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 AUDITORÌA 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 version 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 Rodríguez	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 Tecnología, 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 auditoría. 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 física 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.

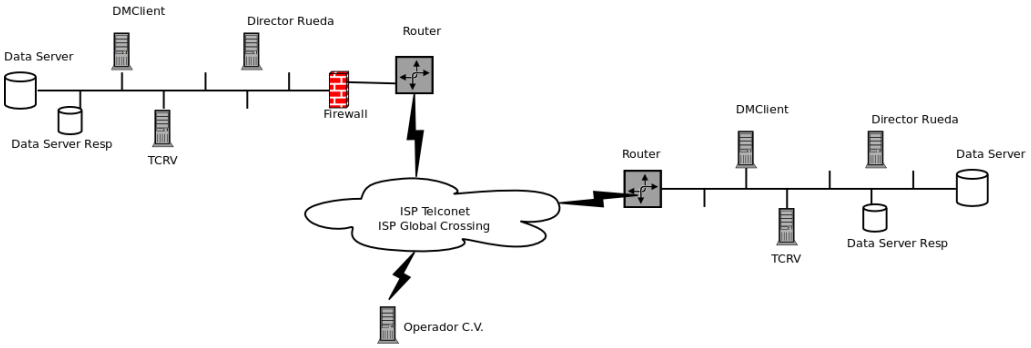
En virtud de lo solicitado, el Economista Arturo Bejarano Ycaza, Director General de la Bolsa de Valores de Guayaquil, autoriza mediante oficio DG.E.2010.0170 de fecha 20 de julio, el tema y lugar con los objetivos y alcance del documento, y designa al Ingeniero Luis Álvarez, como Coordinador del Proyecto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

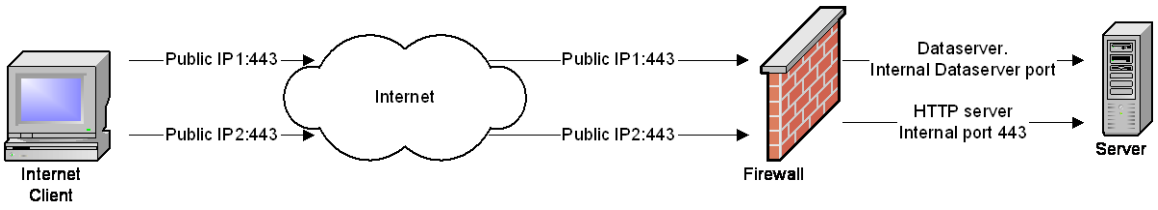
Esta configuración se utiliza en sistemas de tiempo real para proporcionar una mayor velocidad y capacidad en la respuesta a las consultas.

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

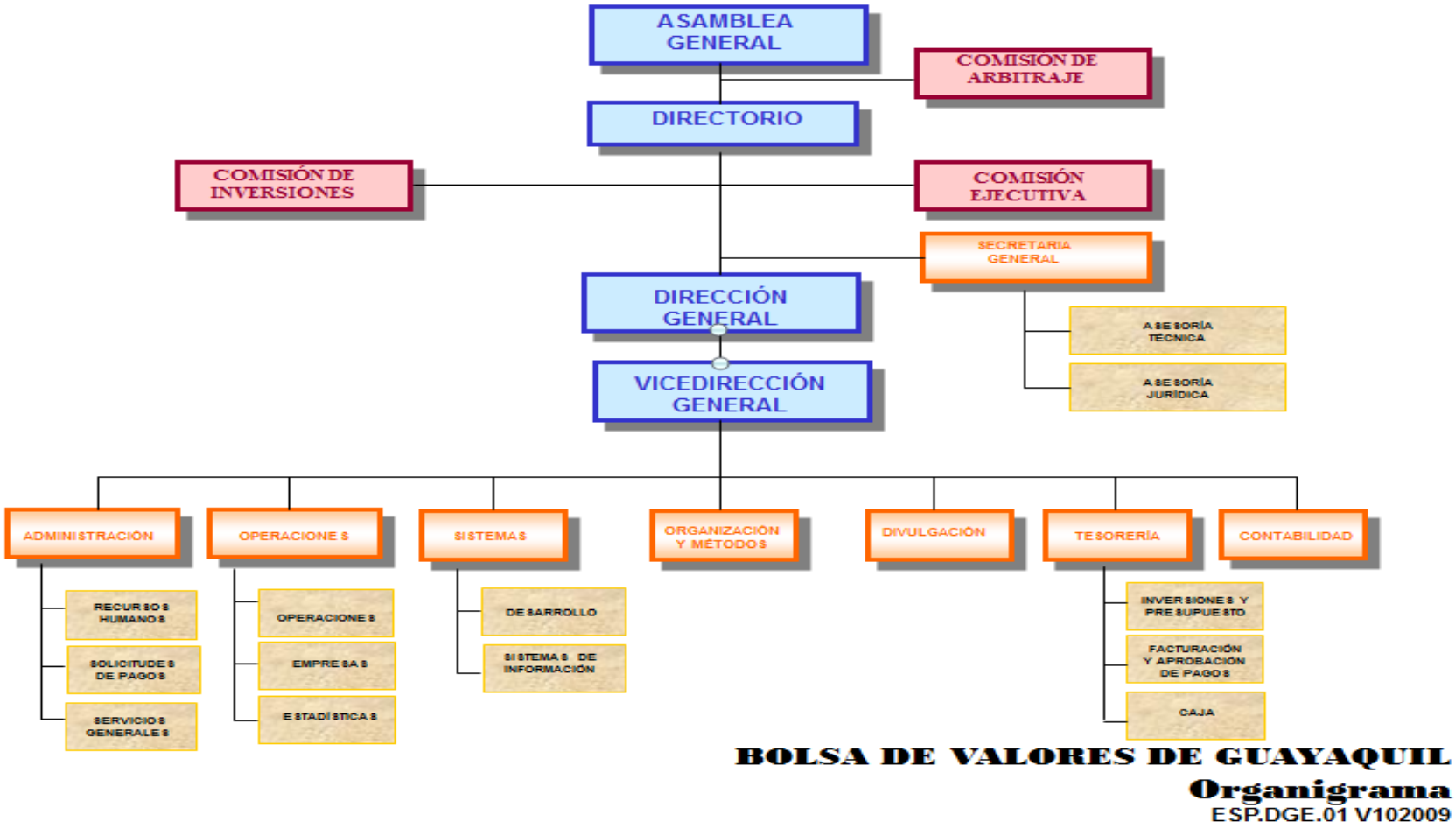
1.3.2. MISIÓN

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. Martin 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. Noemí 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 Políticas 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 Tecnología, 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 sí o no, pero también tenía 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 específicas 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 algorítmicas 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@decevale.com

Mayra Benavidez: mayra_benavid2@hotmail.com

Por la BVG

Luis Álvarez: lalvarez@bvg.fin.ec y luisalvarez@decevale.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 critico 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	SISTEMA: SISTEMA ELECTRONICO BURSATIL -SEB
Persona Encuestada: Luis Alvarez	**Cargo: Director de Sistemas y Operaciones**

Los activos de informacion identificados han sido tasados y se han ordenado de mayor a menor promedio de tasacion

	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 r	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 versión 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

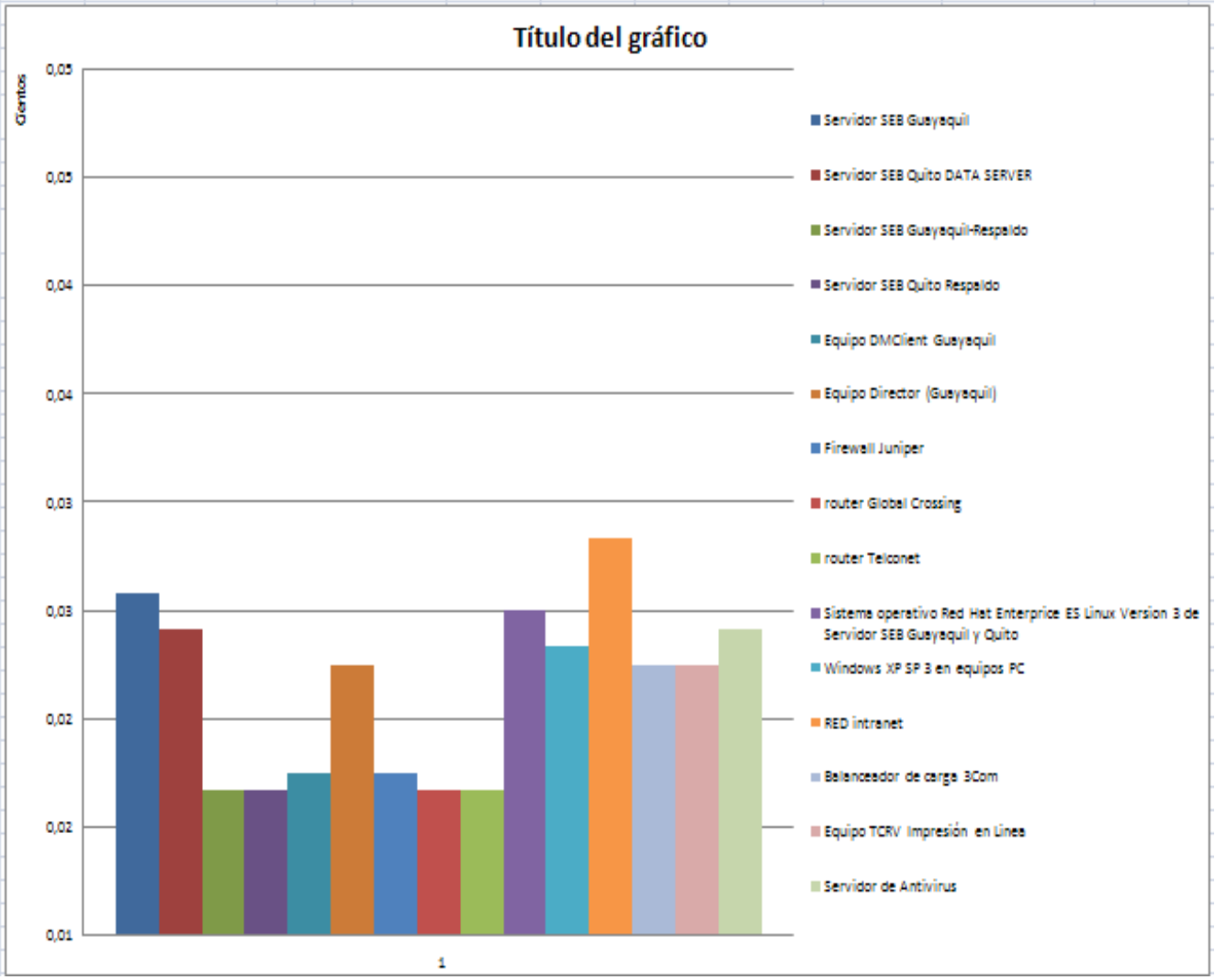
ANLALISIS Y EVALUACION DEL RIESGO
IDENTIFICACION DE VULNERABILIDADES

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 c/vulnerabilidad)	Total de amenaza por cada activo	Selección de Controles
1	Servidor SEB Guayaquil	5	5	5	5	Hacking de información	2	4	3	Utiliza enlace públicos a través de Internet	3	4	3,5	2,5	4	3,25		11.4.3 Identificación de equipos en los redes
						Virus en el Bios	1	3	2	El equipo ya tiene mas de 4 años en una contante	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-Respalda	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	3	2		1	1	1	1	2	1,5	1,66666667	11.4.3 Identificación de
	Servidor SEB Quito Respalda	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	1,66666667	
	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 back	1	3	2		1	1	1	1	2	1,5		10.6.1 Controlar de red
						Saturación del trafico	2	4	3		1	1	1	1,5	2,5	2		10.6.2 Seguridad de los ser
						Deteriro 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 Politica de uso de los servicio de la red
						Deteriro 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 Guayaquil	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 Linea	2,25
Servidor de Antivirus	2,42



