ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DESARROLLO DE UN PLAN DE CONTINUIDAD DEL NEGOCIO DE TI PARA EL ISP "MEGADATOS S.A." DE LA CIUDAD DE QUITO

PROYECTO PREVIO A LA OBTENCIÓN DE TITULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

TIXI CALI GLENDA SORAYA
glenda_tixi@hotmail.com

DIRECTOR: MSC. ING. GUSTAVO SAMANIEGO
gustavo.samaniego@epn.edu.ec

Quito, Agosto 2013

DECLARACIÓN

Yo, Glenda Soraya Tixi Cali, declaro bajo juramento que el trabajo descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mi derecho de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

_____

Glenda Tixi

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Glenda Soraya Tixi Cali, bajo mi supervisión.

_____

Ing. Gustavo Samaniego

DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco ante todo primero a Dios por permitirme que me ponga de pies de todos los días, por siempre estar a mi lado guiándome en cada paso que doy durante el transcurso de mi vida.

A mis padres, Luis y Blanca, por haberme dado la vida, por su dedicación, su infinito amor y su apoyo incondicional, por cada uno de sus consejos, por siempre estar pendientes de todo lo que me hace falta y por de una u otra forma estar siempre a mmi lado.

A mis hermanos Mireya, David y Daniela quienes siempre me apoyan y están con migo en los buenos y malos momentos.

A mi tutor de tesis, Ing. Gustavo Samaniego por brindarme su apoyo y ayudarme a culminar este proyecto.

A mi esposo Rodrigo, por caminar a mi lado y estar incondicionalmente en los días difíciles y en también en los buenos.

A mis amig@s, los cuales son mi segunda familia, los mismos que me ayudan y me brindan su amistad incondicional todos los días.

Finalmente te todos y cada una de las personas que de una u otra forma me ayudaron y me apoyaron para que pueda culminar uno más de mis proyectos.

Glenda Soraya

DEDICATORIA

Dedico este proyecto a mis padres Luis y Blanca por todo el esfuerzo y dedicación que han tenido hacia mí y por brindarme su apoyo incondicional todos los días de mi vida

A mi hijo Mateo, el cual es la mayor bendición que Dios me pudo dar y es el sol que ilumina todos mis días.

Glenda Soraya

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Desarrollar un plan de continuidad de negocio es muy importante para la cualquier tipo de organización ya que nos ayudará a tener las previsiones necesarias para que la empresa siga funcionando en caso de presentarse alguna irrupción.

En el capítulo 1 se realiza una descripción a la empresa, así como un inventario de los activos con los que cuenta la empresa, la descripción de las diferentes áreas y procesos que se tienen dentro de la misma.

En el capítulo 2 se realiza un análisis de riesgos, donde se describen los posibles riesgos que se puede tener dentro de la empresa y se realiza el análisis respectivo de cada uno de ellos, también se realiza el análisis de impacto del negocio el cual nos permite establecer los procesos críticos y conocer cuáles son los requerimientos mínimos para volver a la normalidad en caso de que ocurra alguna disrupción en cualquiera de las operaciones de la empresa.

En el capítulo 3 se realiza el desarrollo del Plan de Continuidad del negocio, dentro de este se va realizar una pequeña introducción sobre la norma BS25999 y algunas definiciones del BCP, luego de esto se procederá a describir las diferentes fases que del BCP: Inicio y Gestión del Proyecto, Evaluación y Gestión de Riesgos, Análisis de Impacto del Negocio (BIA), Desarrollo de Estrategias para la Continuidad del Negocio, Respuestas ante Emergencias, Cronograma de implantación del BCP.

En el capítulo 4 se realiza una evaluación de la aplicabilidad del BCP en tres aspectos. En el aspecto económico, mediante el cual se conocerá el valor de la inversión que se requiere para la implementación del BCP. En el aspecto legal, el cual dará a conocer si el desarrollo del plan infringe alguna ley vigente en el país. Finalmente en el aspecto organizacional, el cual dará a conocer si dentro de la empresa existe el personal necesario para la implementación del BCP o si se necesitara personal extra para dicha implementación.

Finalmente en el capítulo 5 se dan a conocer las conclusiones y recomendaciones que se obtuvieron una vez finalizado el proyecto.

1 SITUACIÓN ACTUAL DE LA EMPRESA MEGADATOS S.A.

1.1 GENERALIDADES DE LA EMPRESA

En el presente capitulo se realiza una breve descripción de la empresa MEGADATOS S.A., misma que cuanta con una misión, visión, valores, políticas, etc., que se las da a conocer. Se procederá a realizar conjuntamente el inventario de los diferentes activos (hardware, software, RR.HH., etc.) existentes en la empresa, así como la descripción de las áreas y procesos con los que se cuenta dentro de la misma.

1.1.1 HISTORIA

MEGADATOS S.A. es una empresa que nace en 1991 como una fundación sin fines de lucro en la Ciudad de Quito, sus inicios fueron como ACCESS INTERNET con razón social MEGADATOS S.A. con el objetivo de brindar Servicios de Internet a la comunidad, por el año de 1999 se empiezan a evaluar algunas opciones de compra/venta pensando siempre en el crecimiento de la empresa, para lograr este objetivo, en septiembre de 2002 se adquiere la empresa RAMTELECOM Telecomunicaciones S.A. convirtiéndose en ACCESSRAM, para esta fecha ya se tenía una sucursal de MEGADATOS en la ciudad de Guayaquil.

Para el 2004 se inicia una fusión con la empresa MEGADATOS S.A., cuyo objetivo era ganar mercado a nivel nacional, especialmente en la Ciudad de Guayaquil, cuya sucursal no contaba con la acogida esperada, convirtiéndose así en MEGADATOS S.A. pero siempre manteniendo la razón social MEGADATOS S.A.

Finalmente para el año 2009 se realiza una alianza estratégica con la empresa TELCONET S.A. cuya finalidad era la de poder compartir la infraestructura robusta que posee dicha empresa, adicional también estaba el hecho de poder compartir el recurso humano entre las dos empresas.

1.1.2 MISIÓN

"Mejorar la calidad de vida de nuestros clientes facilitándoles el acceso a la información, por medio de la provisión de servicios digitales integrados, apoyados en una constante innovación tecnológica y un recurso humano altamente calificado y motivado, contribuyendo así con el desarrollo de la Sociedad de la información en el país".[1]

1.1.3 VISIÓN

"Ser la organización líder en innovación tecnológica, facilitadora del acceso a la información y conocimiento, a través de la provisión de soluciones digitales integradas, producto de la calidad, excelencia y compromiso de su gente, fomentando las relaciones a largo plazo con nuestros clientes". [2]

1.1.4 VALORES

Los valores que se tiene dentro de la empresa MEGADATOS S.A. son:

- Espíritu de Servicio
- Pasión
- Disciplina
- Integridad
- Conciencia empresarial. [3]

1.1.5 POLÍTICA DE CALIDAD

"Asesorar y proporcionar soluciones integrales en telecomunicaciones e Internet; con un permanente mejoramiento de servicios, apoyados por un equipo humano especializado, íntegro y creativo, que hace posible la satisfacción de los clientes".[4]

[1] Fuente: www.ecuanet.com
[2] Fuente: www.ecuanet.com
[3] Fuente: www.ecuanet.com

1.1.6 ESTRUCTURA DE MEGADATOS S.A.

La empresa MEGADATOS S.A. se encuentra estructurada en cinco niveles, los mismos que son:

- Alta dirección
- Nivel directivo
- Nivel ejecutivo
- Nivel ejecutor
- Nivel operativo

Todos y cada uno de los empleados que laboran en MEGADATOS S.A. pertenecen a un nivel específico, esto dependerá de las diferentes funciones y actividades que cada empleado desempeñe dentro de la empresa.

