16	16	6	12	6	4	12	8	8
Computadoras		x	x	4	4	4	12	12	12	4	12	16	16	16	12	16	4	12	8	8
Portátiles	x		x	2	2	2	3	6	6	2	6	8	8	3	6	3	2	6	4	4
Programas de administración																				

1_Datos 2_Sistemas 3_Personal Analisis_Promedio Analisis_Factores Fuente



Matriz de Análisis de Riesgo

Personal	Clasificación: Imagen pública de alto perfil, indispensable para funcionamiento institucional	Clasificación: Perfil medio, experto en su área	Clasificación: Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3 = Mediana, 4 = Alta] — Actos originados por la criminalidad común y motivación política: Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Estorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónico	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Sucesos de origen: Incendio	Inundación / deslave	Sismo
					1	1	3	3	3	1	3	4	4	4	3	4	1	3	2	2
Junta Directiva	x			4	4	4	12	12	12	4	12	16	16	16	12	16	4	12	8	8
Dirección / Coordinación	x			4	4	4	12	12	12	4	12	16	16	16	12	16	4	12	8	8
Administración	x	x		3	3	3	9	9	9	3	9	12	12	12	9	12	3	9	6	6
Personal técnico		x		3	3	3	9	9	9	3	9	12	12	12	9	12	3	9	6	6
Recepción			x	2	2	2	6	6	6	2	6	8	8	8	6	8	2	6	4	4
Piloto / conductor			x	2	2	2	6	6	6	2	6	8	8	8	6	8	2	6	4	4
Informáticos / Soporte técnico																				

1_Datos 2_Sistemas 3_Personal Analisis_Promedio Analisis_Factores Fuente

Análisis de Riesgo promedio

		Probabilidad de Amenaza		
		Criminalidad y Político	Sucesos de origen físico	Negligencia y Institucional
Magnitud de Daño	Datos e Información	5,1	5,3	5,1
	Sistemas e Infraestructura	5,9	6,1	5,8
	Personal	6,7	6,9	6,6

Análisis de Factores de Riesgo

VALORACIÓN Y MAPEO DE RIESGOS

VALORACIÓN Y MAPEO DE RIESGOS

Mapa de Riesgo

NOTA: [illegible]

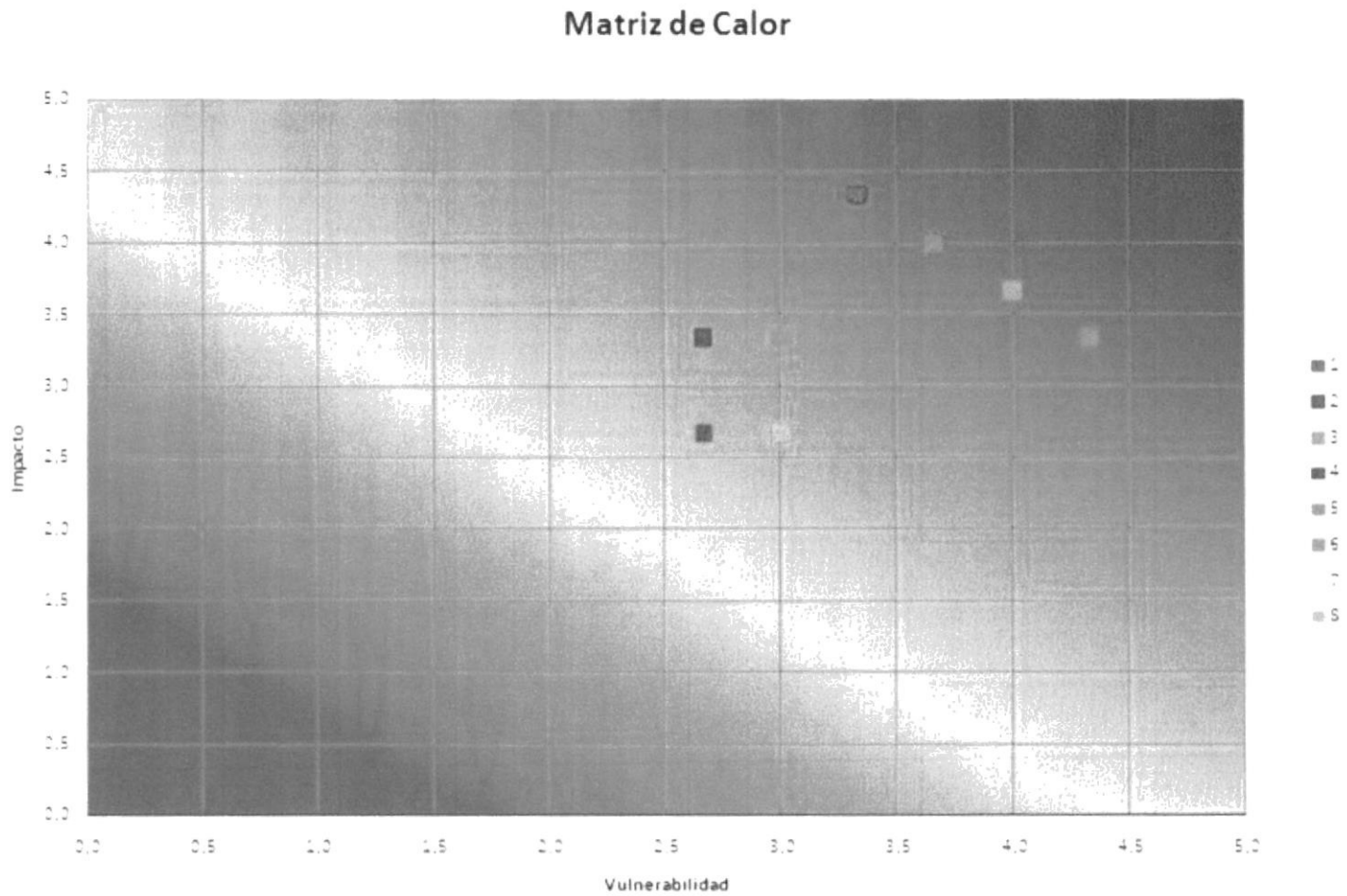
Vulnerabilidad: [illegible] Está en el 1 al 5

Impacto: [illegible]