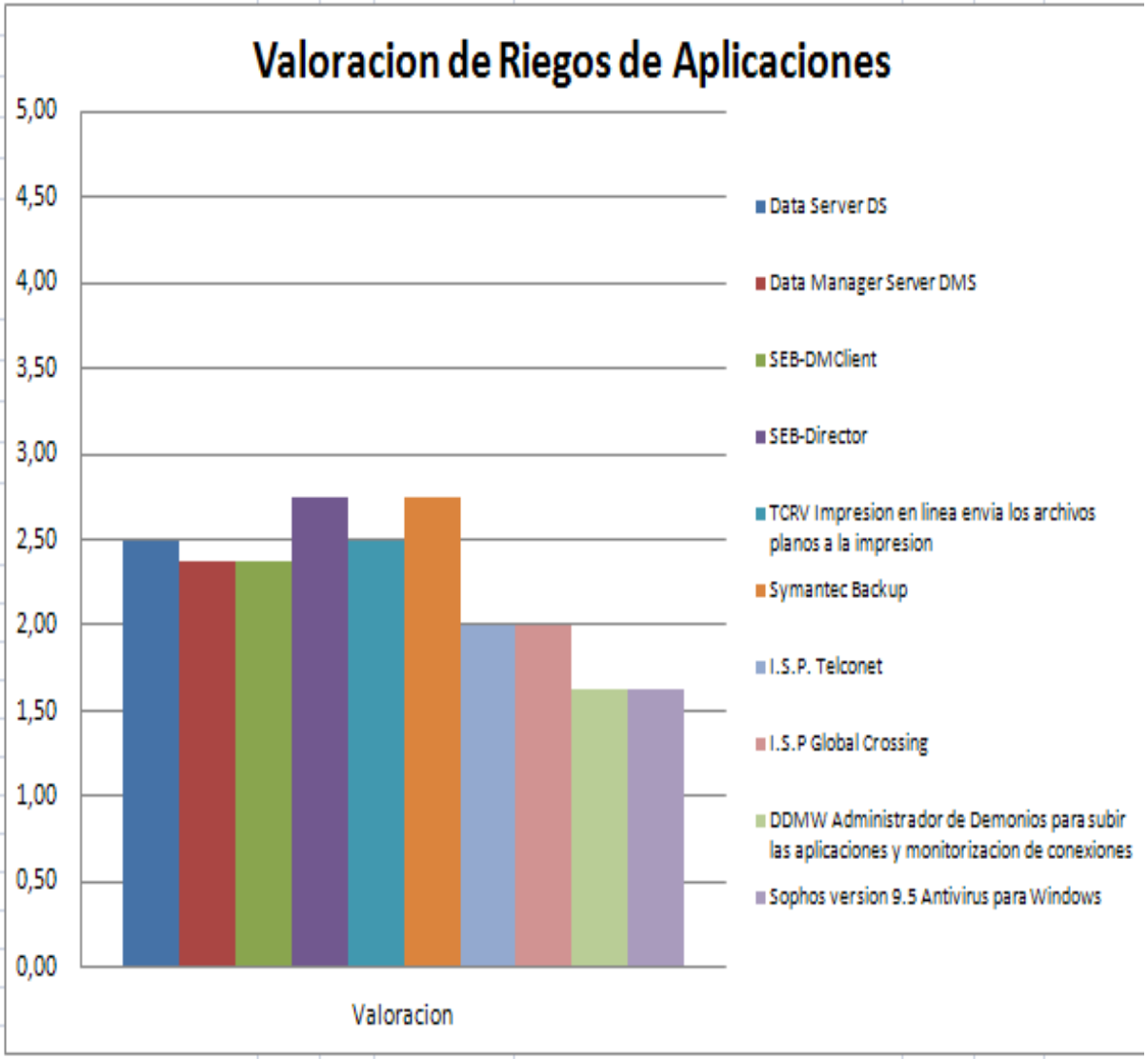
ANLALISIS Y EVALUACION DEL RIESGO

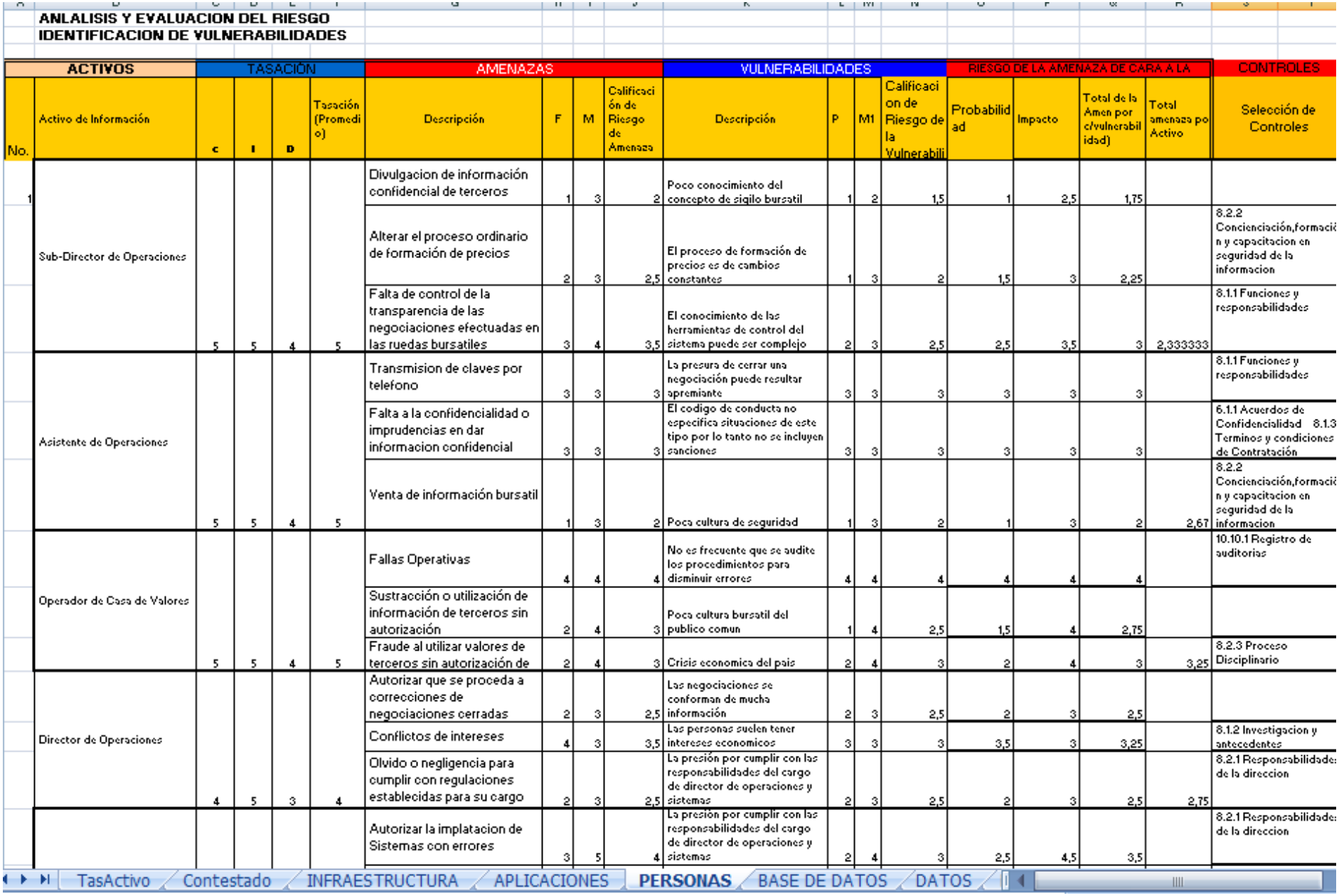
IDENTIFICACION DE VULNERABILIDADES

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	P	M1	Calificación de	Probabilidad	Impacto	Total de la Amen par el vulnerabil	Total de amenazas por Activo	Selección de Controles
1	Data Server DS	4	5	5	5	Perdida de conexión con una de las nadas interconectadas	1	5	3	Las nadas estan conectadas 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 traves 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	5	5	5	Perdida de conexión	1	5	3	El equipo esta conectada a la misma red que todas las 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 una sola usuaria 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 conectada a la misma red que todas las demas equipos	1	2	1,5	1	3,5	2,25		
						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	12.2.1 Validacion de datos de entrada
4	SEB-Director	4	5	5	5	Fallas en ingreso de datos	3	4	3,5	Existen Datos que nos controlan en el ingreso para que puedan ser erroneos Ej. El tipo de sub-esta	1	3	2	2	3,5	2,75		12.2.1 Validacion de datos de entrada
						Acceso 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 Imprimen en linea envia los archivos planos a la impresion					Perdida de conexión con el Servidor	2	4	3	El equipo esta conectada a la misma red que todas las demas equipos	1	3	2	1,5	3,5	2,50		11.4.1 Politicas de uso de los servicios de red
		3	4	4	4	Error por configuración de parametros	2	4	3	Los cambios en la configuración de parametros no requieren	1	3	2	1,5	3,5	2,50	2,50	11.6.1 Restriccion de acceso a la información
	Symantec Backup					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
6		3	4	3	3	Acceso 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
	I.S.P. Telconet					Falta de Disponibilidad	2	3	2,5	El SEB esta configurada para conectarse por Internet	1	1	1	1,5	2	1,75		12.2.2 Control de procesamiento interno
7		3	3	4	3	Ataques de hacking	3	4	3,5	Equipos con IP publicas no protegidos que pueden ser puertos abiertos	1	1	1	2	2,5	2,25	2,00	11.6.2 Aislamiento de los sistemas sensibles
	I.S.P Global Crossing					Falta de Disponibilidad	2	3	2,5	El SEB esta configurada para conectarse por Internet	1	1	1	1,5	2	1,75		12.2.2 Control de procesamiento interno
8		3	3	4	3	Ataques de hacking	3	4	3,5	Equipos con IP publicas no protegidos que pueden ser puertos abiertos	1	1	1	2	2,5	2,25	2,00	11.6.2 Aislamiento de los sistemas sensibles
	DDME Administrador de Domanios para subir las aplicaciones y monitorizacion de conexiones					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
9		3	3	3	3	Desconexion con el server	2	3	2,5	El equipo esta conectada a la misma red que todas las 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
	Saphar version 9.5 Antivirus para Windows					Parar por alto y pro uso 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
10		1	3	3	2	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-DMClient	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
DDMW Administrador de De	1,63
Sophos version 9.5 Antivirus para Windows	1,63