En la figura 1.1 se muestra la estructura de la misma

[4] Fuente: www.ecuanet.com

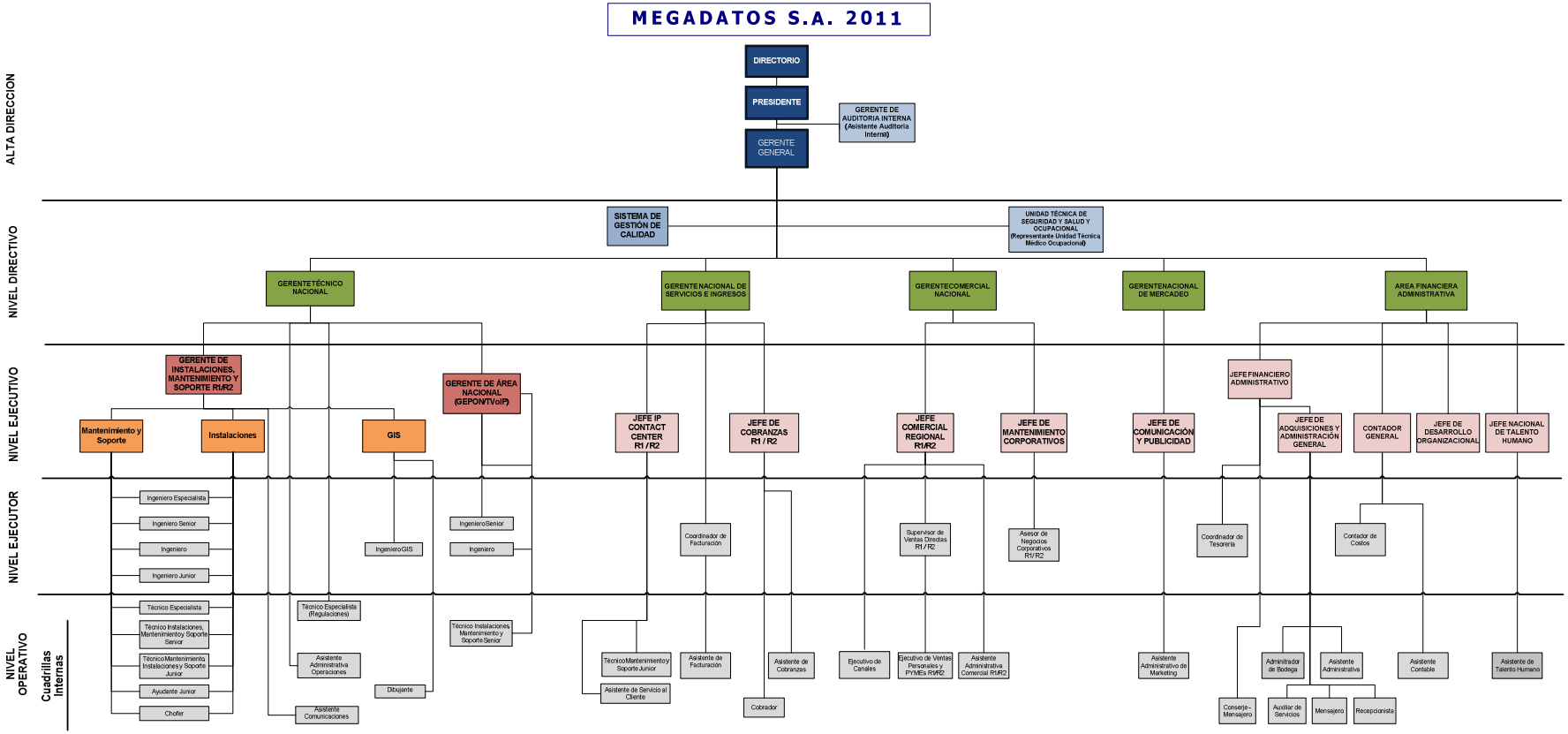


Figura 1.1: Estructura de MEGADATOS S.A

1.1.7 SERVICIOS QUE BRINDA LA EMPRESA

MEGADATOS S.A. pensando en las diferentes necesidades que tienen hoy en día todas y cada una de las familias, y acorde con el crecimiento tecnológico que día a día se incrementa más y más, ha pensado en proveer servicios exclusivamente para el sector hogar.

El producto que comercializa la empresa se llama "NETLIFE". NETLIFE es el primer Internet FTTH (fiber to the home) del país, es el primer internet por fibra óptica. Nuestro producto posee un desempeño único en su categoría, posee una velocidad incomparable lo cual hace que la navegación sea una de las mejores experiencias que el usuario tendrá, todo esto se logra porque el Internet que distribuye la empresa es mediante Fibra Óptica y la compartición que se da, es la menor compartición del mercado.

El FTTH es una nueva tecnología que se basa en la utilización de cables de fibra óptica y que utiliza ases de luz como medio de transmisión de datos y comunicación a gran distancia. La fibra óptica no se destruye ni se deteriora, lo cual permite tener una conexión de calidad.

NETLIFE, es el único servicio que ofrece a los usuarios 5 veces más velocidad en contenido local, para que los clientes puedan disfrutar al máximo y puedan optimizar su tiempo.

BENEFICIOS DE USAR NETLIFE

NETLIFE ofrece los siguientes beneficios:

- La mayor velocidad nunca antes vista en el país, Fibra Óptica directo hasta el hogar.
- La mejor tecnología en comunicaciones a nivel mundial.
- Velocidad simétrica (igual velocidad para subir o bajar archivos)

- 5 veces más velocidad a YouTube y contenido LOCAL.
- Estabilidad permanente y navegación total sin congestiones.
- En el caso de Edificios, la red interna de Fibra Óptica que se debe instalar es GRATIS.
- La menor compartición del mercado.
- Línea directa de comunicación a través del 1700NETLIFE 24 horas.
- Tarifas altamente competitivas.
- Posibilidad ilimitada de aplicaciones sobre la red.
- Horarios extendidos de instalación.

PLANES Y TARIFAS DEL SERVICIO NETLIFE

NETLIFE pensando en las diferentes necesidades de sus clientes ofrece algunas alternativas, las mismas que se acoplan al ritmo de vida de los diferentes tipos de usuario que se tiene.

PLANES HOME

Este tipo de plan es un servicio que aplica solo para planes de hogares, el servicio no está disponible para Cybers, el costo de la instalación incluye Wifi.

En la tabla 1.1 se indica los diferentes planes y costos de este tipo de plan.

Tabla 1.1: Planes Home NETLIFE

VELOCIDAD (Mbps)	COSTO	BENEFICIOS
5/5 Mbps local simétrico 1/1 Mbps Internacional simétrico	$ 30 más $50 de instalación	• 1 Cuenta de Correo • 1 IP Dinámica • Disponibilidad 99% • Compartición 2:1

Tabla 1.1: Planes Home NETLIFE (continuación)

VELOCIDAD (Mbps)	COSTO	BENEFICIOS
10/10 Mbps local simétrico 2/2 Mbps Internacional simétrico	$ 65 más $50 de instalación	• 1 Cuenta de Correo • 1 IP Dinámica • Disponibilidad 98% • Compartición 2:1
20/20 Mbps local simétrico 4/4 Mbps Internacional simétrico	$ 65 más $50 de instalación	• 1 Cuenta de Correo • 1 IP Dinámica • Disponibilidad 98% • Compartición 2:1
40/40 Mbps local simétrico 8/8 Mbps Internacional simétrico	$ 95 más $50 de instalación	• 1 Cuenta de Correo • 1 IP Dinámica • Disponibilidad 98% • Compartición 2:1
60/60 Mbps local simétrico 12/12 Mbps Internacional simétrico	$ 130 más $50 de instalación	• 1 Cuenta de Correo • 1 IP Dinámica • Disponibilidad 98% • Compartición 2:1

PLANES PROFESIONALES

Estos tipos de planes no están disponibles para Cybers, en este tipo de plan se configura el servicio que de NETLIFE máximo en 5 máquinas, el costo de la instalación incluye Wifi.

En la tabla 1.2 se describen los beneficios de este plan.

Tabla 1.2: Planes Profesionales de NETLIFE

VELOCIDAD (Mbps)	COSTO	BENEFICIOS
5/5 Mbps local simétrico 1/1 Mbps Internacional simétrico	$ 40 más $ 80 de instalación	• 1 Cuenta de Correo • 1 IP Fija • Disponibilidad 98% • Compartición 2:1 • Firewall en router • Switch de 4 puertos
10/10 Mbps local simétrico 2/2 Mbps Internacional simétrico	$ 60 más $ 80 de instalación	• 1 Cuenta de Correo • 1 IP Fija • Disponibilidad 98% • Compartición 2:1 • Firewall en router • Switch de 4 puertos
20/20 Mbps local simétrico 4/4 Mbps Internacional simétrico	$ 75 más $ 80 de instalación	• 1 Cuenta de Correo • 1 IP Fija • Disponibilidad 98% • Compartición 2:1 • Firewall en router • Switch de 4 puertos
40/40 Mbps local simétrico 8/8 Mbps Internacional simétrico	$ 105 más $ 80 de instalación	• 1 Cuenta de Correo Electrónico • 1 IP Fija • Disponibilidad 98% • Compartición 2:1 • Firewall en router • Switch de 4 puertos
60/60 Mbps local simétrico 12/12 Mbps Internacional simétrico	$ 140 más $ 80 de instalación	• 1 Cuenta de Correo • 1 IP Fija • Disponibilidad 98% • Compartición 2:1 • Firewall en router • Switch de 4 puertos

PLANES PYMES

Estos tipos de planes no están disponibles para Cybers, y se configura el servicio en máximo 5 máquinas, el costo de la instalación incluye WiFi.

En la tabla 1.3 se muestra los beneficios de este tipo de plan.

Tabla 1.3: Planes PYMES de NETLIFE

VELOCIDAD (Mbps)	COSTO	BENEFICIOS
10/10 Mbps local simétrico 2/2 Mbps Internacional simétrico	$ 100 más $ 100 de instalación	• 5 Cuentas de Correo • 1 IP Fija • Disponibilidad 98% • Compartición 2:1 • Puerto 25 habilitado • Firewall en router • Switch de 4 puertos • 5 cuantas AV/AS/FW
20/20 Mbps local simétrico 4/4 Mbps Internacional simétrico	$ 250 más $ 100 de instalación	• 5 Cuentas de Correo • 1 IP Fija • Disponibilidad 98% • Compartición 2:1 • Puerto 25 habilitado • Firewall en router • Switch de 4 puertos • 5 cuentas AV/AS/FW

1.2 INFRAESTRUCTURA DE LA EMPRESA

El presente proyecto de titulación va enfocado hacia la realización de un Plan de Continuidad de Negocio para la empresa MEGADATOS S.A. de la Ciudad de Quito, por lo cual se analizará solo la infraestructura de dicha ciudad.

1.2.1 DISEÑO DE LA RED DE MEGADATOS S.A.

MEGADATOS S.A. es una empresa que se encuentra ubicada en la Ciudad de Quito en la Avenida Atahualpa E3-13 y Núñez de Vela - Edificio Torre del Puente

La empresa MEGADATOS S.A. se encuentra operando en tres pisos dentro del edificio, el segundo piso donde se encuentran las Áreas de Marketing, Comercial, Recepción, Atención al Cliente, Cobranzas e IP Cotac Center, el tercer piso, donde se encuentran las Áreas de Gerencia General, el Áreas Administrativa, Recursos Humanos, el Dispensario Médico y el Áreas de Contabilidad, y en el octavo piso donde se encuentra el Área de Bodega y Operaciones dentro de la cual se encuentran los departamentos de Instalaciones, GEPON y Soporte, en este piso está ubicado el TELEPUERTO o Cuarto frio, que es donde se albergan los servidores y los equipos de redes y comunicación.