	PROCESO	LIDER PROCESO	RIESGO IDENTIFICADO	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación de Director de Sistemas y Operaciones	Calificación Sub-Director de O&M	Calificación Director General	Controles Seguridad para mitigar riesgos	Costo de aplicar los controles $ (Alto, Medio, Bajo)	Tratamiento al Riesgo
1	CONTROL DE ACCESO	SISTEMAS	En la política de creación de usuarios no se incluye el formato de la clave y se constata que los usuarios pueden utilizar los caracteres que les parece	Alto	3,0	4,0	VOTO IMPACTO	4,0	4,0	5,0	Revisar y Documentar una Especificación o Política que incluya el formato de las claves para mejorar el control	BAJO	MITIGAR
							VOTO VULNERABILIDAD	2,0	3,0	5,0			
2		DIRECCION DE SISTEMAS Y OPERACIONES	La entrega de cuentas de usuario y claves no está definida en un manual documentado y se hace llegar a los usuarios por email	Medio	2,7	2,7	VOTO IMPACTO	2,0	2,0	4,0	Implementar un procedimiento para entrega de claves seguras mediante herramientas que provean las mismas	MEDIO	MITIGAR
							VOTO VULNERABILIDAD	2,0	2,0	4,0			
3	REGISTRO DE POSTURAS Y CIERRE DE NEGOCIACION	CORREDORES DE CASA DE VALORES	Por la presura de cerrar una negociación comenten errores al ingresar datos y/o son nuevos no se percatan de los errores hasta que la operación pasa a otro estado	Medio	3,0	3,0	VOTO IMPACTO	2,0	4,0	4,0	Implementar alrededor de errores y alertas para que se hagan verificaciones antes de cerrar las operaciones	MEDIO	MITIGAR
							VOTO VULNERABILIDAD	2,0	3,0	4,0			
4		DIRECCION DE SISTEMAS Y OPERACIONES	El personal de TI no conoce si existen políticas para controlar el acceso	Medio	2,7	3,0	VOTO IMPACTO	2,0	5,0	3,0	Implementar un procesos de difusión de las políticas y verificar que todos los miembros de TI conozcan y entiendan las políticas	BAJO	MITIGAR
							VOTO VULNERABILIDAD	2,0	3,0	3,0			

5	DESARROLLO	DIRECCION DE SISTEMAS Y OPERACIONES	En el control de cambio de versiones, no se lleva un control sistemático del levantamiento de requerimientos, aunque existan los formatos y procedimientos para el efecto, muchas veces se los pasa por alto	Alto	3,7	4,0	PORCENTAJE	4 C	4,0	4 C	Implementar un procedimiento documentado para el control de cambios que incluya un plan general de pruebas, pasos para levantar un laboratorio de pruebas, verificación de cumplimientos de requerimientos, plan de retroceso	BAJO	MITIGAR
							PORCENTAJE VULNERABILIDAD	3 C	4,0	4 C			
6		DIRECCION DE SISTEMAS Y OPERACIONES	La persona que cumple las funciones de Jefe de Soporte de RECEVAL, es la única persona que se encarga de hacer las pruebas de los cambios y no hay entrenamiento para los otros dos técnicos	Alto	4,3	3,3	PORCENTAJE	2 C	4,0	4 C	Implementar un plan de entrenamiento constante del personal de IT para que conozcan los procedimientos y documentación que esta relacionada al SEB	BAJO	MITIGAR
							PORCENTAJE VULNERABILIDAD	4 C	4,0	5 C			
7		SISTEMAS	No se constata un documento que explique cual metodología conocida se utiliza para el desarrollo de aplicaciones ni para la verificación de software adquirido	Medio	3,0	2,7	PORCENTAJE	2 C	2,0	4 C	Realizar pruebas periódicas de simulaciones de caídas de conexión para verificar el soporte 24x7 de IP Proveedor y validar el tiempo de respuesta del balanceador de cargas cuando un enlace se cae	MEDIO	MITIGAR
							PORCENTAJE VULNERABILIDAD	2 C	2,0	4 C			
8	CIERRE DE LA OPERACIÓN	SISTEMAS	La metodología utilizada por el proveedor tecnológico en el desarrollo no garantiza que se esta cumpliendo con los requisitos de seguridad de información manejada en el SEB	Alto	4,0	3,7	PORCENTAJE	3 C	4,0	4 C	Considerar la norma ISO 15408 como base para generar un procedimiento de evaluación del software adquirido o desarrollado	BAJO	MITIGAR
							PORCENTAJE VULNERABILIDAD	4 C	4,0	4 C			

JULIA MACIAS TULCAN
MAYRA BENAVIDES RODRIGUEZ


Matriz de Calor
Impacto
Vulnerabilidad
0.0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0
1
2
3
4
5
6
7
8

10.2. Controles

10.2.1. Marco Teórico

Los controles se clasifican 3 partes

Automáticos.- Lo realiza de principio a fin un sistema de información

Semiautomáticos.- es ejecutado de manera parcial por una persona pero con la colaboración de un SI

Manual.- Lo ejerce en su totalidad una persona sin la colaboración de un sistema de información

Los controles pueden ser:

Preventivos.- su objetivo es anticiparse a los eventos no deseados actuando sobre las causas del riesgo así como evitando la generación de errores o eventos fraudulentos

Detectivos.- Identifica todos aquellos eventos en el momento que ocurren así como advierte sobre la presencia de riesgos

Correctivos.- Se orienta a la implementación de las acciones correctivas una vez se ha identificado un evento no deseado. su implementación se realiza cuando los controles preventivos y detectivos no se han funcionado lo cual representa que su implementación sea más costosa pues actúan cuando ya se han materializado eventos de pérdidas para la organización.

<u>Factores a considerar al seleccionar los controles</u>

- Análisis Costo-beneficio
- Legislación y regulaciones
- Impacto Operacional
- Seguridad y confiabilidad
- Política Organizacional

- Efectividad

10.2.2 Propuesta de Implementación de controles

Controles Sugeridos para mitigar riesgos	Costo de aplicar los controles $ (Alto, Medio, Bajo)	Tratamiento al Riesgo
Revisar y Documentar una Especificación o Política que incluya el formato de las claves para mejorar el control	BAJO	MITIGAR
Implementar un procedimiento para entrega de claves seguras mediante herramientas que protejan las mismas	MEDIO	MITIGAR
Implementar el registro de errores y alertas para que se hagan verificaciones antes de cerrar las operaciones	MEDIO	MITIGAR
Implementar un procesos de difusión de las políticas y verificar que todos los miembros de TI conocen y entienden las políticas	BAJO	MITIGAR
Implementar un procedimiento documentado para el control de cambios que incluya un plan general de pruebas, pasos para levantar un laboratorio de pruebas, verificación de cumplimientos de requerimientos, cierre de etapa	BAJO	MITIGAR
Implementar un plan de entrenamiento constante del personal de TI para que conozcan los procedimientos y documentación que está relacionada al SEB	BAJO	MITIGAR
Realizar pruebas periódicas de simulaciones de caídas de conexión para verificar el soporte 24x7 del Proveedor y validar el tiempo de respuesta del balanceador de cargas cuando un enlace se cae	MEDIO	ASUMIR DURANTE UN AÑO
Desde el lado del operador de la casa de valores se recomienda una conexión de contingencias	ALTO	MITIGAR
Considerar la norma ISO 15408 como base para generar un procedimiento de evaluación del software adquirido o desarrollado	BAJO	MITIGAR

CAPITULO 11 Conclusiones y Recomendaciones

11.1. Conclusiones

Una de las primeras actividades que realizamos en este proyecto fue dar seguimiento a las propuestas de valor que se sugirieron en un proceso de Auditoria Externa, realizada en el año 2009 por la ESPOL, con la finalidad de unificar los sistemas de negociación bursátil a nivel nacional, e implementar algunas de seguridad.