ANLALISIS Y EVALUACION DEL RIESGO
IDENTIFICACION DE VULNERABILIDADES

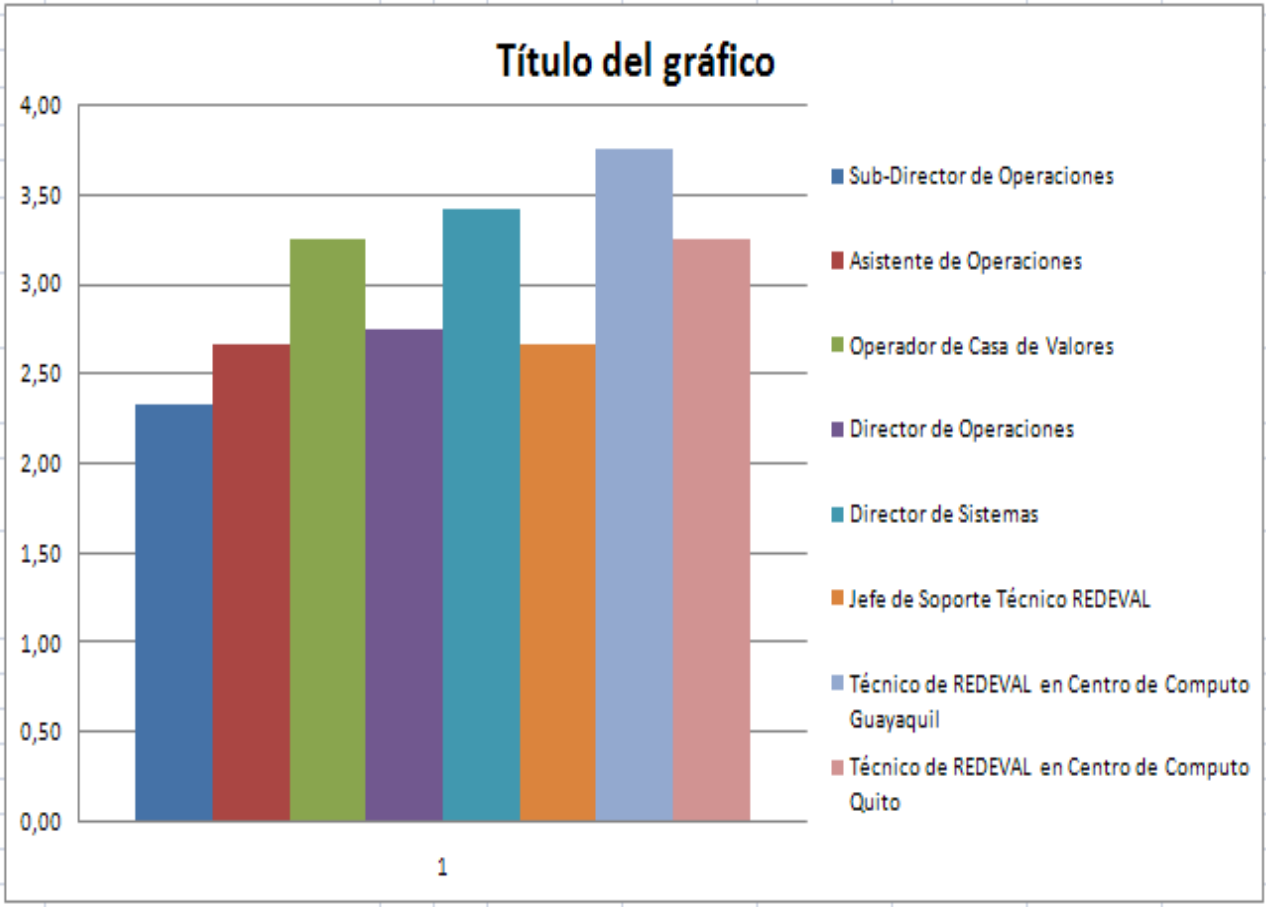
ACTIVOS		TASACIÓN				AMENAZAS				VULNERABILIDADES				RIESGO DE LA AMENAZA DE CARA A LA				CONTROLES
No.	Activo de Información	C	I	D	Tasación (Promedio)	Descripción	F	M	Calificación de Riesgo de Amenaza	Descripción	P	M1	Calificacion de Riesgo de la Vulnerabili	Probabilidad	Impacto	Total de la Amen por 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		
						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	2,333333	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		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	2,67	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		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	3,25	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		
						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	2,75	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	2,5	2,75	8.2.1 Responsabilidades de la direccion
8		Director de Sistemas					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
9							No cumplir los plazos de los proyectos de tecnologia	4	4	4	Poco conocimiento de administración de proyectos	3	4	3,5	3,5	4	3,75		13.2.1 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, choker de información	4	3	3,5	Dependencia de una sola persona quien conoce completamente la herramienta tecnologica	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 magneticos	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 desarrollan los técnicos	2	4	3	3	4	3,5		
15							Profesionales sin conocimiento previo del 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 magneticos	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 entre el personal	3	3	3	Poca difución de las politicas internas al personal	4	4	4	3,5	3,5	3,5		
18							Profesionales sin conocimiento previo del 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 Investigacion 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
20																			
21	Factores de Calificacion de Activo																		
22	I	Integridad																	
23	C	Confidencialidad																	
24	D	Disponibilidad																	
25																			
26	Factores de Calificacion de Riego de Amenaza																		
27	F	probabilidad de Ocurrencia de la amenaza (frecuencia)																	
28	M	Impacto si se Materializa la Amenaza																	
29																			
30	Factores de Calificacion de Vulnerabilidad																		
31	P	Probabilidad que amenaza explote Vulnerabilidades																	
32	M1	Impacto materializarse la Amenaza a causa de la vulnerabbilidad																	

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 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 c/vulnerabilidad)	Total de toda la amenaza	Selección de Controles
						Falta de soporte	4	4	4	es conocida por el	4	4	4	4	4	4,00		12.4.1 Control dels softw
	CTREE+					Obsolecencia y	4	4	4	personal de Tecnologia	4	4	4	4	4	4,00		
1		5	5	5	5	Complejidad de	4	2	3	de la organización sino	4	3	3,5	4	2,5	3,25	3,75	
	Respaldos de ultima versión de la aplicación					Daño fisico de las cintas	4	4	4	No existe un plan de	1	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	1	1	1	2,5	2	2,25		
2		4	5	4	4				0	respaldos porque no lo	1	1	1	1	1	1,00	1,92	

Factores de Calificacion de Activo

I	Integridad
C	Confidencialidad
D	Disponibilidad

Factores de Calificacion de Riesgo de Amenaza

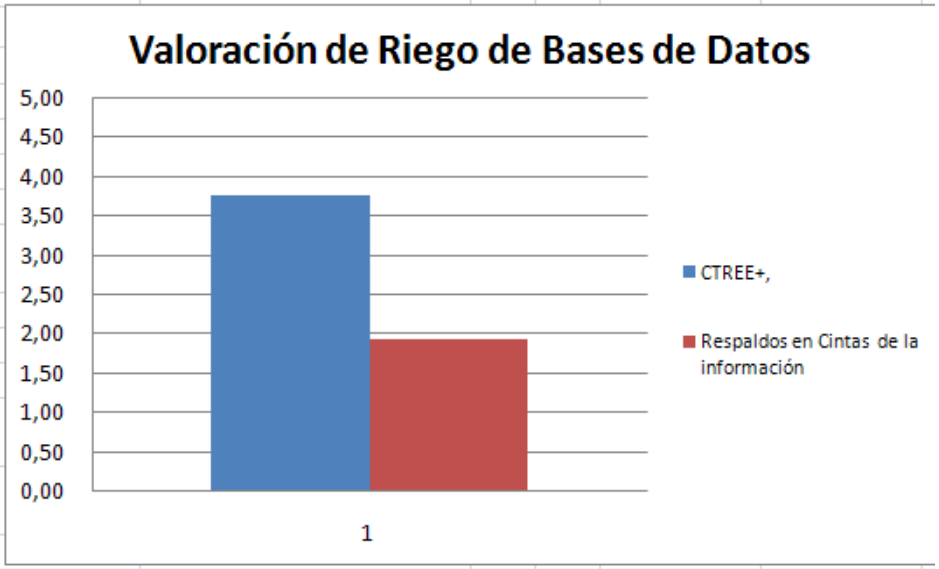
F	probabilidad de Ocurrencia de la amenaza (frecuencia)
M	Impacto si se Materializa la Amenaza

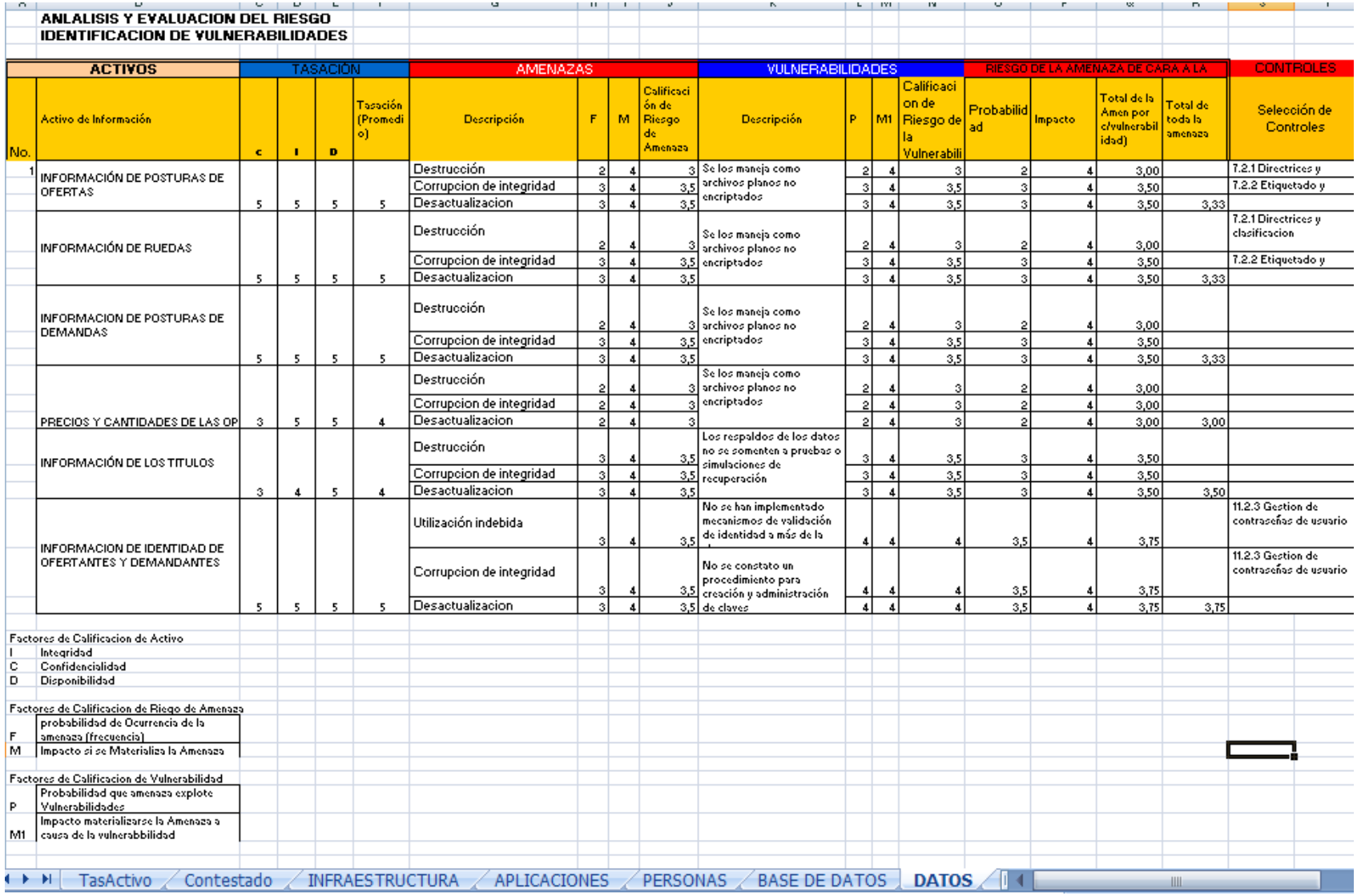
Factores de Calificacion de Vulnerabilidad

P	Probabilidad que amenaza explote Vulnerabilidades
M1	Impacto materializarse la Amenaza a causa de la vulnerabbilidad

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 cl/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 someten 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 a 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 Riego de Amenaza