Los diferentes equipos que sirven para las conexiones dentro de la empresa se encuentran distribuidos en tres *racks,* dos *racks* que se encuentra en el segundo piso, en uno se encuentran las conexiones para los usuarios de segundo y tercer piso, y en el otro se encuentras las conexiones para el Área Comercial y Marketing. El otro *rack* se encuentra en el octavo piso en el TELEPUERTO, dentro de dicho *rack* se encuentra el switch principal, de éste salen las diferentes conexiones hacia todos y cada uno de los equipos que se tienen en la empresa como son los servidores, routers, equipos inalámbricos, estaciones de trabajo, etc.

En la figura 1.2 podemos observar el diagrama de la red interna de MEGADATOS S.A. y todos los equipos que forman parte de ella.

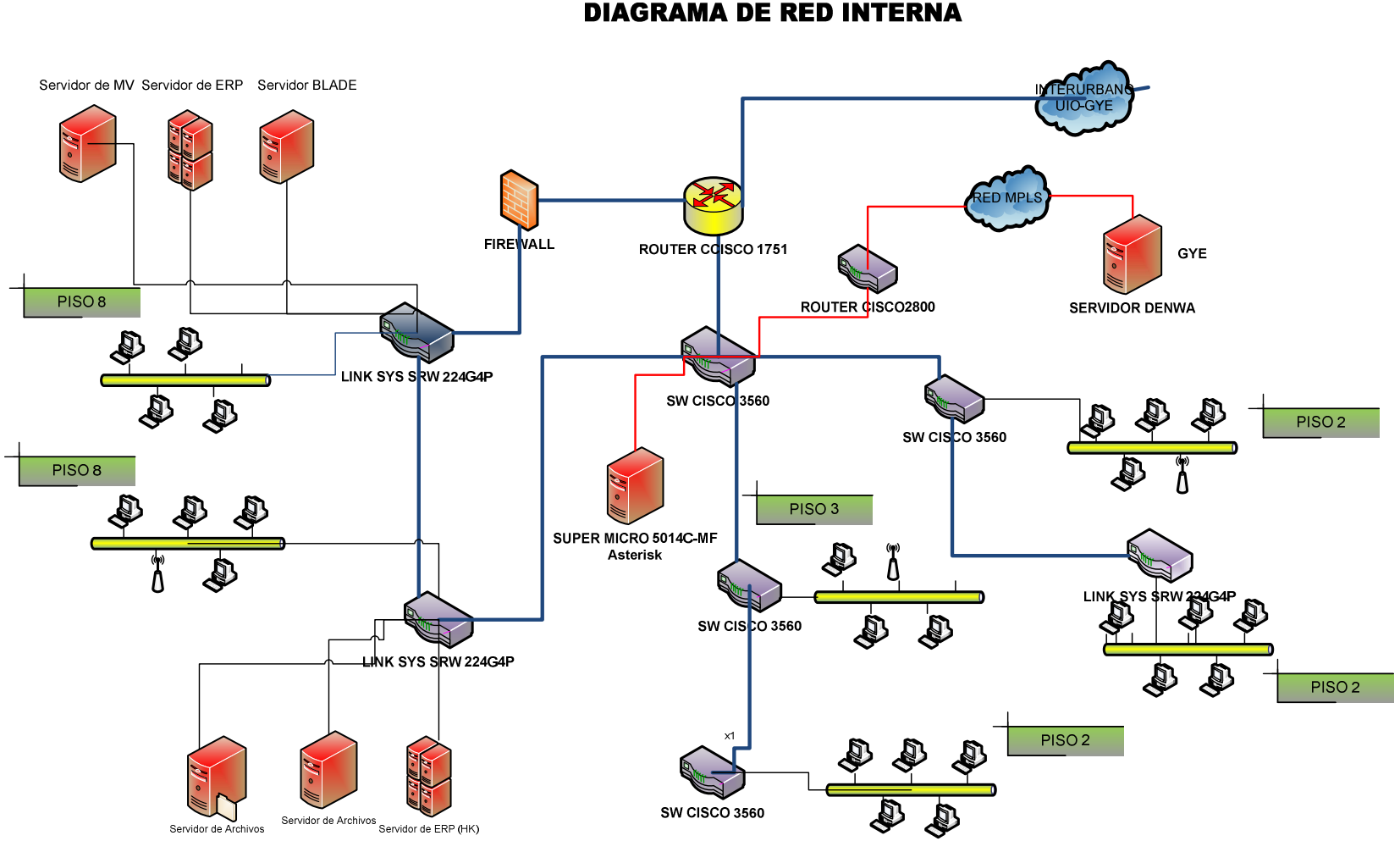


Figura 1.2: Diagrama de la Red de MEGADATOS S.A.

1.2.2 INVENTARIO DE ACTIVOS

Se realiza un estudio más detallado de todos los activos existentes en MEGADATOS S.A. Este inventario de Activos[5] nos servirá como punto de partida y será fundamental para conocer de manera muy precisa lo que se tiene dentro de la empresa y lo que se debe proteger.

A partir de este inventario de Activos se realizará un análisis riesgos a los que éstos activos se encuentran expuestos, así como también cuáles son las fallas de seguridad existentes para cada uno de estos.

1.2.2.1 Inventario de Recursos Humanos

MEGADATOS S.A. es una empresa en la cual trabajan aproximadamente 150 empleados en la ciudad de Quito, los mismos que se encuentran distribuidos en las diferentes áreas que se tiene.

En la tabla 1.4 se detalla el inventario de recurso humano de la empresa MEGADATOS S.A., en donde e indica el área, el cargo y el número de empleados para cada cargo.

Tabla 1.4: Inventario de Recurso Humano

ÁREA	NOMBRE DEL CARGO	# DE EMPLEADOS
Financiero-Administrativa	Analista De Desarrollo Organizacional	1
Comercial	Asistente Administrativa De Contratos	2
Operaciones	Asistente Administrativa Operaciones	1
Financiero-Administrativa	Asistente De Bodega	2
Comercial	Asistente Administrativo Comercial	1

[5] Activos: son todos los recursos de información o los relacionados con este que son necesarios para que la empresa funcione correctamente y alcance los objetivos planteados.

Tabla 1.4: Inventario de Recurso Humano (continuación)

ÁREA	NOMBRE DEL CARGO	# DE EMPLEADOS
Servicios y Aseguramiento de Ingresos	Asistente De Cobranzas	5
Operaciones	Asistente De Comunicaciones	3
Financiero-Administrativa	Asistente De Contabilidad	4
Financiero-Administrativa	Asistente De Control Financiero	1
Marketing	Asistente De Marketing	1
Servicios y Aseguramiento de Ingresos	Asistente De Servicio Al Cliente	5
Financiero-Administrativa	Asistente De Talento Humano	1
Servicios y Aseguramiento de Ingresos	Auxiliar De Cobranzas	1
Financiero-Administrativa	Auxiliar De Servicios Generales	1
Operaciones	Ayudante Jr.	1
Operaciones	Chofer	9
Operaciones	Conserje-Mensajero	2
Servicios y Aseguramiento de Ingresos	Cobrador - Mensajero	2
Operaciones	Coordinador De Instalaciones	1
Servicios y Aseguramiento de Ingresos	Contador De General	1
Operaciones	Coordinador GEPON	1
Servicios y Aseguramiento de Ingresos	Coordinador De Facturación	1
Comercial	Ejecutiva De Canales	1
Operaciones	Dibujante Jr.	1
Financiero-Administrativa	Coordinadora De Tesorería	1
Comercial	Ejecutivo De Ventas	49
Gerencia	Gerente General	1
Marketing	Gerente Nacional De Marketing	1

Tabla 1.4: Inventario de Recurso Humano (continuación)

ÁREA	NOMBRE DEL CARGO	# DE EMPLEADOS
Servicios y Aseguramiento de Ingresos	Gerente Nacional De Servicios De Aseguramiento De Ingresos	1
Operaciones	Gerente Nacional De GEPON	1
Operaciones	Ingeniero	2
Operaciones	Ingeniero Jr.	2
Servicios y Aseguramiento de Ingresos	Jefa De Cobranzas y Facturación	1
Financiero-Administrativa	Jefe De Administración y Finanzas	1
Financiero-Administrativa	Jefe De Adquisidores y Administración General	1
Marketing	Jefe De Comunicación y Publicidad	1
Servicios y Aseguramiento de Ingresos	Jefe De Contac Center R1	1
Comercial	Jefe De Ventas Directas	1
Financiero-Administrativa	Medico Ocupacional	1
Financiero-Administrativa	Jefe Nacional De Talento Humano	1
Operaciones	Programador Jr.	1
Financiero-Administrativa	Subgerente De Control Financiero	1
Financiero-Administrativa	Recepcionista	1
Servicios y Aseguramiento de Ingresos	Supervisor De IP Contac Center	1
Comercial	Supervisor De Ventas	2
Operaciones	Técnico De Instalaciones Jr.	1
Operaciones	Técnico De Mantenimiento Jr.	17
Operaciones	Técnico En Mantenimiento Sr.	5
Operaciones	Técnico En Instalaciones Sr.	1
Operaciones	Técnico De Instalaciones Jr.	1
Operaciones	Técnico Sr.	3
Operaciones	Técnico Jr.	1
TOTAL EMPLEADOS		**150**

1.2.2.2 Inventario Hardware

Se va a detallar cada uno de los equipos computacionales y de comunicación que forman parte de la infraestructura de MEGADATOS S.A., también se describirá las diferentes características y especificaciones que cada activo posee.

1.2.2.2.1 Servidores

Para ayudar la gestión de la empresa MEGADATOS S.A. posee algunos servidores, los mismos que ayudan a las actividades diarias, entre ellos están los servidores de archivos, de correo, servidor de ERP´s, etc.