El presente trabajo nos ha permitido evidenciar la importancia que tiene para las empresas en general, y para los que operan en el Mercados de Valores en particular, la seguridad de sus recursos tecnológicos de hardware y software, equipos y programas que condensan la valiosa información, de todas sus transacciones comerciales, información que se constituye en el alma de la empresa.

Al auditar la Bolsa de Valores de Guayaquil, analizamos su sistema de negociación electrónica, sistema de vital importancia para los miembros del Sector Financiero Bursátil que requiere un nivel óptimo de seguridad para la información que diariamente procesa.

Por lo tanto, las medidas regulatorias que se sugerimos se implementen, es producto de la auditoria realizada, están direccionadas a constituir un mecanismo de seguridad, que va disuadir el impacto que los riesgos pueden generar.

Nuestro compromiso es evitar un impacto mayor de estos conflictos, por lo que sugerimos dar la mayor tranquilidad a los usuarios, al conocer que la Banca Bursátil dispone de un sistema informático en condiciones seguras.

Estas sugerencias también pretenden fomentar una cultura de seguridad de la información, en el personal que opera en la estructura organizacional de las empresas financieras, con lineamientos basados en Estándares Internacionales, para los Sistema de negociación electrónica.

Este tipo de seguridades asigna determinados aplicaciones, para el cliente que se ejecuta en el sistema operativo Windows y para el operador del servidor, que se ejecutan en Red Hat Enterprise Linux (RHEL) del sistema operativo, aplicaciones que permiten interactuar en la gestión de datos.

En esta sociedad de la información, es importante proteger el don social más preciado que es la Información y los sistemas de información, y lo relacionado a su acceso, uso, divulgación, interrupción o destrucción no autorizada.

Es necesario disponer de políticas de procedimientos y de controles de seguridad, para salvaguardar la información como los sistemas que la almacenan y administran, para ello debemos implementar varias estrategias que cubran todos los procesos, en donde la información es el activo fundamental.

11.2. Recomendaciones

- Revisar y mejorar las políticas de creación de usuarios y claves del sistema, ya que no se contempla:
  - El estándar para formatos de los códigos y formato de claves de los usuarios.
  - Caducidad o control de validación de claves
- Mejorar los procedimientos de monitorización en el dm client, y al parecer no lo tienen documentado.
- Implementar un control para el acceso por medio de internet a los equipos DMClient y Director.
- Mejorar los procedimientos para monitorizar en el DMCLIENT, y al parecer no lo tienen documentado.

BIBLIOGRAFÍA

Documentación Revisada

- Informe de Auditoria realizada por la Escuela Superior Politécnica del Litoral a los Sistemas SEB. SIBE y AT
- Metodologia de Desarrollo de la Empresa ICAP (Proveedora del SEB)
- Otros estándares ICAP del Ecuador Sistema de Mercados Financieros Datatec.
- TECHNICAL SPECIFICATIONS DatatecFinancialMarketSystem (Especificaciones Técnicas DATATEC Sistema Electrónico Bursatil).
- Políticas para la Creación de Nuevos Usuarios (Política interna)
- Configuración y Plan de Contingencia para el Sistema Electrónico Bursátil.
- MANUAL DE USUARIO del Sistema Electrónico Bursátil
- Reglamento de Rueda Continua de la Bolsa de Valores de Guayaquil
- Reglamento de Resolución conjunta de Mecanismo de Valores no inscritos en Bolsa (REVNI)
- Subasta Serializada e Interconectada para las Inversiones y Compra Venta de Activos Financieros que realicen las Entidades del Sector Público y Privado.
- Normativa para las Operaciones de Reporto Bursátil de la Bolsa de Valores de Guayaquil.
- ISSO 27002 NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002

Sitios WEB visitados

http://www.mundobvg.com/bvgsite/quienes.htm

http://www.legal.gen.ec/Presidentea-Consejo-Nacional-Valores

http://www.iso27000.es

http://www.commoncriteriaportal.org/cc/

http://seguridad-de-la-informacion.blogspot.com/2009/04/iso-15408-y-el-dni-e-pp-para-el.html

http://www.auditool.org/index.php?option=com_content&view=article&id=838:video-21-identificacion-de-riesgos-y-controles-de-los-procesos&ca

GLOSARIO

Check List.- Lista de verificación

Control.- Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio, serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.

CNV.- Consejo Nacional de Valores

Estándares.- *"Los estándares son* ***acuerdos*** *(normas)* ***documentados*** *que contienen* ***especificaciones técnicas*** *u otros criterios precisos para ser usados consistentemente como* ***reglas, guías, o definiciones de características.*** *Para asegurar que los* ***materiales productos, procesos y servicios*** *se ajusten a su propósito.*

Estándar.- Especificaciones para desarrollar que se sujetan a algo definido dentro de la organización.

FTP .- (File Transfer Protocol) Protocolo de transferencia de archivos

ICAP.-

Lenguaje DFN.- Lenguaje propio especialmente diseñado por ICAP, para la implantación de sistemas transaccionales para los mercados financieros.

Operaciones Bursátiles.-

Objetivos de control.- Una sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

Procedimiento.- conjunto de técnicas de investigación aplicables a una partida o a un grupo de hechos o circunstancias relativas

REDEVAL.- Red Electrónica del Mercado de Valores

Rueda Bursátil.- Es un sistema de negociación continua en el que las ofertas, demandas, calces y cierres de operaciones se efectúan a través de una red de computadoras.

Rueda a Viva Voz.- Es la concurrencia física de los operadores de valores, que representan a las Casas de Valores en la Bolsa para ofertar o demandar títulos de acuerdo a las condiciones del mercado.

SEB (Sistema Electrónico Bursátil)/ Bolsa Electrónica.- Sistema de negociación electrónica, el cual permite la negociación entre participantes, así como la visualización de todas las demandas y ofertas del mercado.