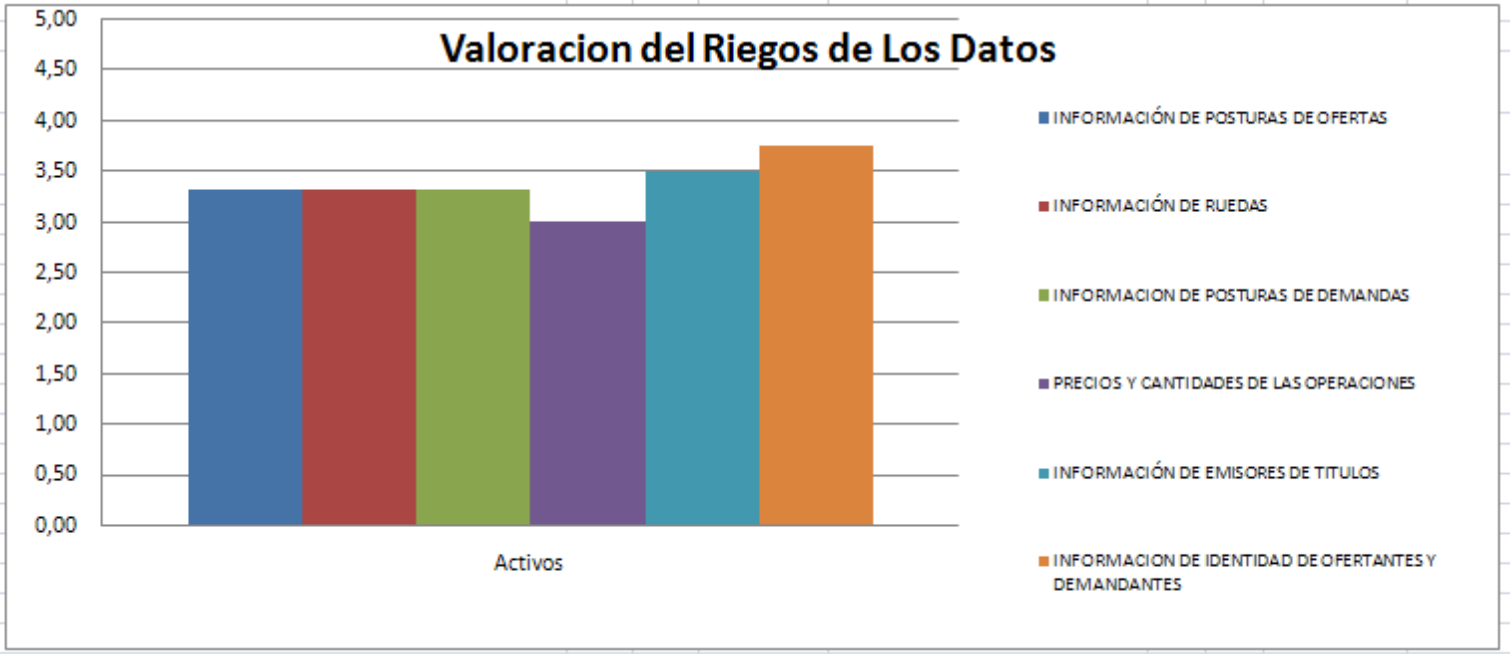
F	probabilidad de Ocurrencia de la amenaza (frecuencia)
M	Impacto si se Materializa la Amenaza

Factores de Calificacion de Vulnerabilidad

P	Probabilidad que amenaza explote Vulnerabilidades
M1	Impacto materializarse la Amenaza a causa de la vulnerabbilidad

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

Activos	Valoración
INFORMACIÓN 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		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 c/vulnerabilidad)	Total de toda la amenaza	Selección de Controles
1	REPORTES DE LIQUIDACIONES	3	5	4	4	Adulteracion	2	4	3	No tienen ningun sistema de validacion como un codigo de Barra solo un numero	3	4	3,5	2,5	4	3,25		10.8.1 Politicas y procedimientos de intercambio de
						Perdida	4	4	4		4	4	4	4	4	4		10.8.2 Acuerdo de intercambio
						Errores de impresión	4	3	3,5	Requiere de un Proceso de impresión con el TCRV	4	3	3,5	4	3	3,5	3,58	15.1.3 Proteccion de los documentos de la
	AUTORIZACIONES PARACREAR USUARIOS DE OPERADORES DE CASAS DE VALORES	3	3	4	3	Falsificacion	2	3	2,5	Son documentos manejados fisicamente pero no se protegen	2	3	2,5	2	3	2,5		
						Adulteración	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	Auge de la delincuencia en la ciudad	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		
						Deteriro	4	3	3,5	No existe una politica que obligue a utilizar un papel resistente 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	4	3	3,5	Falta de control de actualizaciones	4	3	3,5	4	3	3,5		
						Obsolecencia	4	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 Calificacion de Activo

I	Integridad
C	Confidencialidad
D	Disponibilidad

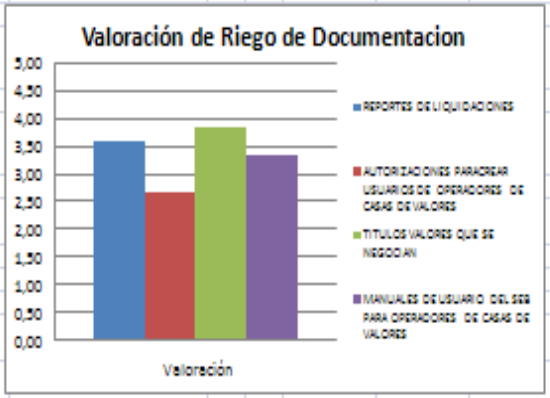
	Valoración
REPORTES DE LIQUIDACIONES	3,58
AUTORIZACIONES PARACREAR USUARIOS DE OPERADORES DE CASAS DE VALORES	2,67
TITULOS VALORES QUE SE NEGOCIAN	3,83
MANUALES DE USUARIO DEL SEB PARA OPERADORES DE CASAS DE VALORES	3,33

Factores de Calificacion de Riesgo de Amenaza

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

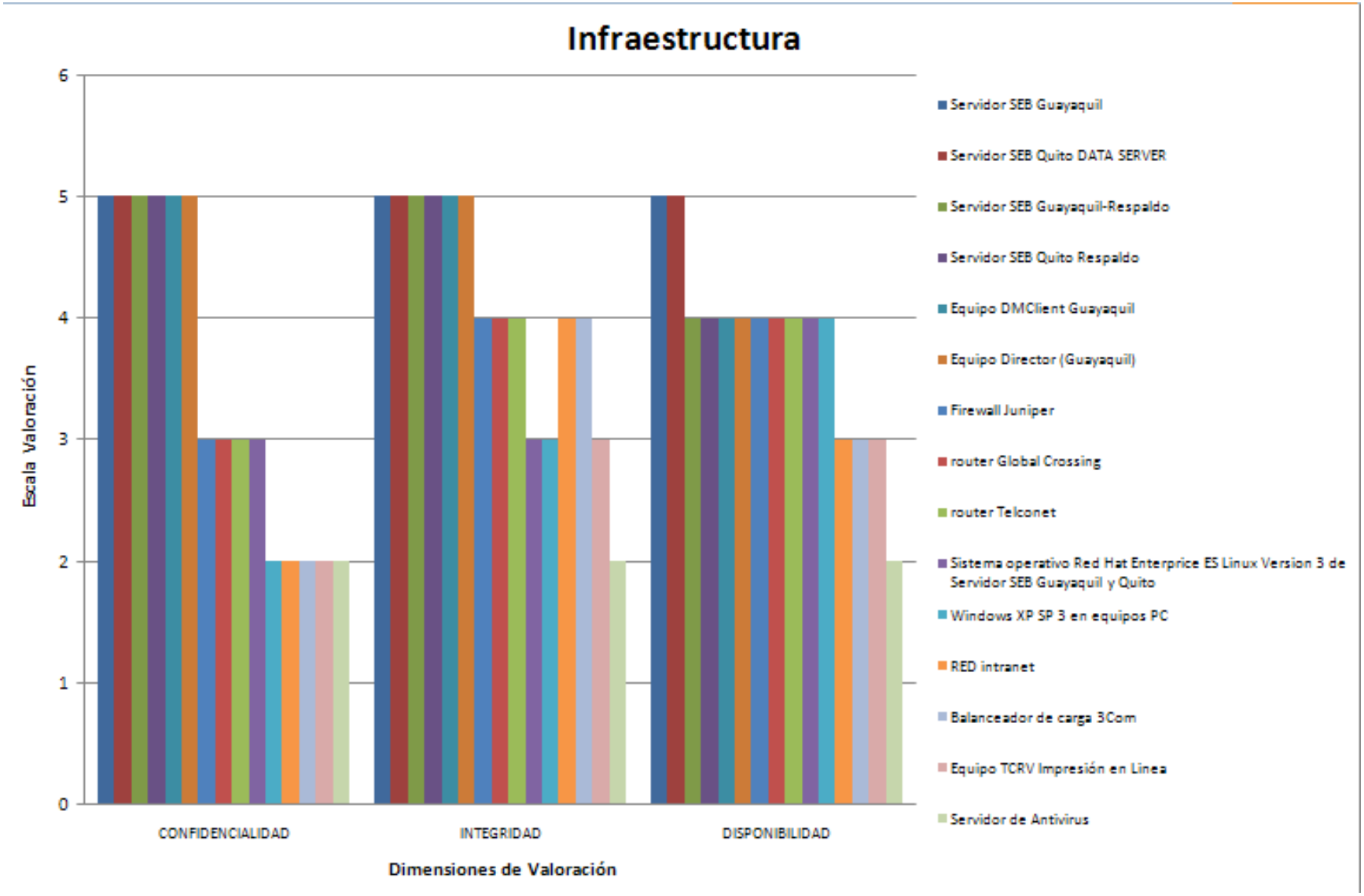
Factores de Calificacion de Vulnerabilidad

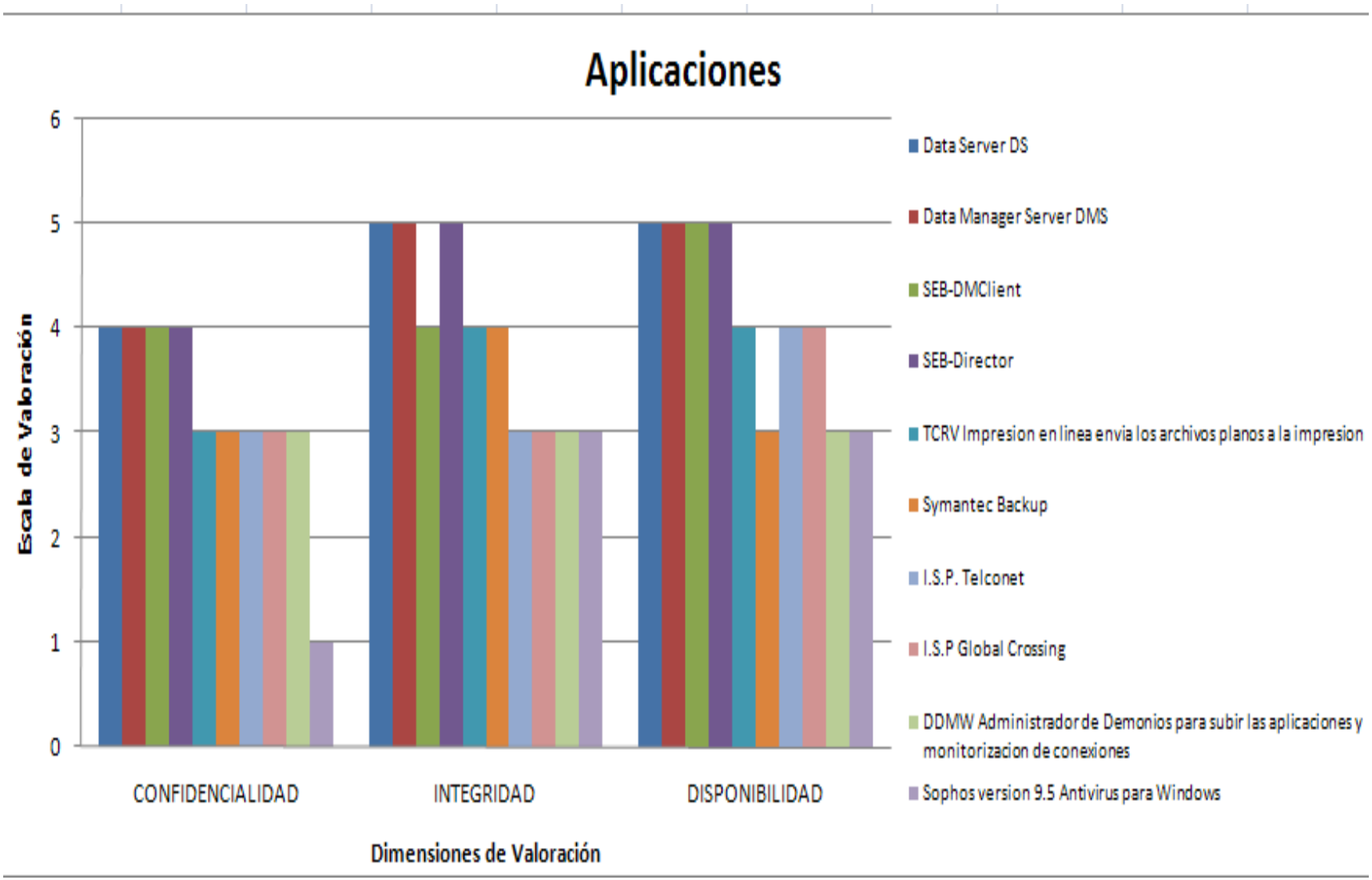
P	Probabilidad que amenaza explote Vulnerabilidades
M1	Impacto materializarse la Amenaza a causa de la vulnerabbilidad