Cabe recalcar que existen algunos servidores que no los administra el Departamento de Soporte de MEGADATOS S.A., pues están a cargo del Departamento de Sistemas de TELCONET, la empresa aliada, pero que físicamente se encuentran en el TELEPUERTO de MEGADATOS S.A., en estos servidores se encuentran las diferentes aplicaciones (ERP´s) las mismas que sirven de apoyo para llevar a cabo las diferentes actividades que se realizan día a día dentro de la empresa.

En la tabla 1.5 de indica el inventario de los servidores que tiene la empresa

Tabla 1.5: Inventario de Servidores

NOMBRE	MODELO	DESCRIPCIÓN	SW INSTALADO
Firewall	Clon	• SO Centos 5.0 • 1.5 GB de RAM • 100 GB de Disco Duro	• Mail • Scaner • Firewall • Mysql • Nagios • Squid • Ip tables • VPN • DHCP
Servidor de Archivos	HP ProLiant DL360	• SO Windows server 2003 Standard Edition SP2 • Intel Xeon, 3.6 GHz • 2 GB DE RAM • 140 GB de Disco Duro	• SK-NET Control de entradas • Fiel Magister 7.2
Servidor Máquinas Virtuales	Clon	• SO Windows Server 2003 Standard Edition SP2 • Intel Pentium 4, 3.0 GHz • 2 GB DE RAM • 240 GB de Disco Duro	• VMware

Tabla 1.5: Inventario de Servidores (continuación)

NOMBRE	MODELO	DESCRIPCIÓN	SW INSTALADO
Servidor de Diagramas de Red	HP ProLiant DL360	• SO Windows server 2003 Standard Edition SP2 • Intel Xeon 3.6 GHz • 2 GB DE RAM • 80 GB de Disco Duro	• Documentación de los enlaces de los diferentes clientes.
Servidor de HK	HP ProLiant DL38G5	• SO Red Hat 4.0 • Intel Xenon 1.86 GH,2 Procesadores • 2 G B de RAM • 250 GB de Disco Duro	• Oracle 10g Release 10.2.0.1.0 • Developer Suite 10g o Discovery Administrator o Discovery client
Servidor Blade	HP Blade System c3000	• SO Windows server 2003 R2 Standard Edition SP2 • Intel Xeon E5220 2,27 GHz • 20 GB DE RAM • 4TB en el CHASIS	• VMware vCenter Server • VMware vCenter • VMware vCenter Converter Client • VMware vSphere Client 4.0

Tabla 1.5: Inventario de Servidores (continuación)

NOMBRE	MODELO	DESCRIPCIÓN	SW INSTALADO
Servidor de correo	Virtualizado	• SO Windows server 2003 Standar Edition SP2 • Intel Xeon 3.6 GHz • 2 GB DE RAM • 220 GB de Disco Duro	• Exchange versión 6.5.7638.1 • Active Directory versión 5.2.3790.3959
Servidor de Antivirus	Virtualizado	• SO Win XP Profesional SP3 • Intel Xeon • 2GB RAM • 40 GB de Disco Duro	• Kaspersky Administration Kid
Servidor de WF	Virtualizado	• SO Win Server Enterprice 2008 SP 2 • Intel Xeon 5520 2,27 GHz • 8GB RAM • 140 GB de Disco Duro	• Lotus domino Server 8.0 • ODBS Oracle Client
Servidor de Gestión de Calidad	Virtualizado	• SO Windows server 2003 Standar Edition SP2 • Intel Xeon E5220 2,27 GHz • 2GB RAM • 180 de Disco Duro	• Documentación de la Página de Calidad.

Tabla 1.5: Inventario de Servidores (continuación)

NOMBRE	MODELO	DESCRIPCIÓN	SW INSTALADO
Servidor de Monitoreo TN	Virtualizado	• SO Win XP Profesional SP3 • Intel Xeon • 2GB RAM • 10 GB de Disco Duro	• ERP
Servidor de Monitoreo TN 2	Virtualizado	• SO Win XP Profesional SP3 • Intel Xeon E5520 2.13 GHz • 1.5GB de RAM • 10 GB de Disco Duro	• ERP
Servidor de SIT	Clon	• SO Red Hat 4.0 • 2.5 GB de RAM 500 GB de Disco Duro	• ERP

1.2.2.2.2 Switches

En la tabla 1.6 se va a describir los diferentes switches que se manejan en la empresa.

Tabla 1.6: Inventario de Switches

MODELO	CANTIDAD	DESCRIPCIÓN
CISCO WS-C3560-24TS	1	• Versión IOS: 12.2 • 118784/12280 Kb de memoria • 2 Interfaces Ethernet virtuales • 2 Interfaces Gigabit Ethernet • 24 Interfaces Fast Ethernet
CISCO WS-C3560-48	1	• Versión IOS: 12.2 • 21013 Kb de memoria • 2 Interfaces Ethernet virtuales • 2 Interfaces Gigabit Ethernet • 48 Interfaces Fast Ethernet/IEEE 802.3
CISCO WS-C2950-24	2	• Versión IOS: 12.1 • 21013 Kb de memoria • 24 Interfaces Fast Ethernet/IEEE 802.3
CISCO WS-C2950-48	1	• Versión IOS: 12.1 • 20957 Kb de memoria • 24 Interfaces Fast Ethernet/IEEE 802.3
LINK SYS SRW224G4P	3	• Boot Version 1.0.1 • Firmware Version 1.0.2 • 24 10/100 ports and • 4 gigabit ports with PoE switch

1.2.2.2.3 Router

En la tabla 1.7 se indica las características del router con el que cuenta la empresa.

Tabla 1.7: Inventario de Router

MODELO	CANTIDAD	DESCRIPCIÓN
CISCO 1811	1	• Versión IOS: 12.4 • 118784/12288 Kb de memoria • 10 Interfaces Fast Ethernet • 1 Interface Serial • 1 Terminal line

1.2.2.2.4 Equipos Inalámbricos

Los equipos inalámbricos que se tiene en la empresa se encuentran distribuidos en los 3 pisos del edificio.

A continuación en la tabla 1.8 se indican los diferentes equipos inalámbricos que se manejan.

Tabla 1.8: Inventario de Equipos Inalámbricos

MODELO	CANTIDAD
TELION HN-4404 AP	1
ETRENDNETTEW-651BR	1
LINKSYS EA4500	3

1.2.2.2.5 Estaciones de Trabajo

MEGADATOS S.A. cuenta con 150 empleados en la ciudad de Quito, no todos los empleados tienen su estación de trabajo existe personal que comparte su estación y algunos definitivamente no la tienen.

En la tabla 1.9 se detalla las características de las estaciones de trabajo de los empleados de MEGADATTOS S.A.

Tabla 1.9: Inventario de Estaciones de Trabajo

TIPO	CANTIDAD	DETALLES
LAPTOPS	56	• 45 con SO Windows 7 • 11 con SO Windows XP
PC´s	34	• 7 con SO Windows 7 • 27 con SO Windows XP

1.2.2.2.6 Equipo Informático Computacional Secundario

Dentro del equipo informático computacional secundario se encuentran todos los equipos que ayudan al desarrollo de las diferentes actividades que se llevan a cabo en la empresa como son: impresoras, escáneres, faxes, proyectores, entre otros;que son equipos que ayudan a la gestión de la empresa pero que no son tan necesarios para la prestación de servicios de la misma.

La mayoría de las impresoras se encuentran conectadas en red y los usuarios tienen acceso a las mismas de acuerdo al piso en el que se encuentran, y su configuración es para cada uno de los usuarios, mismos que cuentan con una clave personal de manera que se pueda realizar una auditoria personal.

A continuación en la tabla 1.10, se describe el equipo informático secundario.

Tabla 1.10: Inventario de Equipo Informático Secundario

TIPO	MARCA	MODELO	CANTIDAD
Impresoras	XEROX	PE 120i	1
		PHASER 3635 MFP	3
	HP	Laser Jet 4000	1
		Laser jet 4250n	1
		Hp laser Jet 4100-4200	1
	LEXMARK	8300 Series	1
		x2630	1
		X734de	1
	EPSON	Epson lx300	1
		Epson lx300	1
		Epson fx-890	1
		Epson fx890	1
Proyectores	EPSON	POWER LITE 510+	1
Faxes	PANASONIC	Panasonic KXFP101	1
TELÉFONOS IP	Grand Stream	BT200	44
		GXP 280	12
		GXP 2000	22
		GXP 2200	4

1.2.2.3 Inventario de Software

Se describirá el Software con el que se cuenta en la empresa, el mismo que ayuda para llevar a cabo las actividades diarias dentro de la misma

Se va a dividir al Software en dos grupos: Software Base y Software de Aplicación.

1.2.2.3.1 Inventario de SW Base

MEGADATOS S.A. posee un contrato de licenciamiento con Microsoft, en este contrato se establece que la empresa podrá tener las últimas versiones de todos los productos adquiridos hasta la fecha de finalización de dicho contrato.

A continuación en la tabla 1.11 se indica el Software base con el que cuenta la empresa, cabe recalcar que este Software se instala dependiendo del área al que pertenece cada usuario.

Tabla 1.11: Inventario de Software Base

NOMBRE	VERSIONES QUE SE USAN
Sistema Operativo	• Windows XP • Windows 7 • Windows Server 2003 • Windows Server 2008
Herramientas	• SQL Server Enterprice Edicion • Oracle 10g Release 10.2.0.1.0 • Kaspersky Antivirus
Office	• 2003 • 2007 • 2010
AutoCAD	• 2011 • 2012

1.2.2.3.2 Inventario de Software de Aplicación

MEGADATOS S.A. posee algunas aplicaciones internas que sirven de apoyo para la gestión de la empresa, las mismas que se han desarrollado internamente y de acuerdo a las diferentes necesidades que se tiene.

Como se mencionó anteriormente todas estas aplicaciones son administradas y desarrolladas por el Departamento de Sistemas de la empresa aliada TELCONET.