ANEXOS

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

"Impulsando la Sociedad del Conocimiento"

CEC-A-081-2010

Guayaquil, 08 de julio del 2010

RECIBIDO
20 JUL 2010
Secretaría General

Señor
Luis Alvarez Villamar
Vice-director de Operaciones y Sistemas de
Corporación Civil Bolsa de Valores de Guayaquil
Presente

Estimado Señor:

El Centro de Educación Continua de la ESPOL (CEC) ofrece distintos cursos y programas de post-grado atendiendo las necesidades de los profesionales y del sector empresarial de nuestro país.

Cada uno de nuestros programas busca los mejores resultados en el aprendizaje mediante la aplicación de los conocimientos adquiridos en proyectos que son desarrollados en empresas que deseen brindar su aporte en la formación de nuestros profesionales y beneficiarse de los resultados de los proyectos.

En este contexto, un grupo de participantes del Diplomado de Auditoria Informática ha propuesto a la Corporación Civil Bolsa de Valores de Guayaquil para el desarrollo de su proyecto final para lo cual requerimos su aceptación formal.

El proyecto es el siguiente:

TEMA: Auditoria de la Seguridad de la Información en el Sistema Electrónico Bursátil (SEB)

Los objetivos y alcance del Tema se encuentran en el documento Anexo.

Integrantes del equipo del proyecto:

Lcda. Mayra Benavides Rodríguez
Ing. Julia Macías Tulcán

Contando con su respuesta afirmativa, le agradecemos la colaboración y las facilidades que brinden a los integrantes del equipo para el desarrollo del proyecto.

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

"Impulsando la Sociedad del Conocimiento"

Una vez finalizado el proyecto, le comunicaremos la fecha de presentación, en la cual, esperamos contar con su presencia.

Atentamente,

Mae. Julia Bravo
Directora
Centro de Educación Continua - CEC

ANEXO

INTRODUCCION

Utilizar el término *seguridad de información*, no es otra cosa que la Protección de la Información y de los sistemas de información del acceso, uso, divulgación, interrupción o destrucción no autorizada. Es importante, señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: La información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada: Esto afecta su disponibilidad y la pone en riesgo. Además debemos considerar a la información como un activo crítico de las organizaciones y como tal se debe preservar su integridad, confidencialidad y disponibilidad.

No obstante es preciso indicar que no es posible eliminar por completo los riesgos, sin embargo es posible reducirlos mediante la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

La Bolsa de Valores de Guayaquil tiene un sistema de negociación electrónica el cual permite la negociación entre participantes, así como la visualización de todas las demandas y ofertas del mercado. Este sistema es vital para el servicio que brinda esta entidad a los miembros del Sector Financiero Bursátil y como tal debe mantener un nivel optimo respecto a la seguridad de la información que procesa.

Es importante que las empresas evalúen las vulnerabilidades a las que están expuestos sus sistemas transaccionales y hagan un mejoramiento de sus controles, implementando estrategias que cubran los procesos.

Los riesgos son uno de los principales problemas en la seguridad que debe enfrentar TI, y para mitigarlos los daños que se puedan generar, se deben asumir medidas para evitar estos conflictos y tener un sistema en condiciones de producir; aunque estas seguridades no proporcionen el 100% de tranquilidad ya que día a día aparece un ataque diferente.

METODOLOGÌA Y ACTIVIDES A REALIZAR

La metodología de trabajo propuesta es la que se describe a continuación:

- ✓ Revisión de documentación Normativas de la Bolsa de Valores de Guayaquil.
- ✓ Revisión de políticas y procedimientos relativos al uso y protección de la información.
- ✓ Revisión e identificación de riesgos en la seguridad de la información
- ✓ Desarrollo de pruebas de controles en la seguridad de la información

ESTÁNDARES INTERNACIONALES DE LA SEGURIDAD DE LA INFORMACIÓN

PARA ESTABLECER LAS MÉTRICAS DE EVALUACIÓN:

- ISO/IEC 27000-series
- ISO/IEC 27002
- Common Criteria
- Orange Book
- COBIT4.0
- COSO

GRUPO DE TRABAJO

EL equipo de trabajo está conformado por:

NOMBRES	TITULO ACADEMICO	CARGO
Julia Macías Tulcán	Ingeniera en Sistemas Computacionales	Representante del Equipo y Auditora
Mayra Benavides Rodríguez	Licenciada en Informática	Auditora

DETERMINACIÒN DE LA DURACION DE PROYECTO

Anl. Emma Pilozo.

1)

Acciones

Software de proyectos para definir actividades, tiempo de duración, recursos

Medios

- Informes sobre los avances de actividades. Estableciendo puntos críticos.
- Pruebas en cada etapa
- Actualización recursos y tiempos

2) No hemos implementado medidas para los ciclos de sistemas, porque hasta el momento, solo se ha realizado mantenimiento de aplicaciones existentes.

Los mantenimientos de nuevas opciones, son de plazo máximo de 3 dias. Los mismos que se los realizando llenando el formulario FOR –SIS-16 V032010

3) Los registros de actividades indicadas en el formulario anterior.

Las atenciones de los usuarios se los realiza de la siguiente forma:

- El usuario envía un correo, aceptando la atención al requerimiento.
- Este correo es archivado en una determinada carpeta con el formato .msg.

4) Los mantenimientos y/o actividades del departamento de sistemas, son revisados por el área de OYM. Quienes después de realizar las pruebas, indica los cambios o sugerencias, antes de su paso para la productividad de lo realizado en el área indicada.

5) No, para mi conocimiento. Sé que sólo se ha usado: ISO 9000 — 2008 -Sistemas de Gestión de la Calidad – Fundamentos y vocabulario

7 **Y** 8) No se han aplicado standards, porque no se ha realizado desarrollo nuevo.

Se pretende aplicar para el desarrollo del nuevo aplicativo lo siguiente:

- Estándares de Nombres de tablas, índices, claves primarias, variables, claves foraneas.
- Estándares en nombre de los programas, con el aplicativo que se vaya a usar.
- La documentación, se la pretende obtener del aplicativo a utilizar.

- Cualquier aplicativo a elegir, debe tener la particularidad, de control de Base, en cuanto a diseño e impacto.
- Se controlará redundancia innecesaria.
- El software realizará los programas de procesamiento, con su metodología propia.
- Para la programación de la base, aplicaremos el estándar recomendado por Oracle. Usaremos esta programación como segundo control del aplicativo.
- La programación del Look an fell, se la realizará por medio de la librería Sencha. No nos hemos puesto de acuerdo, sobre la metodología a usar para esta librería.
- Las pruebas de sistemas, las realizaremos en el prototipo de Diseño.
- Hasta el momento no hemos pensado en la documentación para los casos de pruebas.