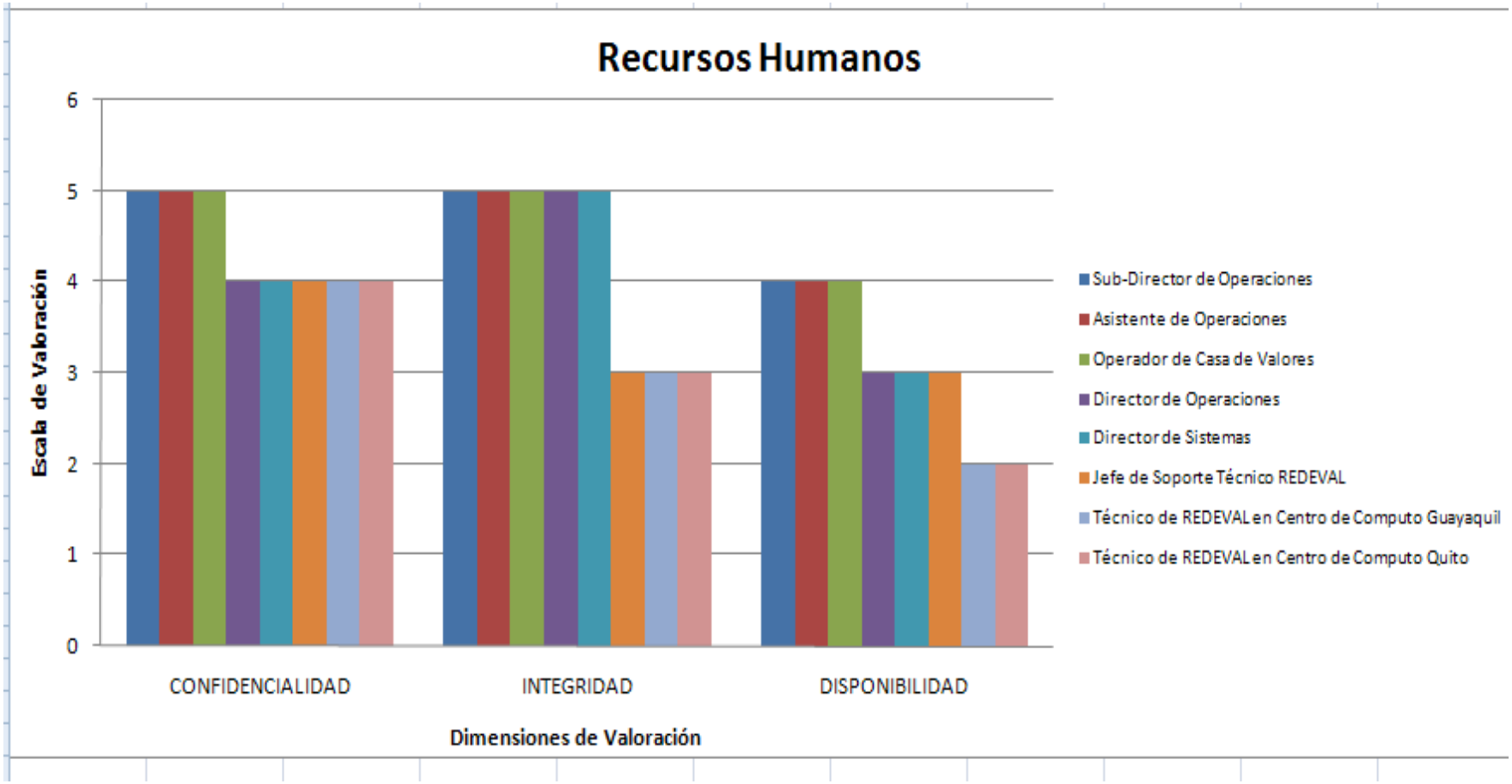


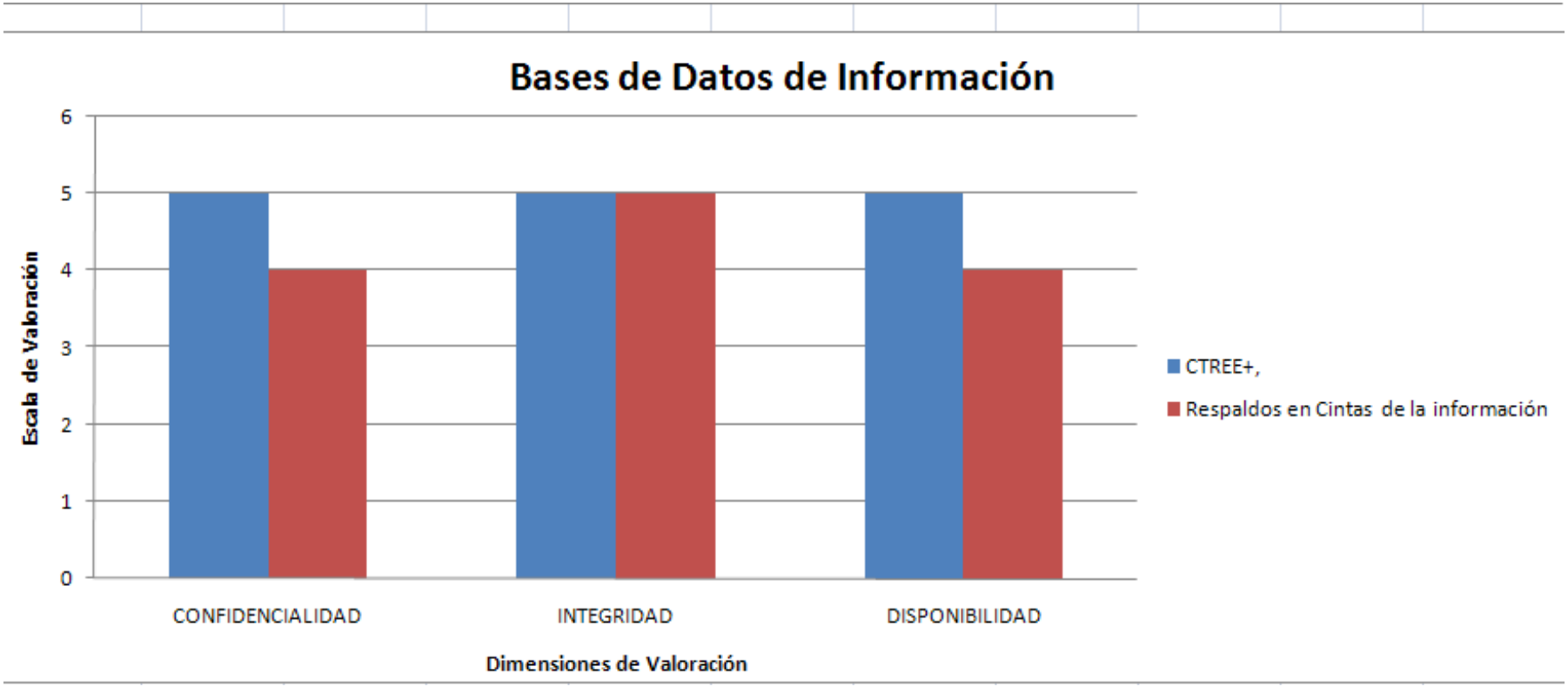
APLICACIONES | PERSONAS | BASE DE DATOS | DATOS | DOCUMENTACION | Graficos de Tasacion