Las aplicaciones internas que se manejan se describen en la tabla 1.12

Tabla 1.12: Inventario de SW de Aplicación

SIGLAS	NOMBRE	FUNCIÓN	SOPORTE	LENGUAJE	PLATAFORMA
WF	Work FLow	Sistema de Manejo de flujo de trabajo	Departamento de Sistemas TN	• Lotus scrip • Lotus Formula • Java Scrip • Html • Xml	• SO Win Server Enterprice 2008 SP 2 • Lotus domino Server 8.0 • ODBS Oracle Client
HK	Hiper K	ERP, maneja clientes servicios, contabilidad, facturación y cobranza	Departamento de Sistemas TN	• Oracle Forms	• SO Red Hat 4.0 • Oracle 10g Release 10.2.0.1.0 • Developer 6i o Oracle Forms o Oracle Reports • Developer Suite 10g o Discovery Administrator o Discovery Client
SITMD	Sistema Integrado Telconet MD	Sistema de manejo de clientes, provisioning, y facturación	Departamento de Sistemas TN	• Synfoni	• SO Centos 5.4 • MySql 5.5 • PHP 5.2 • Apache
NAF	Sistema Financiero	Sistema Administrativo Financiero	Departamento de Sistemas TN	• Oracle Forms • Pl/sql	• Centos 3.9 • Oracle Data Base 10g Release 10.2.0.1.0 64 bits • Forms Reports 6.0

1.3 ÁREAS DE MEGADATOS S.A.

La empresa MEGADATOS S.A. está constituida por las siguientes áreas: Operaciones, Servicios y Aseguramiento de Ingresos, Comercial, Marketing, y el área Financiera Administrativa. Cada área está conformada por departamentos, los mismos que ayudan al desarrollo de diferentes actividades que se llevan a cabo dentro de la empresa.

A continuación se va a describir cada área y los departamentos con los que se cuenta en cada una de ellas.

1.3.1 ÁREA DE OPERACIONES

El área de Operaciones es la encargada de realizar la coordinación de las instalaciones a los clientes, se encarga de dar soporte de segundo y tercer nivel y brindar mantenimiento a los equipos instalados, también gestiona la extensión y crecimiento de la red del producto NETLIFE y la realización de investigaciones de nuevas tecnologías.

Dentro del área de operaciones se encuentran los siguientes departamentos:

- Instalaciones, mantenimiento y soporte.
- GEPON
- Legalizaciones
- GIS

1.3.2 ÁREA DE SERVICIOS Y ASEGURAMIENTO DE INGRESOS

Esta área es la encargada de satisfacer las necesidades de los clientes de MEGADATOS S.A. relacionados con la calidad, características y disponibilidad del servicio ofrecido, receptando y gestionando los requerimientos, quejas y reclamos a través de una adecuada gestión del Área de Servicios y monitoreado mediante encuestas periódicas de satisfacción de clientes.

Adicional, esta área se encarga de generar, administrar y controlar los documentos necesarios que garanticen la oportuna y eficaz gestión para la provisión adecuada de recursos económicos para la organización, con un flujo de ingresos apropiado que permita la correcta operación y crecimiento de la empresa en beneficio de nuestros clientes y accionistas.

Los departamentos que son parte de esta área son los siguientes:

- Facturación y Cobranzas
- IP Contac Center
- Sistema de Gestión de Calidad

1.3.3 ÁREA COMERCIAL

Es la encargada de comercializar los diferentes servicios que ofrece la empresa, asesorar y brindar servicios digitales integrados, facilitando el acceso a la información de nuestros clientes, garantizando relaciones a largo plazo

En esta área se encuentran los siguientes departamentos:

- Ventas Directas
- Canales
- Mantenimiento Corporativos

1.3.4 ÁREA DE MARKETING

Marketing es la interface que busca una relación/asociación de largo plazo con el cliente, a través del establecimiento de ofertas de valor atractivas y diferenciadas que satisfagan las necesidades del mercado, aumentando el valor de marca y manteniendo una comunicación adecuada con cliente.

Las actividades que se involucran dentro de Marketing inician con la investigación de mercado, adquiriendo conocimiento del mismo y del cliente para atender sus

necesidades, generando así un mayor impacto para la venta del producto. Otra actividad que realiza el área de marketing es la administración de productos, que en base a la información de investigación de mercado, pueden crear nuevos productos atractivos al mercado o modificar los existentes para obtener un objetivo deseado, de esta forma la administración de productos engloba la gestión de características del producto, precios del producto, consenso de procesos, promociones, restricciones y limitaciones del producto, posicionamiento en el mercado. Finalmente existe la actividad de comunicación que se enfoca en transmitir en forma efectiva y positiva todo aspecto de interacción entre la empresa y el cliente a través de publicidad, relaciones públicas y guiones de comunicación para las demás áreas.

Dentro de esta área se encuentran los siguientes departamentos:

- Desarrollo de Productos
- Comunicación y Publicidad
- Investigación de Mercado

1.3.5 ÁREA FINANCIERA ADMINISTRATIVA

Es el área encargada de proveer y asegurar que el producto, bien o servicio adquirido, cumpla con los requisitos de compra especificados, en base a una adecuada evaluación y selección de proveedores, cumpliendo los tiempos de entrega establecidos.

También se encarga de facilitar la implantación y administración de los procesos de TALENTO HUMANO de MEGADATOS S.A. Lo que permitirá cumplir con los objetivos estratégicos y la misión de la unidad para la que ha sido creada.

Los departamentos que se encuentran dentro de esta área son:

- Administración y Adquisiciones:
- Contabilidad:
- Auditoría y Control Financiero:

- Tesorería:
- Desarrollo Organizacional y Talento Humano

En el anexo 1 se puede observar el organigrama de MEGADATOS S.A.

1.4 PROCESOS DE MEGADATOS S.A.

A continuación se describen las diferentes funciones y dentro de estas los diferentes procesos que se tiene en MEGADATOS S.A. Para la recopilación de esta información se dialogó con los jefes de cada área, y en base a esto se pudo determinar que la empresa cuenta con las siguientes funciones:

1.4.1 MARKETING

Desarrollar y comunicar constantemente ofertas de valor atractivo para el mercado en base a las capacidades de la empresa y al mismo tiempo generándole un beneficio a la misma.

Dentro de la función de marketing tenemos los siguientes procesos:

- Proceso de Investigación de mercado:
- Proceso de Planificación, diseño, modificación y eliminación de productos:
- Proceso de Comunicación:

1.4.2 GESTIÓN COMERCIAL

Asesorar y brindar servicios digitales integrados, facilitando el acceso a la información de nuestros clientes, garantizando relaciones a largo plazo.

Dentro de esta función se tiene:

- Proceso de gestión comercial

1.4.3 ATENCIÓN AL CLIENTE

Satisfacer necesidades de los clientes de MEGADATOS, receptando y gestionando los requerimientos y reclamos a través de una adecuada gestión de nuestro CALL CENTER y monitoreando mediante encuestas periódicas la satisfacción de nuestros clientes.

Dentro de esta función tenemos al proceso de:

- Proceso de atención al cliente.

1.4.4 FACTURACIÓN Y COBRANZAS

Administrar y asegurar la facturación y cobranzas de la empresa de manera que permitan la provisión adecuada de recursos económicos para la organización, con un flujo de ingresos apropiado para la operación y crecimiento de la empresa en beneficio de nuestros clientes y accionistas.

Dentro de esta función se encuentra el proceso de:

- Proceso de facturación y cobranzas.

1.4.5 DISEÑO, PLANIFICACIÓN E IMPLEMENTACIÓN DE RED GEPON

Dimensionar e implementar adecuadamente la Red GEPON según la estrategia de Marketing y Comercial, apoyados en un diseño que genere estabilidad y escalabilidad sobre la red.

Dentro de esta función están los siguientes procesos:

- Implementación de red GEPON
- Instalación de OLT GEPON.

1.4.6 O & M SERVICIOS Y RECURSOS

Mantener la infraestructura de Telecomunicaciones garantizando niveles óptimos de servicio a nuestros clientes, administrando, gestionando los recursos de la infraestructura y coordinando con proveedores el cumplimiento de las SLA's para mantener, optimizar y mejorar la operación que permitirá cumplir con los niveles de disponibilidad de la Red de Acceso para satisfacer los servicios contratados por el cliente.

Dentro de esta función los procesos que se encuentran son:

- Operación y mantenimiento de servicios y recursos
- Gestión de capacidad y recursos

1.4.7 INSTALACIÓN, TRASLADO Y CANCELACIÓN

Realizar instalación, traslado y cancelaciones según el catálogo de productos y servicios de NETLIFE, siguiendo estándares de calidad y en los tiempos fijados por la Alta Dirección, cumpliendo las metas empresariales y entregando un servicio de excelencia al cliente.

Los procesos de esta función son:

- Proceso de instalación y traslados
- Proceso de cancelación

1.4.8 SOPORTE DE NIVEL 2

Dar solución oportuna y eficiente a las incidencias técnicas escaladas por el IP Contac Center (IPCC) presentadas en el servicio brindado a nuestros clientes.

Los procesos pertenecientes a esta función son:

- Proceso de Soporte de nivel 2

- Proceso de CYBERS

1.4.9 SOPORTE DE NIVEL 3

Analizar y solucionar problemas técnicos de nivel 3 presentados durante la operación en cuanto a Red de Acceso y equipamiento final del cliente, garantizando de esta manera un tiempo de solución y funcionamiento de equipamiento acorde a los productos ofrecidos por la empresa considerando la satisfacción del cliente.

Los procesos son:

- Gestión de incidencias nivel 3
- Prueba de equipos

1.4.10 ADQUISICIONES

Asegurar que el producto, bien o servicio adquirido cumple los requisitos de compra especificados en base a una adecuada evaluación y selección de Proveedores, cumpliendo tiempos de entrega establecidos.