Revisión de Recomendaciones dadas por la ESPOL a BVG en auditoria anterior. (Septiembre 2009)

Se requiere hacer una revisión de la adopción que la Bolsa de Valores de Guayaquil, hizo a las recomendaciones sugeridas por los auditores externos en la Auditoria del SEB realizada en septiembre del 2009.

Por lo que solicitamos responder a cada una de las preguntas indicadas a continuación, adjuntado su repuestas a este cuestionario.

Nombre del Entrevistado: Anl. Emma Pilozo.

1. Que técnicas de seguimiento y control de proyectos en el desarrollo y/o compra de software, se han implementado.
2. Que métricas en el ciclo de desarrollo o compra de software se utilizan ?
3. Que tipo de registros de las actividades del área de informática se han implementado?
4. Como se ha mejorado la documentación de políticas, procedimientos, y estándares de documentación se ha utilizado para el efecto?
5. Se utilizan estándares internacionales en todas las actividades informáticas?
6. Se han utilizado estándares internacionales de tecnología en el desarrollo o compra de software, de los mencionados a continuación?

- ISO/IEC 16085:2004 information technology - Software life cycle processes - Risk management
- ISO/IEC 16326:1999 software engineering - Guide for the application of ISO/IEC 12207 to project management
- ISO/IEC 18019:2004 Software and system engineering - Guidlines for the design and preparation of user documentation for application software ISO/IEC TR 19759:2005 SoftwareEngineering - Guide to the software Enfineering Body of knowledge (SWEBOK)
- ISO/IEC TR 19760:2003 Systems enfineering - A guide for the application of ISO/IEC 15288 (System life cycle processes)

7. Indique si se ha implementado para el desarrollo de sistemas los siguientes puntos:
    - Resumen de los estándares y procedimientos a seguir para el desarrollo de sistema
    - Descripción de los estándares y procedimientos a seguir para el desarrollo del sistema
    - Documentar los estándares y procedimientos haciendo referencia a las tareas y técnicas de la base de conocimientos apropiadas y anotando cualquier excepción de los procedimientos.
8. Indique si se ha implementado estándares de desarrollo de sistemas para la documentación de elementos tales como:
    - Convención de nombres para los ficheros (permanentes y temporales)
    - Procedimientos,
    - Variables,

- Ficheros de prueba.
- Actualización de la documentación
- Control de versiones de la documentación
- Formato homogéneo de la documentación
- Nivel de detalle requerido para la documentación de proyectos
- Paquetes entregables requeridos (p. ej. documentación escrita, casos de pruebas)
- Flujo lógico de procedimientos dentro de un programa
- Tamaño y complejidad de los procedimientos
- Separación de las funciones de entrada/salida de las funciones computacionales.
- Procedimiento de manejo de errores
- Uso de variables globales vs. variables locales
- Niveles máximos de anidamiento.
- documentación mínima de las pruebas y los casos de pruebas
- Documentación de los casos de prueba, los resultados esperados y los datos de pruebas
- Métodos para ejecutar pruebas
- Métodos para documentar los resultados reales
- Métodos para la corrección de errores

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO

AUDITORÍA DE CONTROLES

Empresa: Bolsa de Valores de Guayaquil.

Área de Control: Organizacion y Metodos - Auditoria

Nombre de Entrevistado: Ana. Ana León Celi

Cargo de Persona Encuestada: _____

Dominio 5
Dominio 6
Dominio 8

FECHA		
DIA	MES	AÑO
17	08	2011

	PREGUNTAS	RESPUESTAS			Comentarios acerca de todas las respuestas negativas. Información adicional acerca de las respuestas positivas.
		N/A	SI	NO	
Revisión de la Organización del ambiente Informático					
1	El área de TI dispone de una organización funcional		X		Existe un area de Centro de Computo donde estan los operadores y responsables del Soporte El area de los Analistas de Sistemas El area de Organizacion y Metodos
2	El organigrama funcional es adecuado para el tamaño del área				8.1.1
3	Se han definido políticas y procedimientos para cada una de las actividades de TI		X		Existen Politicas para ciertos procesos de T.I. y están documentadas en el Manual de Calidad DOMINIO 5 Objetivo 5.1 5.1.1: Documento Politica de Seguridad Polit Seg de la Inform 5.1.2
4	Existe una adecuada separación de funciones en todas las áreas funcionales		X		6.1.3 10.1.3
5	La gerencia de TI ha definido una planificación estratégica real de las tareas a efectuarse			X	No es conocido por todo el personal de Sistemas. Los Directores la elaboran pero no se entrega un documento, se asignan tareas de acuerdo a requerimientos por cambios en Leyes o Reglamentos 6.1.
6	Existe una adecuada separación de funciones dentro del sector de Control de datos, bibliotecas de archivos, control impreso, montaje de trabajo			X	Estas funciones no están definidos. 6.1.3
7	Dispone de estándares operativos adecuados que otorguen seguridad a los procedimientos y métodos de operación			X	Las funciones estan definidos y el personal conoce por su experiencia los procedimientos y métodos. No se sigue ningún estandar internacional conocido.

Firmas:

_____ _____

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO

AUDITORÍA DE CENTRO DE CÓMPUTO

Empresa: Bolsa de Valores de Guayaquil

Área de Control: Sistemas

Nombre de Entrevistado: Ing Helen Egas

Cargo de Persona Encuestada: Analista de Sistemas

FECHA		
DIA	MES	AÑO

	PREGUNTAS	RESPUESTAS N/A	SI	NO	Comentarios acerca de todas las respuestas negativas. Información adicional acerca de las respuestas positivas.
Revisión de la metodología para el desarrollo de sistemas de información					
1	Existe una metodología para el desarrollo de proyectos			X	Para el desarrollo interno se utiliza el manual de Procedimientos de y para el SEB se les desarrollo Externo
2	Se mantiene un control de cambios de las librerias de las aplicaciones en produccion ?		X		Para este se utiliza los formularios que lo maneja
3	Se mantiene documentacion de los procesos implementados y correspondientes alcances y requerimientos de usuario ?		X		Se existen formatos para requerimientos y los Manuales de Procedimientos y los Manuales que entrega ICAP como Especificaciones
4	Se mantiene documentado el plan de pruebas previa salida a produccion de los cambios aplicados a los sistemas?			X	No se hace un plan de pruebas documentado solo se indica la fecha de inicio y se prepara los equipos del C.C. para el laboratorio y está a cargo de los operativos de Red VAL.

Firmas:

Encuestado

Auditor Encuestador

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO

AUDITORÍA DE CENTRO DE CÓMPUTO

Empresa: Bolsa de Valores de Guayaquil

Área de Control: Centro de Computo

Nombre de Entrevistado: Eladio Ronquillo.