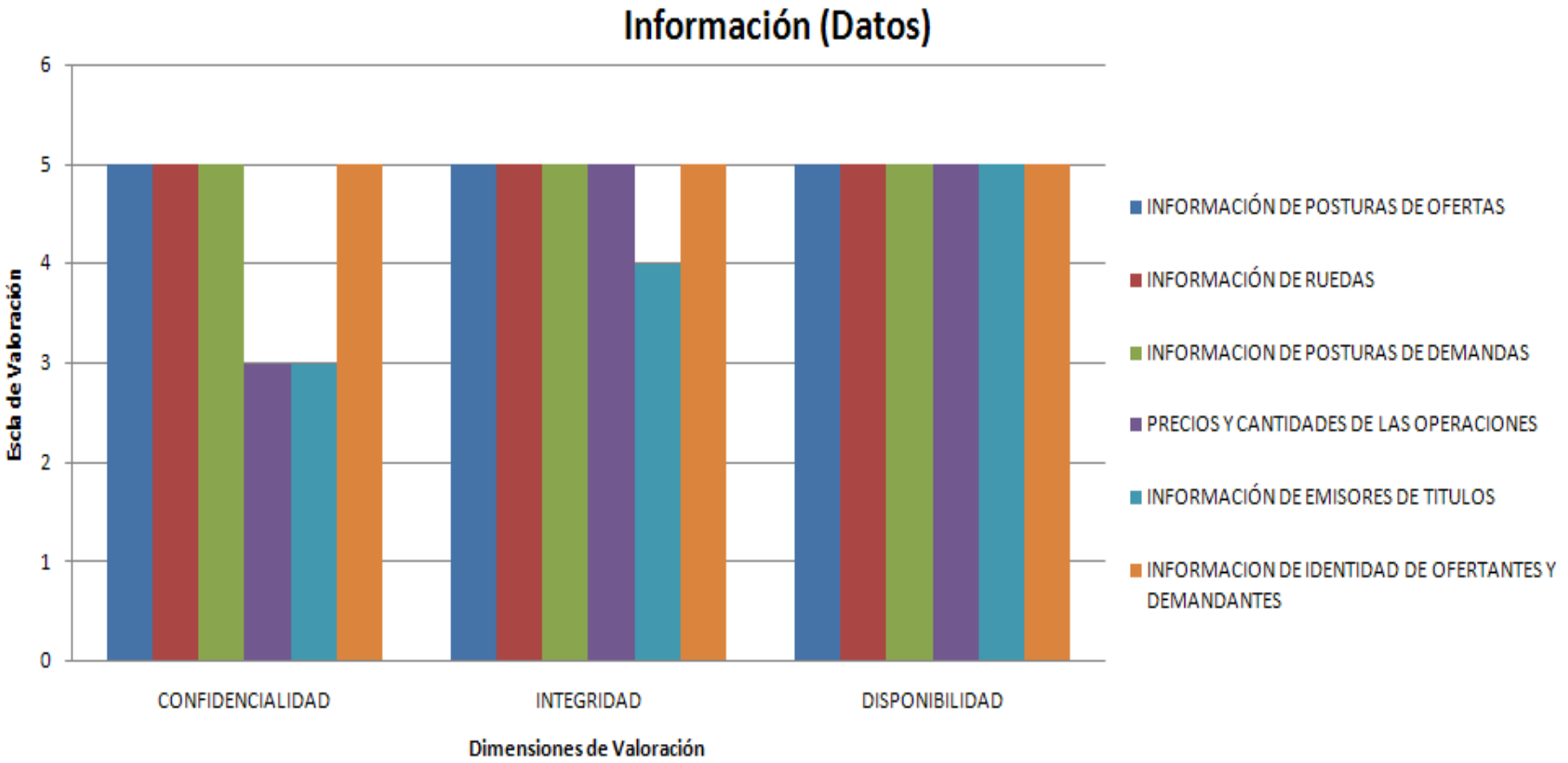
TASACION DE CRITICIDAD DE LOS ACTIVOS

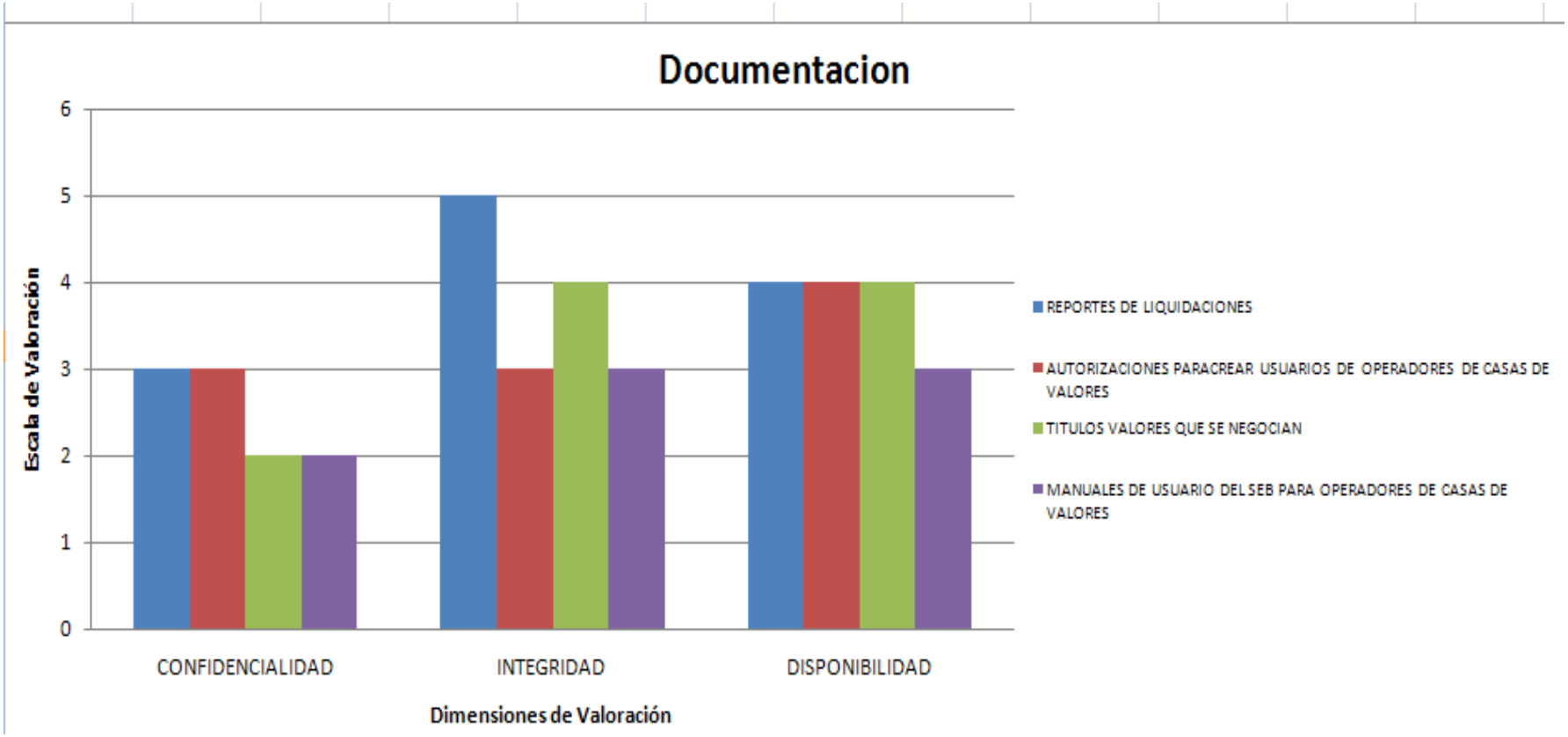

Infraestructura
Escala Valoración
6
5
4
3
2
1
0
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
Servidor SEB Guayaquil
Servidor SEB Quito DATA SERVER
Servidor SEB Guayaquil-Respaldo
Servidor SEB Quito Respaldo
Equipo DMClient Guayaquil
Equipo Director (Guayaquil)
Firewall Juniper
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 Impresión en Linea
Servidor de Antivirus


Aplicaciones
Escala de Valoración
6
5
4
3
2
1
0
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
Data Server DS
Data Manager Server DMS
SEB-DMClient
SEB-Director
TCRV 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

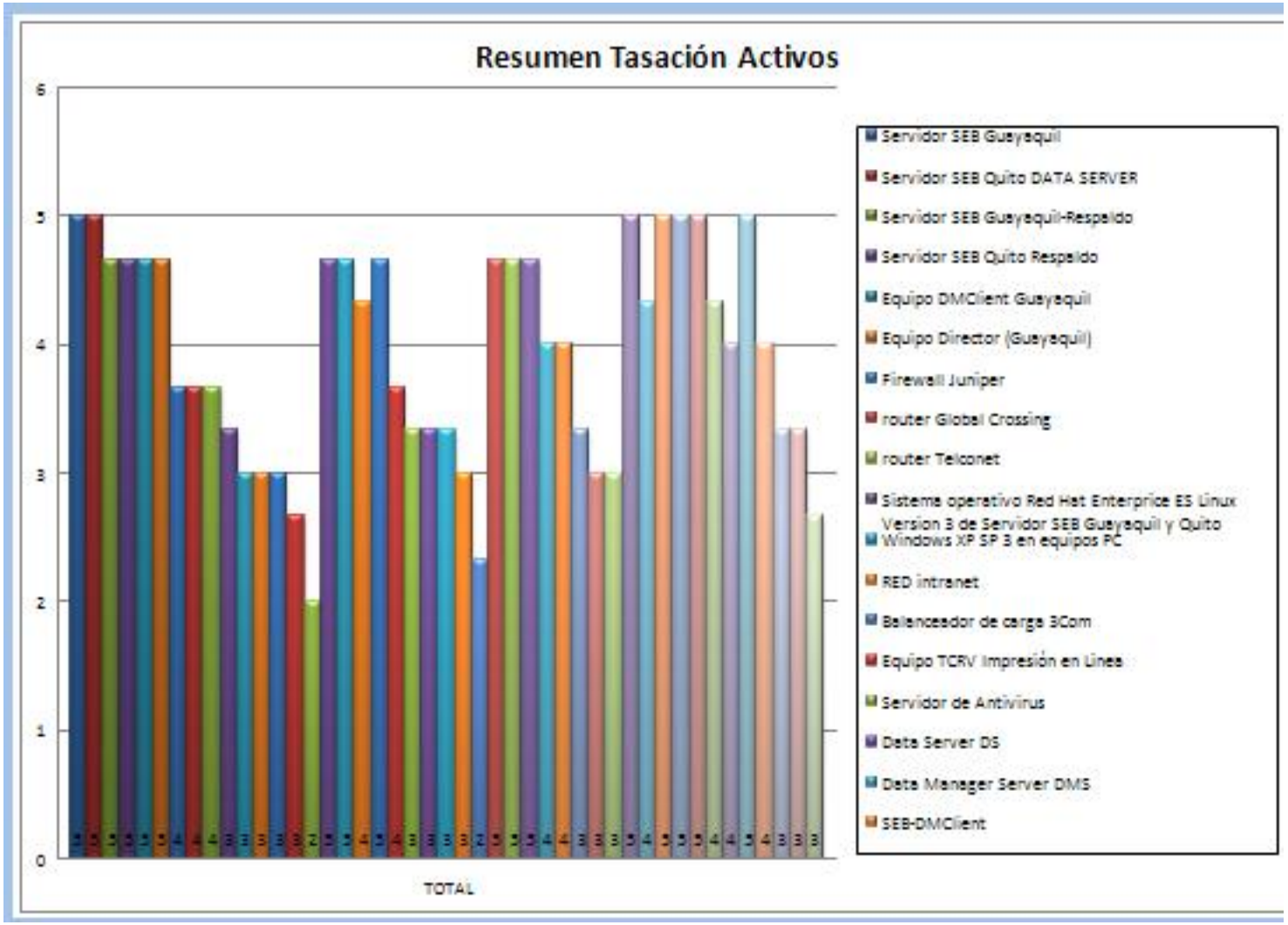

Recursos Humanos
Escala de Valoración
6
5
4
3
2
1
0
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
Sub-Director de Operaciones
Asistente de Operaciones
Operador de Casa de Valores
Director de Operaciones
Director de Sistemas
Jefe de Soporte Técnico REDEVAL
Técnico de REDEVAL en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