Los procesos de esta función son:

- Proceso de adquisiciones
- Proceso de selección de proveedores

2 ANÁLISIS DE RIESGOS Y ANÁLISIS DEL IMPACTO DEL NEGOCIO (BIA)

2.1 ANÁLISIS DE RIESGOS

En este capítulo se va a describir la metodología que utilizará para realizar el análisis de riesgos, se describirá cada paso de la metodología y su aplicación para el caso de la organización. Una vez que se realice estos pasos preliminares, se obtendrá un reporte de análisis de riesgos, el mismo que contendrá los resultados obtenidos en cada paso de la metodología.

2.1.1 DEFINICIÓN DE RIESGO

Riesgo es la probabilidad de que algo pueda ocurrir o acontecer, que algún hecho indeseable llegue a suceder. Existen algunos factores que están relacionados con el riesgo como son los factores sociales, humanos, políticos, ambientales, etc.

El riesgo es la probabilidad de que una amenaza o un peligro lleguen a suceder convirtiéndose en un desastre; las amenazas o vulnerabilidades por separado no pueden representar algún peligro, pero si estas se unen, podrían llegar a convertirse en un riesgo y causar un gran daño.

En la figura 2.1, se puede observar la relación causa efecto que se tiene

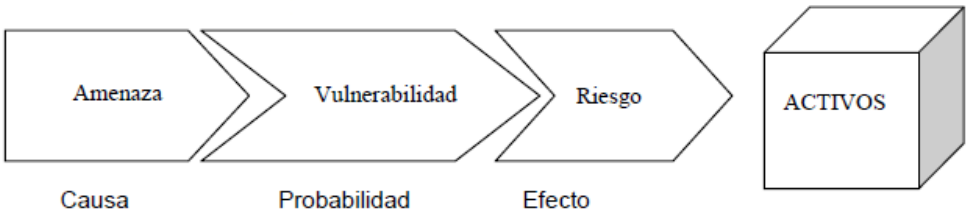


Figura 3.3: Relación Causa – Efecto entre elementos del Análisis de riesgo

Fuente: ISO 27001: 2005

2.1.2 METODOLOGÍA

La importancia de realizar un análisis de riesgo es debido a que el Plan de Continuidad del Negocio consta básicamente de las medidas que se deben tomar frente a una situación creada como consecuencia de la materialización de un riesgo.

Los recursos de tecnologías de la información así como cualquier otro activo de la empresa se encuentran expuestos a riesgos, de ser el caso de que uno de estos riesgos se materialice o llegara a ocurrir podría causar un menor o mayor impacto en el cumplimiento de los objetivos de la organización. En la actualidad la mayoría de las empresas se ven expuestas a una amplia gama de amenazas y/o riesgos que pueden afectar gravemente a los activos de la información y que pueden poner en peligro las funciones de la misma. El objetivo principal que se tiene con el análisis de riesgos es el de proteger los activos que se tienen dentro de la organización.

La metodología que se va a utilizar para la evaluación de riesgos se ha tomado de la "Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información" publicada por NIST (National Institute of Standards and Technology) en su publicación especial NIST SP 800-30.

Esta Guía está estructurada por cinco secciones, las mismas que se listan a continuación:

- Sección 1: Introducción,
- Sección 2: Visión de la Gestión de Riesgos
- Sección 3: Evaluación del Riesgo
- Sección 4: Mitigación del Riesgo
- Sección 5: Evaluación y Valoración.

De acuerdo al alcance de este proyecto nos centraremos en la sección 3 de la guía que es la de la Evaluación del Riesgo.

Algunos de los conceptos que se manejan dentro de la guía son:

- Riesgo: Es la probabilidad de que una amenaza explote una potencial vulnerabilidad en un Activo, en un Dominio o en toda la Organización, y el impacto que provoca ese evento[6].
- Sistema: Es alguno de los siguientes conceptos:
    - Un sistema de computación (mainframe, mini computadora, computadora)
    - Un sistema de red (LAN)
    - Un dominio de red
    - Un Host (un sistema de computación)
    - Nodos de red, routers, switches, y firewalls
    - Una aplicación de red o local en cada sistema de computación
- Vulnerabilidad: Una falla o debilidad en los procedimientos, diseño, implementación, o controles internos de la seguridad del sistema que podría ser explotada (accidental o intencionalmente) y resultar en una brecha de seguridad o en una violación de la política de seguridad del sistema.
- Fuente de Amenaza: Intento y/o métodos dirigidos a la explotación intencional de una vulnerabilidad, o una situación que pueda accidentalmente utilizar una vulnerabilidad.
- Amenaza: El potencial de que una fuente de amenaza explote (accidental o intencionalmente) una vulnerabilidad específica[7].

2.1.2.1 Pasos de la metodología

La metodología de la "Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información" publicada por NIST (National Institute of Standards and Technology) en su publicación especial NIST SP 800-30 consta de 9 pasos los mismos que son los siguientes:

1. Caracterización del Sistema

[6] NIST SP 800-30: Guía de la Gestión de Riesgos para Sistemas TI.
[7] NIST SP 800-30: Guía de la Gestión de Riesgos para Sistemas TI.

2. Identificación de Amenazas
3. Identificación de Vulnerabilidades
4. Análisis de Controles
5. Determinación de la Probabilidad
6. Análisis del Impacto
7. Determinación del Riesgo
8. Recomendaciones para el control
9. Documentación de resultados

A continuación en la figura 2.2 se muestra los nueve pasos que se tienen en la metodología para la evaluación del riesgo.

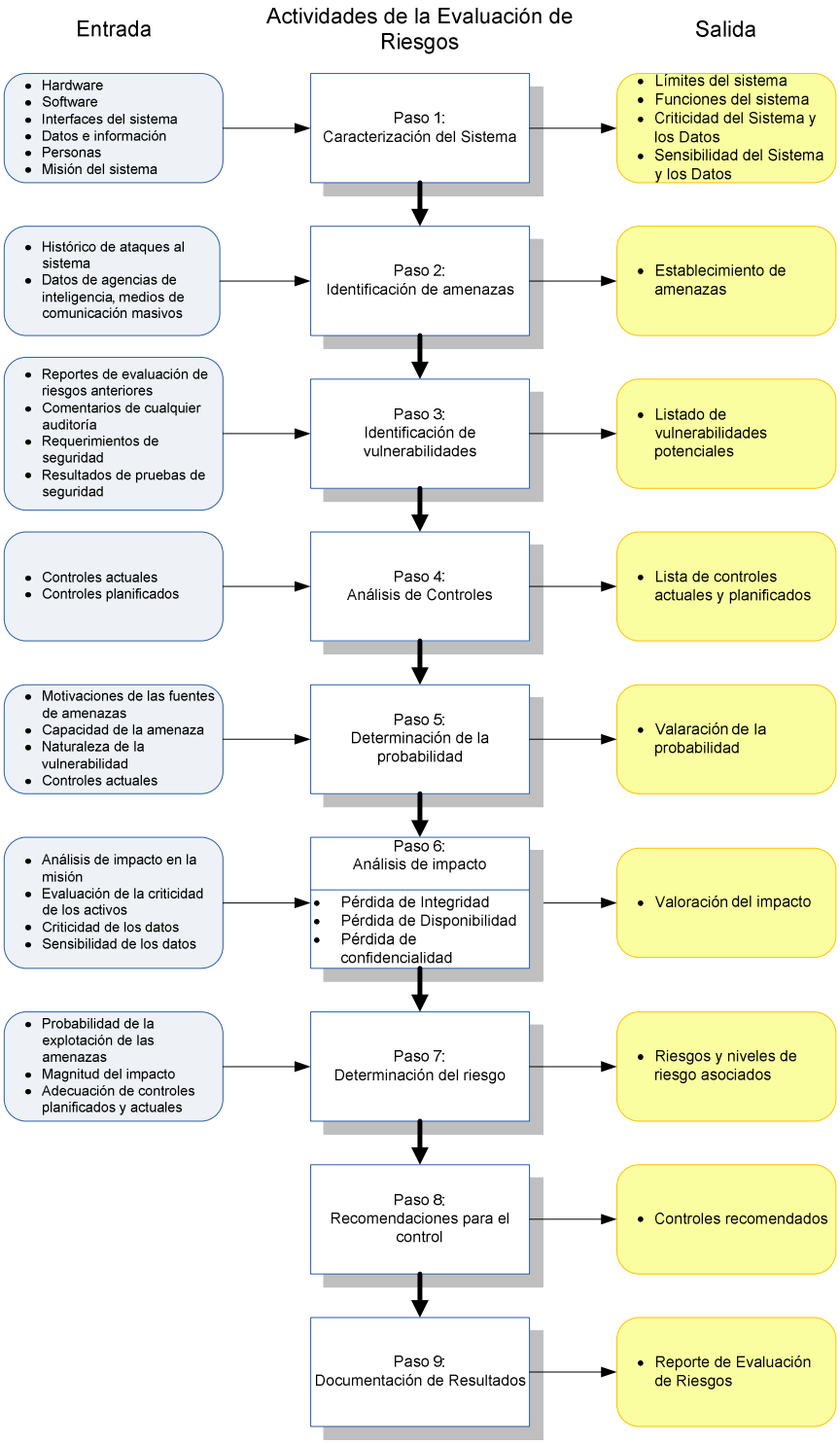


Figura 3.4: Pasos de la metodología de evaluación del Riesgo

FUENTE: NIST SP 800-30

2.1.2.1.1 Paso 1: Caracterización del sistema

En esta sección se identifica las bondades del sistema con los recursos y la información que constituye el sistema (software, hardware, interfaces del sistema, datos y usuarios).

Para la realización de esto se va a identificar el nivel de importancia (NI) que tiene cada grupo de activos dentro de la empresa en base a tres factores que son: confidencialidad, integridad y disponibilidad.