Cargo de Persona Encuestada: Técnico

FECHA		
DIA	MES	ANO
23	08	2011

	PREGUNTAS	RESPUESTAS			Comentarios acerca de todas las contestaciones negativas. Información adicional acerca de las contestaciones positivas.
		N/A	SI	NO	
Revisión de la Transmisión de Datos					
1	Utiliza Modem para la Transmisión de Datos			X	
2	Dispone de un Modem de reserva en areas claves de la Red			X	
3	Utiliza Modems con capacidad de detectar mal funcionamiento	X			
4	Utiliza equipos Routers para la transmision de datos		X		Router CISCO 1600 con PROV. CNT. Administrado y Configurado.
5	Utiliza Routers con capacidad de administración		X		La Administra el Provee CNT.
6	Utiliza swichts administrables en su red interna		X		3COM es el SWIT principal. 10.1.100.X.
7	Se registra fecha y hora de los mensajes enviados y recibidos		X		El SEB si se registran con log del sistema con Mensajes.
8	Aplica numeración consecutiva a los mensajes en la transmisión de los mismos	X			Se almacena por Tiempo Cronologico.
9	Utiliza mecanismos de devolucion de llamadas Call Back para las lineas de comunicación		X		La Central Telefonica permite dejar Mensaje
10	Utiliza encriptación algoritmicas para la transmisión de datos		X		El SEB si lo maneja para transmitir los datos
Recuperación de desastres					
11	Posee la organización procedimientos que aseguren razonablemente la continuidad del negocio?.		X		Es muy conocido por el personal y usuarios para el SEB.
12	Existe una evaluación de riesgo?			X	No hay algo formalizado
13	Existe un plan formal de contingencias aprobado por la Gerencia General o Alta Dirección?		X		SI
14	Se tiene definidos niveles de emergencias y tolerancias sobre las interrupciones?			X	Formalmente no se lo conoce
15	Se dispone de un sitio alterno para la recuperacion, y de poseerlo, se tiene un inventario de elementos almacenados en este sitio y su mantenimiento?			X	Solo el Servidor para el SEB q' está en Quito.
16	El personal esta capacitado sobre el plan de contingencias?			X	Formalmente NO.
17	Existe un plan de mantenimiento para actualización del plan de contingencias			X	No se conoce formalmente.
18	Existe un registro de las pruebas realizadas al plan de contingencia?			X	No lo conoce.
19	Posee un plan formal de pruebas			X	No lo conoce.
20	En caso de tener contratado el servicio de contingencias, se tiene un procedimiento para esta contratación?	X			

Firmas:

Encuestado

Auditor Encuestador

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO

AUDITORIA DE CENTRO DE CÓMPUTO

Empresa: _____

Área de Control: Sistemas.

Nombre de Entrevistado: Anl. Maura Brito

Cargo de Persona Encuestada: Analista Program.

FECHA		
DIA	MES	AÑO
	08	2010

	PREGUNTAS	RESPUESTAS N/A	SI	NO	Comentarios acerca de todas las contestaciones negativas. Información adicional acerca de las contestaciones positivas.
Seguridad en los Sistemas de Bases de Datos:Aspectos Legales,sociales y éticos					
1	La Base de Datos que utiliza la organización mantiene licencias de uso actualizadas			X	Es licenciada Oracle - pero no esta actualizada.
2	Existe una Política de la organización para discriminar entre información de uso público y confidencial o privado.		X	X	Existe pero no esta seguro, revisar en OYM
3	Existe un área funcional especifica para la administración de la Base de Datos			X	
4	El personal encargado de la seguridad de la Base de Datos, ha sido capacitado y tiene experiencia para esta actividad.			X	
5	El personal encargado de la seguridad de la Base de Datos, cumple esta unica función.			X	
Seguridad en los Sistemas de Bases de Datos: Controles de tipo físico, acceso a las instalaciones					
6	El acceso físico al Servidor de Base de Datos esta bloqueado para el personal que no tiene la función de DBA		X		
7	Es posible realizar un monitoria de los usuarios que se conectan remotamente a la Base de Datos.		X		Pero no se realiza como funcion especifica del personal.
8	Existe algún esquema de ambiente de pruebas de la Base de Datos (cual es)		X		Desarrollo y Produccion
Seguridad en los Sistemas de Bases de Datos: Identificación de usuarios: voz, retina del ojo, etc.					
9	Existe un esquema organizacional para el control de privilegios y roles de usuarios de la Base de Datos			X	Aun se esta diseñando el esquema en Area de Sistemas.
10	Las contraseñas de los usuarios puede ser manipulada por el administrador de la Base de Datos	X			Aun se maneja en desarrollo
11	El personal del área de desarrollo tiene acceso a la Base de Datos de producción		X		Para pruebas de producción.
Seguridad en los Sistemas de Bases de Datos:Controles de disponibilidad y continuidad					
12	Existe un procedimiento para respaldo y recuperación de la Base de Datos			X	Aun esta en primeras etapas de utilizacion
12	Se utiliza los conceptos de backup incremementales para los respaldos de la Base de Datos (Diga la Frecuencia)	X			
13	Con que frecuencia se realiza un backup total de la Base de Datos	X			
6	Utiliza alguna herramienta especializada para la realización de los respaldos de la Base de Datos	X			
7	El Jefe de Operaciones o quien haga sus funciones revisa y aprueba la lista de los archivos magnéticos que van al lugar de back-up	X			
8	Se hace un inventario semestral de los archivos magnéticos que están en los lugares de back-up y se confronta contra el listado producido por el paquete de manejo de librerías.	X			
9	Se hace un inventario semestral de los archivos magnéticos que están en la cintoteca y se confronta contra el listado producido por el paquete de manejo de librerías.	X			
10	Si hay diferencias en la confrontación de los inventarios, se reportan al Jefe de Operaciones	X			
11	Las diferencias de la confrontación de los inventarios se investigan y corrigen rápidamente en los registros del paquete de manejo de librerías	X			
12	Los archivos en los lugares de back-up se revisan periódicamente para verificar que la información que esta en el back-up es adecuada (que periodicidad aplican?)	X			
13	Se realiza un proceso de revisión similar con los archivos de los programas en back-up.	X			

Firmas:

Encuestado

Auditor Encuestador

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO

AUDITORÍA DE CENTRO DE CÓMPUTO

Empresa: _____

Área de Control: Sistemas

Nombre de Entrevistado: Anl. Maura Brito y Tecn Eladio

Cargo de Persona Encuestada: Analista y Soporte Operativo

FECHA		
DIA	MES	AÑO
	08	2010

	PREGUNTAS	RESPUESTAS			Comentarios acerca de todas las contestaciones negativas. Información adicional acerca de las contestaciones positivas.
		N/A	SI	NO	
Revisiones de control Nuevas Tecnologías implantadas o migradas		Solitus			
1	Existen pistas de auditorias habilitadas en los sistemas y aplicaciones		X		Logs, q' estan en el mismo ser. de la Aplicación
2	Existe controles de acceso logico a los datos y aplicaciones alojadas en los servidores				
3	Existen herramientas de software capaces de efectuar una rápida y confiable recuperación de información almacenada en base de datos			X	No hay controles / acceso para si procedimiento para detectar accesos y modificaciones en los datos para recuperación
4	Existen programas o aplicaciones actualizados que tengan la documentacion para auditoria y modificación o mantenimiento de sus controles de acceso.			X	
Revisiones de Control					
5	Existen pistas de auditorias habilitadas en los sistemas y aplicaciones				Rechazada (1)
6	Existe un sistema de seguridad para la identificacion de usuarios de los sistemas		X		Modulo de Usuarios pero no se utiliza porque nadie esta utilizandolo
7	Utiliza técnicas para frustrar el uso de contraseñas falsas			X	
Otros controles de Proceso					
8	Se verifican los documentos de autorización u otra información en todos los archivos de entrada en batch para asegurar que la información es completa y autorizada para proceso por el usuario.			X	No se verifica es el sistema el que debe discriminar
9	Se verifican los documentos de autorización u otra información en todos los archivos de entrada en batch para asegurar que la información es completa y autorizada para proceso por el usuario.	X			
10	Se identifica con labels internos y externos todos los archivos batch que se procesan.			X	Es el usuario quien revisa
11	Se valida la completitud de todas las transmisiones de datos en línea con controles de programa y/o hardware.		X		Las aplicaciones tienen las validaciones en programación
12	Se registran todas las terminaciones anormales causadas por sofware?		X		Se registran en logs.
13	Se reportan al Jefe de Operaciones, estadísticas que incluyen el tiempo perdido por terminación anormal de programas.	X		X	

14	Las terminaciones anormales por programa, también se reportan al grupo de programación (sistemas, DBMS, o aplicación)		X		Se reportan para buscar Soluciones pero no lo reporta estadísticamente
15	Las terminaciones anormales se reportan al usuario si se interrumpe el proceso de aplicación.		X		Lo automático, las aplicaciones
16	Las instrucciones de operación para los operadores incluyen información sobre los archivos requeridos para cada trabajo. CL.		X		El SEB se opera en C.C. las Aplic. Bolsa. Operación intuido x Externas
17	Estas instrucciones incluyen también información sobre las respuestas a todas las paradas programadas. CL.		X		las instr. se envían por correo. Reposar Doc. de Instructivos.
18	Para los programadores en línea existen procedimientos de checkpoint y reinicio.	X			
19	Todos los equipos (computador y telecomunicaciones) están protegidos adecuadamente contra incendio.		X		En el Centro C. existe extintor y en todas las áreas
20	Hay controles adecuados de humedad y temperatura para los equipos sensibles. CL.				
Redes y Sistemas Distribuidos					
21	Existen políticas de seguridad? ¿Cuáles?			X	Solo es conocido por el proveedor Global Crossing.
22	Existe un procedimiento para las altas, bajas y modificaciones de acceso a la red. ¿Como es?			X	Si comunica con un correo.
23	Existe personal asignado			X	El personal de soporte ayuda, la inst. se hace con un proveedor,
24	Conoce Ud. Dónde están ubicados los respaldos de la información	X		\	Respaldos Semanales en C.C
25	Conoce Ud., sobre las políticas de seguridad? ¿Qué metodología se utilizó para la difusión?			X	

Firmas:

2 personas

Encuestado Auditor Encuestador

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO

AUDITORÍA DE CENTRO DE CÓMPUTO

Empresa: _____

Área de Control: Centro de computo

Nombre de Entrevistado: Ing. Gladis Ronquillo.

Cargo de Persona Encuestada: Tecnico.

FECHA		
DIA	MES	AÑO
23	Agosto	2011

	PREGUNTAS	RESPUESTAS			Comentarios acerca de todas las contestaciones negativas. Información adicional acerca de las contestaciones positivas.
		N/A	SI	NO	
Revisión de soporte a usuario					
1	Las Pcs tienen instalado software licenciado?		x		todo lo que es Microsoft esta licenciado
2	Existen manuales de operación y usuario de los software y aplicaciones utilizadas por los usuarios finales. ?		X		Existe el documento.
3	Existe personal capacitado con experiencia que atienden los requerimientos de los usuarios. ?		X		los tecnicos de Redeval.

Firmas:

Encuestado

Auditor Encuestador

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO
AUDITORÍA DE CONTROLES

Empresa: ______________________________

Área de Control: ______________________________

Nombre de Entrevistado: ______________________________

Cargo de Persona Encuestada: ______________________________

FECHA		
DIA	MES	AÑO
	06	2011

	PREGUNTAS	RESPUESTAS N/A	SI	NO	Comentarios acerca de todas las contestaciones negativas. Información adicional acerca de las contestaciones positivas.
	Revisión de los controles del software de aplicación				
1	Se han detectado errores en la información por falta de control en el ingreso de datos en el SEB ?		X		Sai se detectan: se lleva a lab el error para simulación para solicitar corrección a ICAP.
2	Se mantiene documentación acerca el manejo de excepciones en el procesamiento de información diario realizado en el SEB?		X		FOR-38 para control. – Los log capturados del SEB no es automático.
3	El sistema se comporta y cumple los objetivos con los que fue diseñado y cumple los requerimientos especificados en el alcance de la solución ?		X		Se lo debe probar en lab. pero si no sucede se debe simular el comportamiento para solicitar corrección
4	¿Se verifica que las transacciones cumplan con las regulaciones vigentes? De que forma?		X		No hay verificación formal. En lab se verifica funcionalidad de acuerdo a lo solicitado (Existe un formato) Sistemas verifica la funcionalidad
5	¿Existen validaciones para el ingreso de datos de tal manera que cumplan con el formato establecido? Revisar el formato		X		empresa con los datos que tenga que ver con el cambio funcional solicitado. Existe un check list pero no se utiliza quedó en desuso. Se realizan basado en la experiencia y conocimiento del SEB (Heley – J.A. Aguil)
6	¿Se verifica que las transacciones cumplan con las políticas internas?		X		Se basa en el pedido o solicitud. pero hay un documento que lo formalice.
7	¿Existen autorizaciones según el rol para el acceso a lectura y/o escritura de datos?		X		Se maneja a través del documento que se envía por mail interno. Y en el C.C. un operador crea el usuario
8	¿Se realizan procesos automáticos de actualización masiva de datos?				Al inicio del día: se actualiza las tablas de desarrollo desde el servidor. El archivo es un .cmd. Se documenta en bitácora cuando sucede.
9	¿Se dispone de un calendario de estos procesos automáticos?	X		X	Se hace todos los días las actualizaciones de Tablas de Pagos y se hacen procedimientos manuales de verificación
10	¿Existe un control para verificar que los procesos cumplan con los diseños aprobados?		X		FOR-38
11	¿Existen políticas de cambio de clave para el acceso a los datos en producción?				Los operadores se lo conocen por su experiencia en el manejo del SEB
12	¿Se verifica que las salidas de datos cumplan con las definiciones establecidas?		X		En el laboratorio por conocimiento y experiencia