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

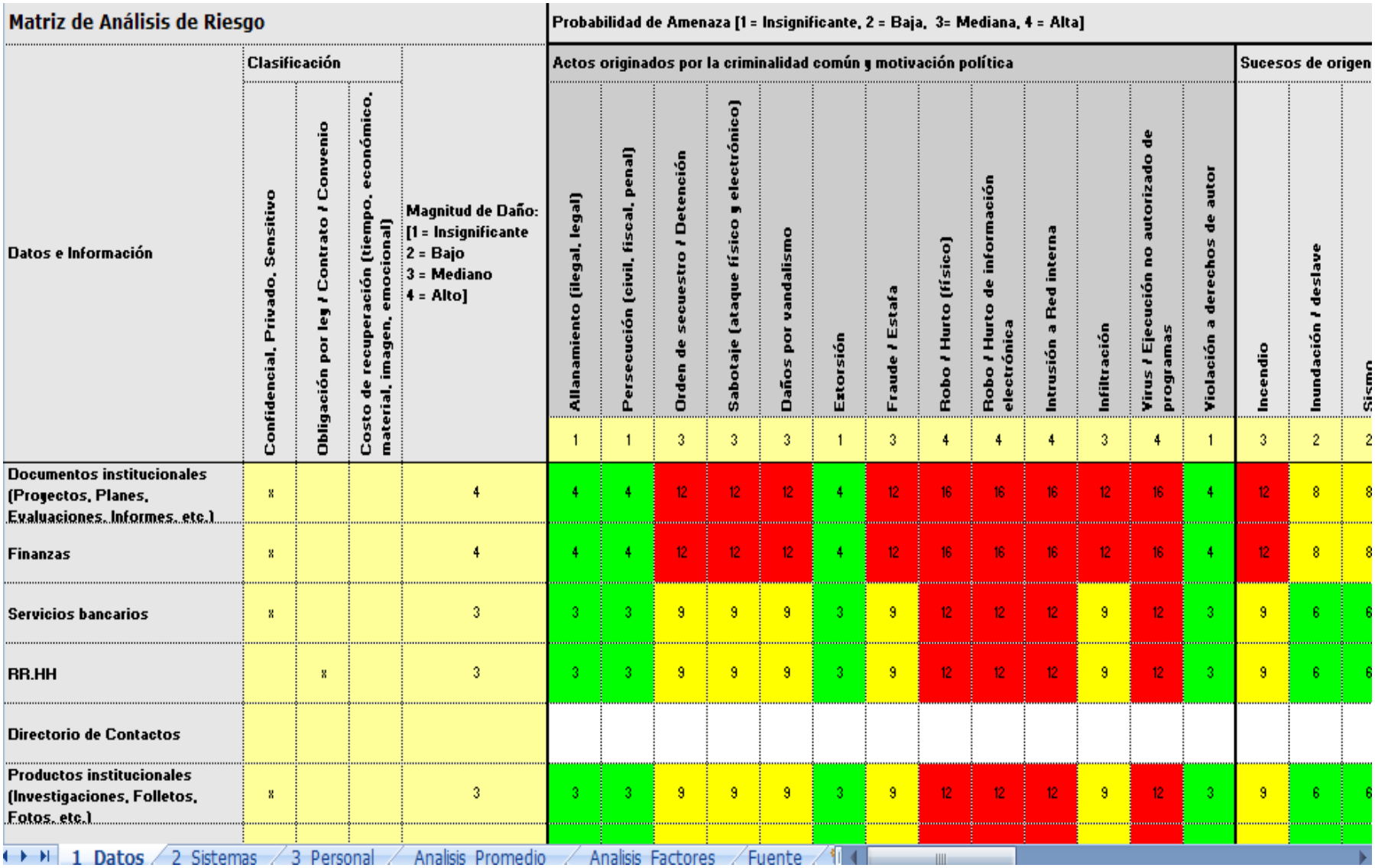

Información (Datos)
Escla de Valoración
6
5
4
3
2
1
0
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
INFORMACIÓN DE POSTURAS DE OFERTAS
INFORMACIÓN DE RUEDAS
INFORMACION DE POSTURAS DE DEMANDAS
PRECIOS Y CANTIDADES DE LAS OPERACIONES
INFORMACIÓN DE EMISORES DE TITULOS
INFORMACION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


Documentacion
Escala de Valoración
6
5
4
3
2
1
0
CONFIDENCIALIDAD
INTEGRIDAD
DISPONIBILIDAD
Dimensiones de Valoración
REPORTES DE LIQUIDACIONES
AUTORIZACIONES PARACREAR 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 DMClient Guayaquil
Equipo Director (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 Impresión en Linea
Servidor de Antivirus
Data Server DS
Data Manager Server DMS
SEB-DMClient

MATRIZ ANÁLISIS DE RIESGO

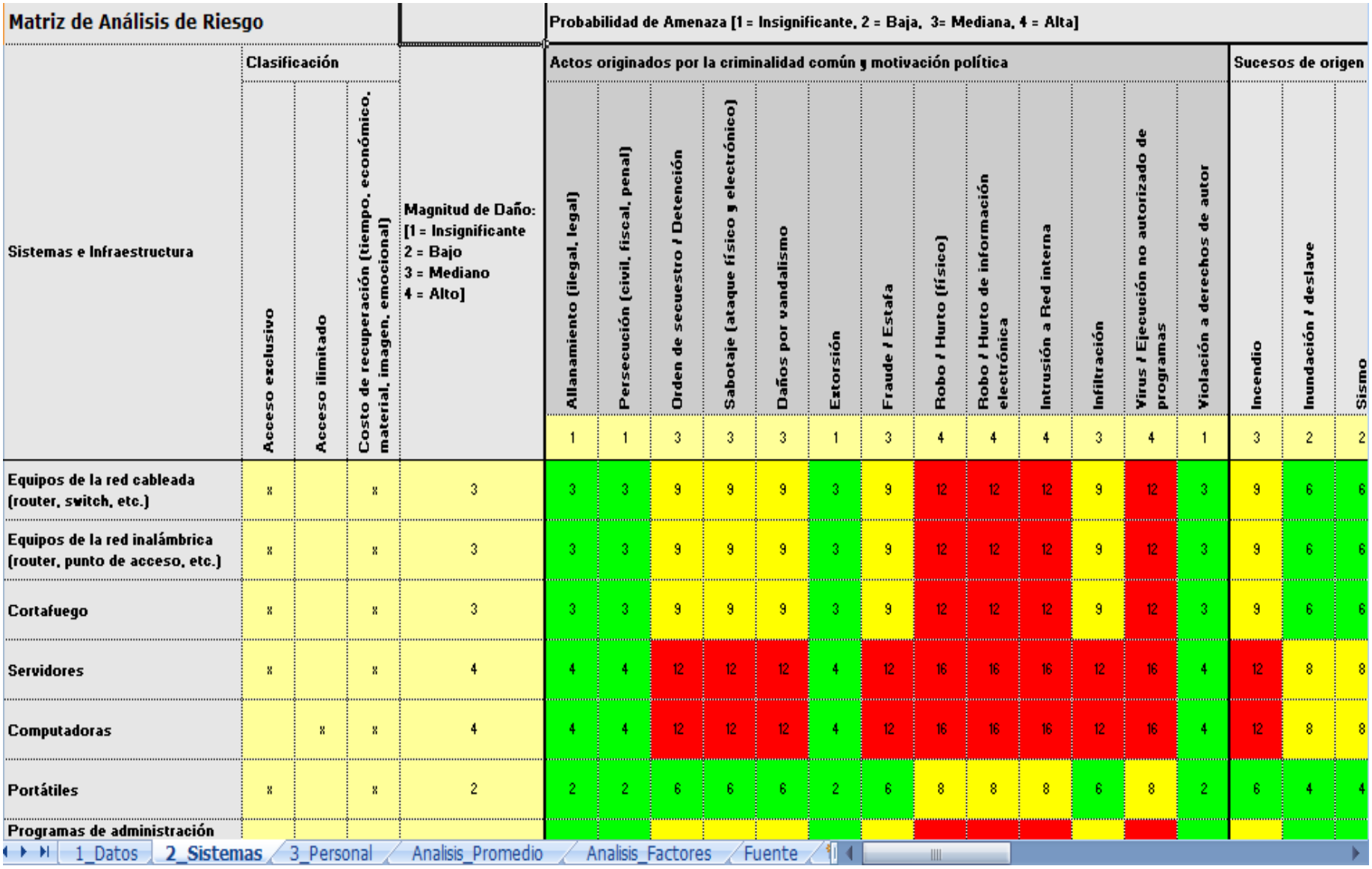


Matriz de Análisis de Riesgo

Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]

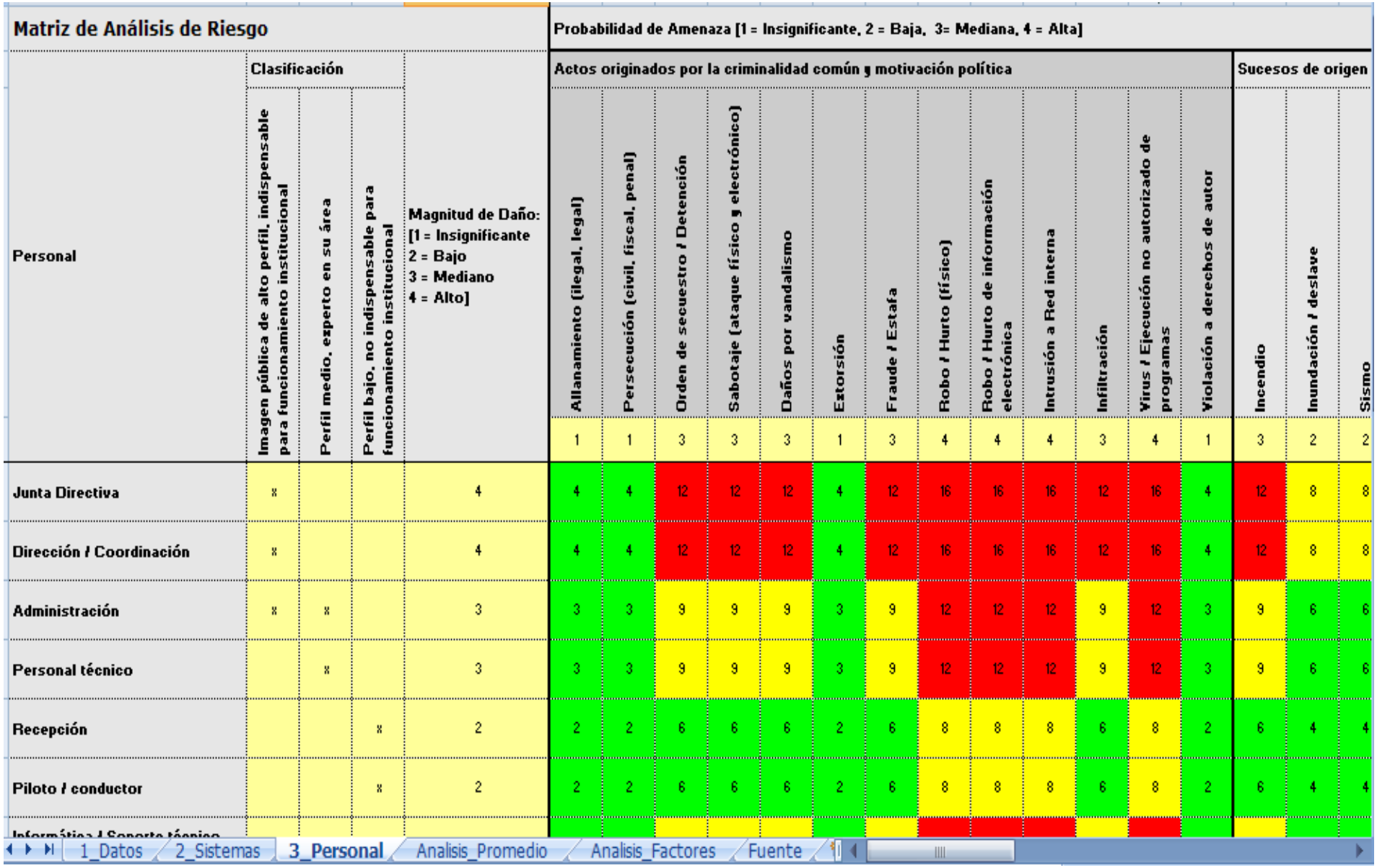
Datos e Información	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política													Sucesos de origen		
	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)		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 electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	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)	Orden 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 autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo
					1	1	3	3	3	1	3	4	4	4	3	4	1	3	2	2
Equipos de la red cableada (router, switch, etc.)	x		x	3	3	3	9	9	9	3	9	12	12	12	9	12	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	12	9	12	3	9	6	6
Cortafuego	x		x	3	3	3	9	9	9	3	9	12	12	12	9	12	3	9	6	6
Servidores	x		x	4	4	4	12	12	12	4	12	16	16	16	12	16	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	6	6	6	2	6	8	8	8	6	8	2	6	4	4
Programas de administración																				

1_Datos | 2_Sistemas | 3_Personal | Analisis_Promedio | Analisis_Factores | Fuente