Antes de realizar el cálculo del nivel de importancia (NI), primero se va a describir lo que significa cada uno de los factores involucrados para dicho cálculo.

- **Confidencialidad:** la confidencialidad asegura que la información sea accesible solo para aquellos usuarios que estén autorizados, es decir, evita que la información sea usada por usuarios no autorizados.
- **Integridad:** asegura que la información no sea falsa, también asegura exactitud y completitud, es decir, que los datos que se han recibido y/o se han recuperado sean exactamente los mismos que fueron enviados y/o almacenados, la información no debe tener alguna modificación.
- **Disponibilidad:** garantiza que la información se encuentre siempre disponible, que los usuarios autorizados pueden tener acceso a ésta cuando lo requieran o lo necesiten.

Para poder establecer el nivel de importancia de cada activo, primero vamos a describir las escalas y el criterio que se va a utilizar para tal efecto.

En las tablas 2.1, 2.2, y 2.3 se describen las escalas para los tres factores antes mencionados: confidencialidad, integridad y disponibilidad respectivamente.

Tabla 2.1: Valoración de la Confidencialidad de Activos de Información

FACTOR CONFIDENCIALIDAD (Conf)		
Nivel	**Categoría**	**Descripción**
1	Bajo	Puede ser revelado o proporcionado a cualquiera.
		En caso de revelar su contenido, las consecuencias en la entrega de servicio podrían ser imperceptibles.
2	Medio	Puede ser revelado o proporcionado solo a funcionarios de MEGADATOS S.A.
		En caso de revelar su contenido, las consecuencias en la entrega de servicio podrían ser moderadas.
3	Alto	Puede ser revelado o proporcionado solo al departamento de Operaciones de MEGADATOS S.A.
		En caso de revelar su contenido, las consecuencias en la entrega de servicio podrían ser altas
4	Muy Alto	Puede ser revelado o proporcionado solo al departamento de Operaciones de MEGADATOS S.A., siempre que autorice el Gerente Nacional de dicho Departamento
		En caso de revelar su contenido, las consecuencias en la entrega de servicio podrían ser catastróficas.

Tabla 2.13: Valoración de la Integridad de Activos de Información

FACTOR INTEGRIDAD (Int)		
Nivel	**Categoría**	**Descripción**
1	Bajo	La modificación de su contenido no afectaría la entrega de servicios.
2	Medio	La modificación de su contenido tendría una afectación media en la entrega de servicios.
3	Alto	La modificación de su contenido afectaría de manera considerable en la entrega de servicios.
4	Muy Alto	La modificación de su contenido afectaría de manera muy relevante en la entrega de servicios.

Tabla 2.3: Valoración de la Disponibilidad de Activos de Información

FACTOR DISPONIBILIDAD (Disp)		
Nivel	**Categoría**	**Descripción**
1	Bajo	En caso de que su contenido no estuviese disponible, las consecuencias en la entrega de servicios podrían ser reducidas.
2	Medio	En caso de que su contenido no estuviese disponible, las consecuencias en la entrega de servicios podrían ser moderadas.
3	Alto	En caso de que su contenido no estuviese disponible, las consecuencias en la entrega de servicios podrían ser altas.
4	Muy Alto	En caso de que su contenido no estuviese disponible, las consecuencias en la entrega de servicios podrían ser fatales.

El producto de estos tres factores (confidencialidad, integridad y disponibilidad) finalmente nos va a dar el Nivel de Importancia (NI) en la entrega de servicio para cada activo, en la tabla 2.4 se establece la escala del NI, el mismo que va desde 1 a 64. Para el cálculo de esto se consideró la siguiente fórmula:

Conf x Int x Disp = NI

Formula 1: Nivel de Importancia de los Activo

A partir de la categorización que se describió en las tablas 2.1, 2.2, 2.3 se va a presentar una estimación de los Niveles de Importancia que se tienen.

Tabla 2.4: Rangos de importancia de Activos de Información

RANGOS DE IMPORTANCIA DE LOS ACTIVOS DE INFORMACIÓN		
Nivel	**Categoría**	**Descripción**
1 a 4	Bajo	Activo de importancia baja para asegurar la confidencialidad, integridad y disponibilidad de la información asociada a la entrega de servicios a los usuarios.
5 a 16	Medio	Activo de importancia media para asegurar la confidencialidad, integridad y disponibilidad de la información asociada a la entrega de servicios a los usuarios.
17 a 36	Alto	Activo de importancia alta para asegurar la confidencialidad, integridad y disponibilidad de la información asociada a la entrega de servicios a los usuarios.
37 a 64	Muy Alto	Activo de importancia muy alta para asegurar la confidencialidad, integridad y disponibilidad de la información asociada a la entrega de servicios a los usuarios.

2.1.2.1.2 Paso 2: Identificación de amenazas

El objetivo de este paso, es el de identificar las fuentes de amenazas potenciales que pueden llegar a darse dentro de la empresa MEGADATOS S.A. y compilarlas o resumirlas dentro de un listado.

2.1.2.1.3 Paso 3: Identificación de la vulnerabilidad

Este paso desarrolla una lista de vulnerabilidades del sistema (fallas o debilidades) que pudieran ser explotadas por las potenciales fuentes de amenaza que se obtuvieron en el paso 2.

2.1.2.1.4 Paso 4: Análisis de Controles

Analiza los controles que han sido implementados o están planificados para minimizar o eliminar la probabilidad de que se explote una amenaza sobre una vulnerabilidad del sistema.

2.1.2.1.5 Paso 5: Determinación de la probabilidad

Determina la probabilidad que se puede presentar en caso de que una vulnerabilidad potencial pueda ser explotada o llegue a darse dentro del ambiente de amenazas asociado.

Para la determinación de la probabilidad se usará los niveles definidos en la guía NIST SP 800-30.

Tabla 2.5: Definición de la Probabilidad de Amenaza[8]

Nivel de Probabilidad	Definición de la Probabilidad
Alta	La fuente de amenaza está altamente motivada y es lo suficientemente capaz, y los controles para prevenir que se explote una vulnerabilidad son inefectivos.
Media	La fuente de amenaza está motivada y es capaz, pero los controles implementados pueden impedir la explotación exitosa de una vulnerabilidad.
Baja	La fuente de amenaza carece de motivación y capacidad, o los controles implementados previenen la explotación de una vulnerabilidad, o al menos la dificultan significativamente.

2.1.2.1.6 Paso 6: Análisis del Impacto

Determina el impacto adverso resultante de una explotación exitosa de una amenaza sobre una vulnerabilidad.

De igual manera que en el paso anterior, para el análisis del impacto se va a tomar en cuenta las magnitudes descritas en la guía NIST SP 800-30

[8] Fuente: Guía NIST 800-30

Tabla 2.6: Definición de la Magnitud del Impacto [9]

Magnitud de Impacto	Definición de Impacto
Alta	La explotación de una vulnerabilidad 1. Puede resultar en una alta pérdida de los principales activos tangibles o recursos. 2. Puede significar violación, daño o dificultad de la misión, reputación o interés de la organización. 3. Puede resultar en muerte humana o en una lesión seria.
Media	La explotación de una vulnerabilidad 1. Puede resultar en una pérdida de los activos tangibles o recursos. 2. Puede significar violación, daño o dificultad de la misión, reputación o interés de la organización. 3. Puede resultar en una lesión humana.
Baja	La explotación de una vulnerabilidad 1. Puede resultar en la pérdida de algunos activos tangibles o recursos. 2. Puede afectar notablemente a la misión, reputación o interés de la organización.

2.1.2.1.7 Paso 7: Determinación del Riesgo

Este paso permite evaluar el nivel del riesgo para el sistema TI. Para el cálculo del nivel del riesgo se realiza una matriz, la misma que toma el nombre de matriz del nivel del Riesgo.

[9] Fuente: Guía NIST 800-30

Para el cálculo de la matriz del nivel del Riesgo se emplea una matriz de 3x3, donde la filas corresponden a la probabilidad de amenaza (alta, media y baja) y las columnas al impacto de la amenaza (alto, medio y bajo).

La escala del nivel de riesgo es la siguiente:

- Baja: mayor a 1 hasta 10
- Media: mayor a 10 hasta 50
- Alta: mayor a 50 hasta 100

En a tabla 2.7 se muestra la matriz del nivel del Riesgo

Tabla 2.7: Matriz del Nivel del Riesgo [10]

Probabilidad de Amenaza	**Impacto**		
	Bajo (10)	**Medio (50)**	**Alto (100)**
Alta (1.0)	Bajo 10 x 1.0 = 10	Medio 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Media (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
Baja (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10

2.1.2.1.8 Paso 8: Recomendaciones de control

Se proveen los controles que podrían mitigar o eliminar los riesgos identificados, y que sean apropiados para las operaciones de la organización.

[10] Fuente: Guía NIST SP 800-30

2.1.2.1.9 Paso 9: Documentación de Resultados

Una vez que se ha completado la evaluación del Riesgos, los resultados se documentan en un reporte oficial.

2.2 EVALUACIÓN Y CONTROL DEL RIESGO

2.2.1 INTRODUCCIÓN

En un mundo muy cambiante como es el mundo en que vivimos, donde el crecimiento de las tecnologías de la información en los últimos años se ha visto muy acelerado se puede ver que así como existen nuevas oportunidades también han aparecido nuevas amenazas. Hoy en día se puede observar que una gran mayoría de personas puede tener acceso a las tecnologías de la información, dejando atrás aquellas épocas en donde solo cierto grupo de personas podía tener acceso a las tecnologías.

Realizar un análisis apropiado de riesgos nos permitirá identificar, evaluar y reducir estos riesgos a un nivel aceptable, mediante la implementación de mecanismos y controles apropiados.