13	¿Existe un proceso formal de control de cambios?				FOR-38 y FOR-39 - Control - Acta hb
14	¿Se graba el usuario, fecha y hora de ejecución de las transacciones?			X	- El registro tiene esos campos
15	Existe un Registro de log del sistema: Tanto de transacciones correctas e incorrectas		X		Se guarda en el Servidor y por reportes sólo por medio del Sistema en C.C. por un operador. Solo los revisa ECAP y se le envía un detalle completo si existe algunos. ECAP le indica cuando existe un reporte para q le revisen los operadores.
16	Existe un Registro de autoría de los usuarios que usan la aplicación		\	X	
17	Existe un Reporte del perfil del menú de los usuarios.			X	Si existe y pueden existir usuarios obsoletos porque no llega el requerimiento formal de deshabilitación. El reporte no da la info que estamos.
18	Se Realizan transacciones previamente ingresadas para verificar la valides de los resultados y comprobar validaciones.		X		En el laboratorio existen operaciones de transacciones probadas
19	Existe lista de errores reportados y control del seguimiento y la solución de los mismos		X		FOR-39.
20	Es posible obtener reportes de las alertas enviadas por el sistema SEB		X		Las alertas de Usuario, conexiones pero no se crean reporte si se le necesita (archivo excell)
21	Existe un plan de contingencia para transacciones en línea		X		Documentado
22	Existe reporte de los usuarios activos e inactivos que tienen acceso al sistema (verificar)		X		
23	Existe un registro de las autorizaciones para transacciones especiales en el sistema (verificar)		X		El operador Director es el unico autorizado y tiene las opciones.
24	Existen políticas de mantenimiento de claves de usuarios.(verificar)		X		Manual.
25	Verificar el reporte de cuentas de usuarios bloqueados		X		De la alerta se genera el excell.
26	Existen políticas de manejo de terminales o pc`s en los que se utiliza el SEB (verificar)		X		No hay restricciones normativas solo q requerimientos de Internet.
27	Existe un Inventario de terminales o pc`s donde se accede a las aplicaciones		X		Si existe un Inv General donde se identifica donde se encuentra (Internamente Externamente) las PC y se entregan a las áreas de Sistemas

Firmas:

Encuestado

Auditor Encuestador

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO

AUDITORÍA DE CENTRO DE CÓMPUTO

Empresa: Bolsa de Valores de Guayaquil

Área de Control: Centro de Computo

Nombre de Entrevistado: Eladio Rengullo

Cargo de Persona Encuestada: Técnico

FECHA		
DIA	MES	AÑO

PREGUNTAS		RESPUESTAS			Comentarios acerca de todas las contestaciones negativas. Información adicional acerca de las contestaciones positivas.
		N/A	SI	NO	
Medidas de prevención de los Usuarios para manejar la protección frente a la presentación de virus.					
1	Se evita abrir archivos que provengan de emisores no reconocidos ?		X		Correo - Los equipos se protegen con SOPHOS 9.5 Servidor y PC.
2	En caso de bajar archivos ejecutables o programas, estos son grabados en un directorio determinado para aplicarles un programa antivirus actualizado ?		X		Los PC los revisa con el antivirus El servidor de correo, toma los .exe y .zip y los pone en directorio de Cuarentena
3	La actualización del programa antivirus es permanente, y frecuente la instalación de nuevas versiones por parte de los usuarios.		X		Actualización en línea en el Servidor (2003 Server) Consola principal.
4	Se tiene la precaución de no dejar dispositivos moviles instalados al momento del arranque ?		X		No hay acceso desde los equipos a Disp. por puertos USB. Restricciones a través de Políticas en Server. Domain BVG DOMAIN
5	Las computadoras aplican un *set up* que modifique la secuencia de arranque de la PC de "primero arranca diskettera y luego disco rigido", por la secuencia inversa, es decir: primero disco rigido y luego diskettera.			X	Tienen Arranque fijo y los cambios son manuales

Firmas:

Eladio Rengullo

Encuestado

Auditor Encuestador

CUESTIONARIO DE EVALUACION DEL CONTROL INTERNO

AUDITORÍA DE CENTRO DE CÓMPUTO

Empresa: ______DECEVALE

Área de Control:____________CENTRO DE COMPUTO

Nombre de Entrevistado: ___CHARLES CALI

Cargo de Persona Encuestada: ____________ASIST. SISTEMAS

FECHA		
DIA	MES	AÑO

	PREGUNTAS	RESPUESTAS			Comentarios acerca de todas las contestaciones negativas. Informacion adicional acerca de las contestaciones positivas.
		N/A	SI	NO	
Condiciones de Seguridad física de un Centro de Cómputo					
1	Los equipos de computación se encuentran ubicados en un recinto cerrado ?		X		Existe un area de servidores
2	Dicho recinto contiene aberturas provistas de sistemas de bloqueo de accesos adecuados? (Puertas con sistema de seguridad)		X		puertas con sistema de seguridad
3	El local está provisto de sistema detector de fuego?		X		
4	El local se encuentra sobre una plataforma que asegura la imposibilidad de ser afectado por inundación?		X		ESTA EN UN PRIMER PISO ALTO
5	Solo personal autorizado puede desbloquear el acceso?		X		
6	El área se encuentra resguardada y si sólo el personal autorizado tiene acceso a la misma		X		
7	Mantiene un área de comunicaciones separada del área de procesamiento de datos			X	En el mismo cuarto de servidores esta el área de comunicaciones
8	Existen ID de acceso al personal auotorizado al cuarto de conmutación		X		
9	Mantiene actualizada la lista del personal autorizado para acceder al area de procesamiento de datos y el area de comunicaciones		X		Esa lista la meneja el Dpto De Gestion de Calidad
10	Existe y es conocido un plan de actuación para el personal de centro de computo, en caso de incidentes naturales u otros que involucren gravemente la instalación.		X		Existe un plan de seguridad pero no se realiza simulacros ni pruebas
11	Existe separación del ambiente de pruebas y el ambiente de produccion			X	Solo a nivel de Web; en sistemas - los 2 servidores de desarrollo están junto al de [illegible].

Firmas:

Encuestado

Auditor Encuestador