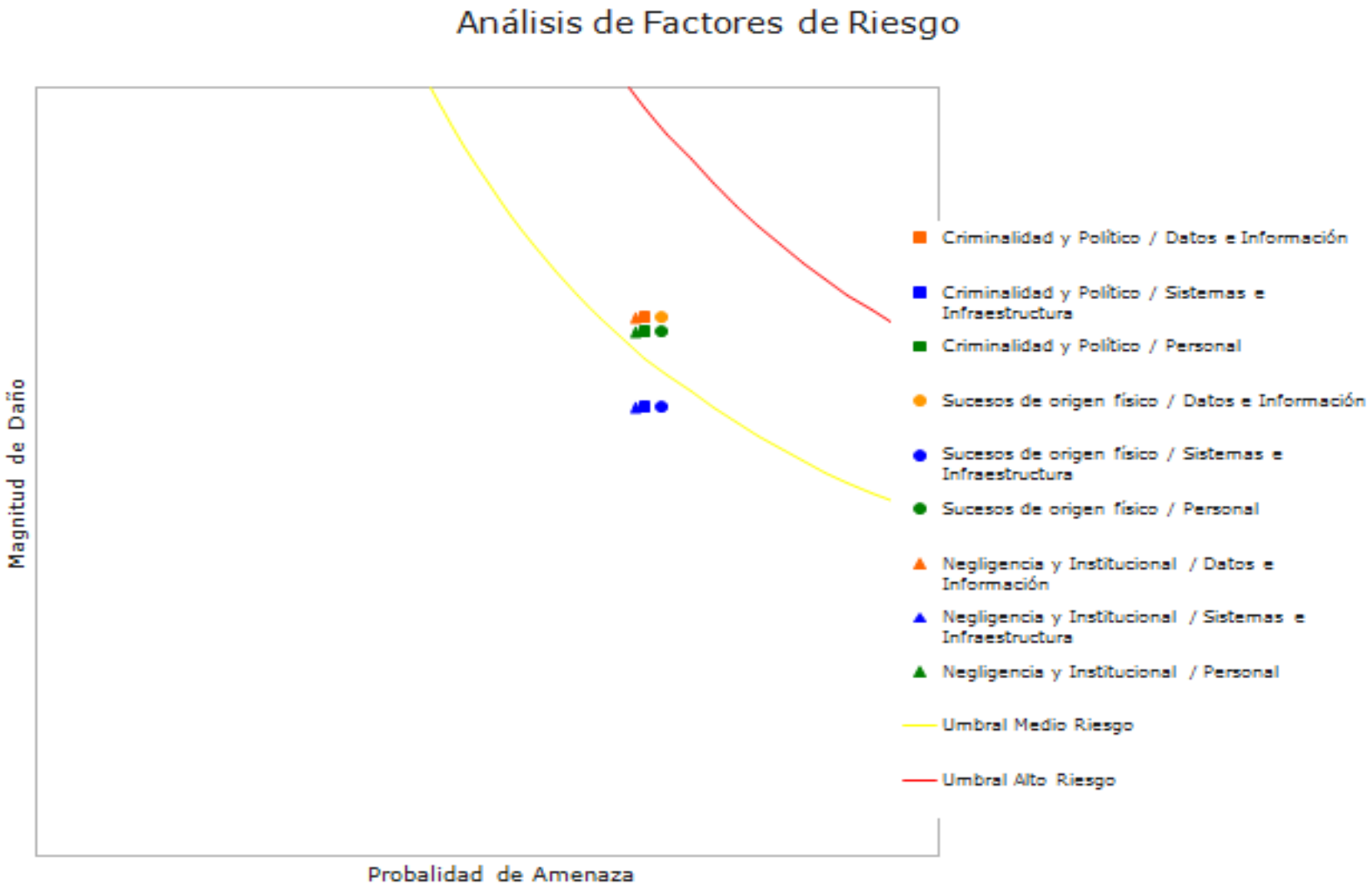


Matriz de Análisis de Riesgo					Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]														
Personal	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Actos originados por la criminalidad común y motivación política													Sucesos de origen		
	Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional		Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden 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 autorizado de programas	Violación a derechos de autor	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
Informática / 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
Magnitud de Daño
Probalidad de Amenaza
Criminalidad y Político / Datos e Información
Criminalidad y Político / Sistemas e Infraestructura
Criminalidad y Político / Personal
Sucesos de origen físico / Datos e Información
Sucesos de origen físico / Sistemas e Infraestructura
Sucesos de origen físico / Personal
Negligencia y Institucional / Datos e Información
Negligencia y Institucional / Sistemas e Infraestructura
Negligencia y Institucional / Personal
Umbral Medio Riesgo
Umbral Alto Riesgo

VALORACIÓN Y MAPEO DE RIESGOS

VALORACIÓN Y MAPEO DE RIESGOS

Mapa de Riesgo

NOTA: Llenar solo las celdas que se encuentran sombreadas en color verde, las celdas restantes se encuentran bloqueadas para protección de las formulas que graficarán los riesgos.

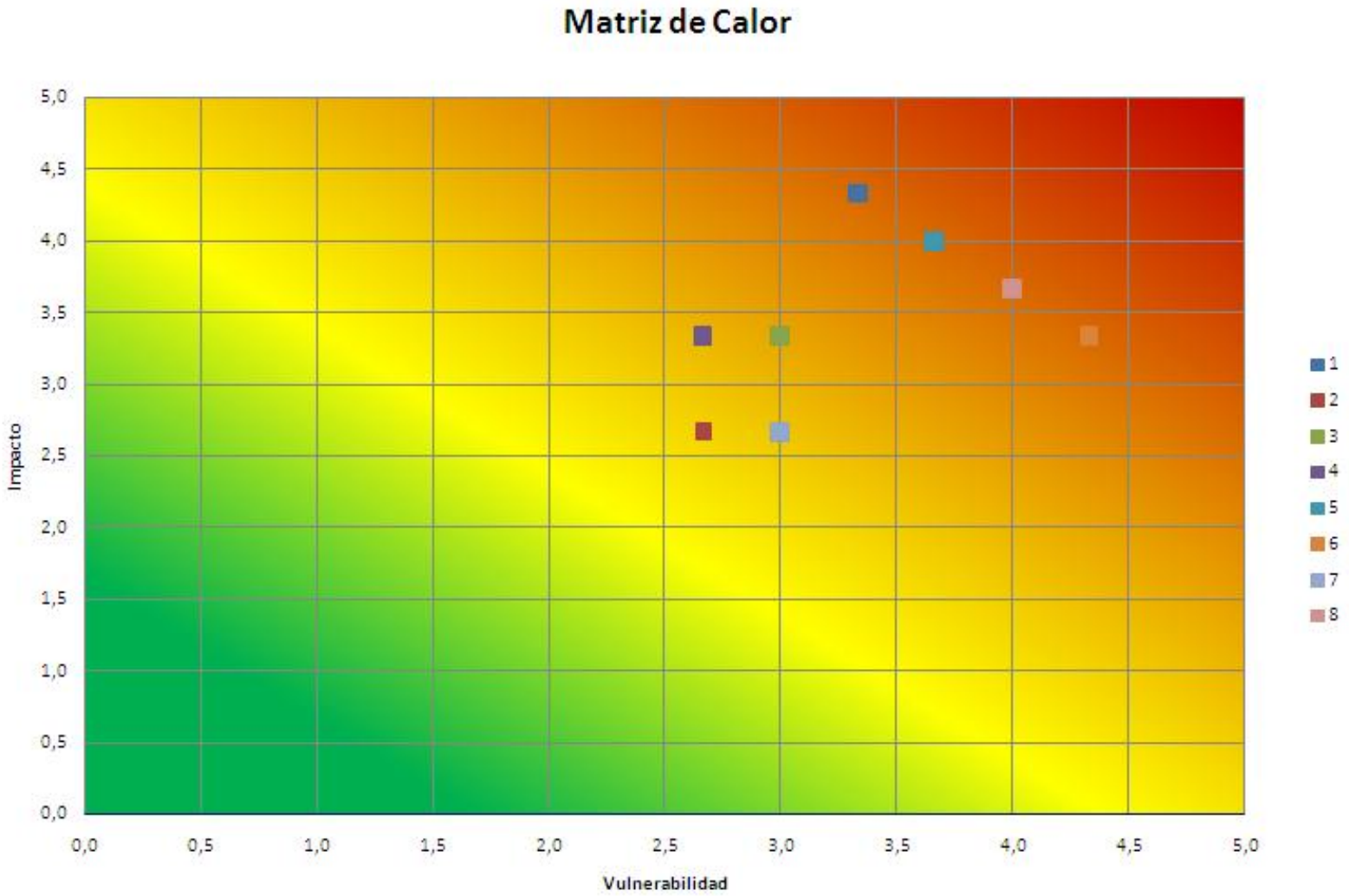
Vulnerabilidad: Nivel de exposición para que un riesgo se materialice, considerando la estructura de control actual Escala 1 al 5

Impacto: Posibilidad de que la magnitud del Riesgo afecte el cumplimiento de los objetivos

	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 Sugeridos para mitigar riesgos	Costo de aplicar los controles $ (Alto, Medio, Bajo)	Tratamiento al Riesgo
1	CONTROL DE ACCESO	SISTEMAS	En la politica de creacion de usuarios no se incluye el formato de la clave y se constato que los usuarios pueden utilizar los caracteres que les parezca	Alto	3,3	4,3	VOTO IMPACTO	4,0	4,0	5,0	Revisar y Documentar una Especificación o Politica 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 esta definida en un manual documentado y se le hace llegar a los usuarios por e-mail	Medio	2,7	2,7	VOTO IMPACTO	2,0	2,0	4,0	Implementar un procedimiento para entrega de claves seguras mediante herramientas que protejan las mismas	MEDIO	MITIGAR
							VOTO VULNERABILIDAD	2,0	2,0	4,0			
3	REGISTRO DE POSTURAS Y CIERRE DE NEGOCIACION	OPERDORES DE CASA DE VALORES	Por la presura de cerrar una negociación comenten errores al ingresar datos y si son nuevos no se percatan de los errores hasta que la operación pasa a otro estado	Medio	3,0	3,3	VOTO IMPACTO	2,0	4,0	4,0	Implementar el regsitro 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 politicas para control de acceso	Medio	2,7	3,3	VOTO IMPACTO	2,0	5,0	3,0	Implementar un procesos de difusion de las politicas y verificar que todos los miembrosd de TI conocen y entienden las politicas	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 sistematico del levantamiento de requerimientos, aunque existen los formatos y procedimientos para el efecto, muchas veces se los pasa por alto	Alto	3,7	4,0	VOTO IMPACTO	4,0	4,0	4,0	Implementar un procedimiento documentado para el control de cambios que incluya un plan general de pruebas, pasos para levantar un laboratorio de pruebas, verificacion de cumplimientos de requerimientos, cierre de etapa	BAJO	MITIGAR
							VOTO VULNERABILIDAD	3,0	4,0	4,0			
6		DIRECCION DE SISTEMAS Y OPERACIONES	La persona que cumple las funciones de Jefe de Soporte de REDEVAL es la unica 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	VOTO IMPACTO	2,0	4,0	4,0	Implementar un plan de entrenamiento constante del personal de TI para que conozcan los procedimientos y documentación que esta relacionada al SEB	BAJO	MITIGAR
							VOTO VULNERABILIDAD	4,0	4,0	5,0			
7		SISTEMAS	No se constato un documento que explique que metodologia reconocida se utiliza para el desarrollo de aplicaciones ni para la verificacion de software adquirido	Medio	3,0	2,7	VOTO IMPACTO	2,0	2,0	4,0	Realizar pruebas periodicas de simulaciones de caidas 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	MITIGAR
							VOTO VULNERABILIDAD	2,0	3,0	4,0			
8	CIERRE DE LA OPERACIÓN	SISTEMAS	La metodología utilizada por el proveedor tecnologico en el desarrollo no garantiza que se se esta cumpliendo con los requisitos de seguridad de información manejada en el SEB	Alto	4,0	3,7	VOTO IMPACTO	3,0	4,0	4,0	Considerar la norma ISO 15408 como base para generar un procedimiento de evaluación del software adquiridp o desarrollado	BAJO	MITIGAR
							VOTO VULNERABILIDAD	4,0	4,0	4,0			

JULIA MACIAS TULCAN
MAYRA BENAVIDES RODRIGUEZ


Matriz de Calor
Impacto
Vulnerabilidad
5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0,0
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.

Factores a considerar al seleccionar los controles

- 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 Auditoría 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 auditoría 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 Auditoría realizada por la Escuela Superior Politécnica del Litoral a los Sistemas SEB, SIBE y AT
- Metodología 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