Los resultados que se obtuvieron por medio del análisis del Riesgo cuya metodología fue expuesta en la sección 2.1.2, fueron evaluados en base a los diferentes activos que se encuentran en la empresa, para lo cual a dichos activos se los dividió en 6 grupos, los mismos que son: Servidores, Equipos de redes y comunicación, Laptops, Equipos de escritorio, Equipo Computacional Secundario y Recurso Humano.

En el anexo 3 se adjunta la Matriz del Riesgo de todos los grupos de activos con los que cuenta la empresa.

A continuación se procede a realizar una descripción basada en el análisis del primer grupo de activos que tiene la empresa los Servidores; el análisis de los demás grupos de activos se encuentra en el Anexo 3 (Matriz de Riesgos).

2.2.2 EVALUACIÓN DEL RIESGO

Para la evaluación del riesgo lo primero a realizarse es el cálculo del nivel de importancia que tiene cada uno de los siguientes 6 grupos de activos que se tiene en la empresa.

- Servidores
- Equipos de redes y comunicaciones
- Laptops
- Equipos de escritorio
- Equipo Computacional Secundario
- Recurso Humano

Los resultados se muestran a continuación en la tabla 2.8

Tabla 2.8: Cálculo del Nivel de Importancia de los Activos de MEGADATOS S.A.

CALCULO DEL NIVEL DE IMPORTANCIA						
ACTIVO	**N° ACTIVO**	**Conf**	**Int**	**Disp**	**NI**	
SERVIDORES	Servidor de Archivos	3	3	2	18	Alto
	Servidor de Máquinas Virtuales	2	2	1	4	Bajo
	Servidor de Diagramas de Red	3	3	1	9	Medio
	Firewall	4	4	4	64	Muy Alto
	Servidor de Hiperk	3	4	3	36	Alto
	Servidor Blade	4	4	4	64	Muy Alto
	Servidor de correo	3	4	3	36	Alto
	Servidor de Antivirus	3	3	3	27	Alto
	Servidor de WF	3	4	2	24	Alto
	Servidor de Gestión de Calidad	3	3	1	9	Medio
	Servidor de Monitoreo TN	2	2	1	4	Bajo
	Servidor de Monitoreo TN 2	2	2	1	4	Bajo

Tabla 2.8: Cálculo de Nivel de Importancia de los Activos de MEGADATOS S.A. (continuación)

ACTIVO	N° ACTIVO	Conf	Int	Disp	NI	
EQUIPOS DE REDES Y COMUNICACIÓN	Switch CISCO WS-C3560-24TS	3	4	4	48	Muy Alto
	Switch CISCO WS-C3560-48	3	3	2	18	Alto
	Switch CISCO WS-C2950-24	3	3	2	18	Alto
	Switch CISCO WS-C2950-48	3	3	2	18	Alto
	Switch CISCO WS-C2950-48	3	3	2	18	Alto
	Switch LINK SYS SRW224G4P	3	3	2	18	Alto
	Switch LINK SYS SRW224G4P	3	3	2	18	Alto
	Switch LINK SYS SRW224G4P	3	3	2	18	Alto
	Router CISCO 1811	4	4	4	64	Muy Alto
	Equipos Inalámbricos	3	2	1	6	Medio
EQUIPOS DE ESCRITORIO	Todos los equipos	2	3	1	6	Medio
LAPTOPS	Todos los equipos	3	3	2	18	Alto
EQUIPO COMPUTACIONAL SECUNDARIO	Impresoras, scaners, faxes, proyectores	2	3	1	6	Medio
RRHH	Todos el personal	2	3	3	18	Alto

Servidores

Después de haber realizado una valoración de los diferentes servidores que se tiene en MEGADATOS S.A., y observando su nivel de importancia, se puede decir que los servidores más críticos son el servidor de Firewall y el servidor BLADE donde se encuentran virtualizados algunos servidores que son de importancia. Estos servidores sirven de apoyo y ayudan para que se lleven a cabo de la mejor manera los diferentes procesos de la empresa.

Equipos de redes y de Comunicación

Dentro de este grupo de activos, se puede observar que el switch más crítico que se tiene dentro de la empresa es el switch CISCO WS-C3560-24TS pues desde éste salen la mayoría de las conexiones hacia los diferentes equipos que brindan servicio a toda la empresa.

También es importante el router CISCO 1811, el mismo que se encuentra en el TELEPUERTO, en este router se encuentran las diferentes configuraciones hacia las siguientes conexiones: Guayaquil, la central telefónica y la conexión hacia el interurbano.

Equipos de Escritorio

El nivel de importancia que tienen los equipos de escritorio en la empresa es medio, por lo tanto, si alguno de estos equipos de escritorio llegara a fallar y/o a extraviarse, no afectaría mayormente a las actividades del negocio, seria una afectación media.

La información que se alberga en estos activos es información que afectaría en un grado medio a los diferentes procesos que se llevan a cabo en la empresa.

Laptops

En base al análisis realizado las laptops tienen un nivel de importancia alto, son la herramienta de trabajo de la mayoría de los empleados de la organización y contienen información de valor para la empresa debido a que la laptops son asignada generalmente a los gerentes, jefes y coordinadores de las diferentes áreas de la empresa, si se llegara a presentar algún inconveniente con estos activo podría ver afectado algún proceso de la empresa.

Equipos computacionales Secundarios

El nivel de importancia de este grupo de activos es medio, se puede decir que la falla de uno de estos afectaría en un grado medio las diferentes funciones del negocio.

Recurso Humano

El recurso humano es un factor esencial dentro de la empresa, de este depende el buen funcionamiento de la misma, a pesar de que no todo el RR.HH. tiene las mismas funciones y la misma remuneración se va a valorar a todos los empleados como un solo activo.

El nivel de importancia de este activo es alto, en caso de que llegara a faltar o ausentarse alguno de los diferentes empleados se podrían ver afectados los diferentes procesos y servicios que presta la empresa de una manera alta.

2.2.2.1 Establecimiento de Amenazas y de las Acciones de la Amenaza

Para la recolección de información sobre de las diferentes amenazas que existen dentro de la organización se conversó con los jefes de las cada una de las diferentes áreas con las que cuentan MEGADATOS S.A.

En la tabla 2.9, se va a describir las amenazas que se tiene y el impacto que se generaría en caso de que una amenaza llegara a materializarse.

Tabla 2.9: Amenazas/Impacto

TIPO	Nro	AMENAZAS	IMPACTO/Acciones de Amenaza
Ambientales	1	Terremotos/Sismos	• Daño total o parcial de toda la infraestructura de la empresa • Accidentes e incluso pérdidas humanas.
	2	Erupciones Volcánicas	• Daño total o parcial de toda la infraestructura de la empresa • Accidentes e incluso pérdidas humanas.
	3	Deslizamientos	• Daño total o parcial de toda la infraestructura de la empresa • Accidentes e incluso pérdidas humanas.
Humanas	1	Desconfiguración involuntaria del equipo	• Pérdida total o parcial del servicio que brinda el activo
	2	Desconexión de puerto	• Desconexión del servicio para clientes internos
	3	Ingreso a la configuración de equipos por personal no autorizado	• Cambio no autorizado en la configuración del equipo. • Detención de servicio. • Robo de información
	4	Ingreso de personal no autorizado a las instalaciones	• Falla momentánea en los servicios, robo y/o perdida de equipos y pérdidas económicas
	5	Suplantación de identidad	• Cambio no autorizado de configuraciones, violación de la confidencialidad de la información. • Peligro de robos y ataques.
	6	Modificación de información contenida en equipos	• Cambios no autorizados, conflictos entre el personal por desconocimiento de los cambios realizados

Tabla 2.9: Amenazas/Impacto (continuación)

TIPO	Nro	AMENAZAS	IMPACTO/Acciones de Amenaza
Humanas	7	Divulgación de información	• Violación de la confidencialidad de información, mal uso de la información por agentes externos
	8	Error en la etiquetación de activos	• Información sensible podría verse afectada, pérdida de información crítica.
	9	Mantenimiento inadecuado de equipos	• Daño del equipo, afectando al servicio que bridan
	10	Robo o Pérdida del equipo	• Falla momentánea en los servicios y pérdidas económicas
	11	Inundaciones por falla en tuberías del edificio	• Daño de equipos, suspensión temporal de los servicios
	12	Incendios provocados por personal de la empresa	• Pérdida total o parcial de todo el edificio y de equipos • Pérdidas humanas y económicas
	13	Respaldos mal realizados	• Pérdida de la información almacenada en el equipo
	14	Pérdida de Información clave contenida en los equipos	• Pérdida total o parcial de los servicio
	15	Ataques a la red	• Pérdida o daños de los equipos. Suspensión total o parcial del servicio que brinda el activo
	16	Falta de equipos de respaldos	• Pérdida total o parcial de la entrega del servicio que brinda el activo

Tabla 2.9: Amenazas/Impacto (continuación)

TIPO	Nro	AMENAZAS	IMPACTO/Acciones de Amenaza
Tecnológicas	1	Daño de hardware	• Pérdida total o parcial de la entrega del servicio que brinda el activo
	2	Daño de software	• Daño permanente del equipo. Pérdida total o parcial de la entrega del servicio que brinda el activo
	3	Inhibición de puerto	• Desconexión del servicio para clientes internos
	4	Falla eléctrica	• Daño total o parcial de los equipos
	5	Falla en el UPS	• Pérdida de todo el servicio para usuarios internos y se puede quemar el activo
	6	Daño en medios de transmisión	• Pérdida temporal del servicio que brinda
	7	Daño en el aire acondicionado	• Calentamiento de equipos y posible daño de los mismos
	8	Virus, troyanos, gusanos, etc.	• Pérdida temporal del servicio que brinda
			• Violación de la seguridad de información
	9	Software desactualizado	• Falla en la prestación de los servicios que ofrece el activo y pérdidas económicas
	10	Software no licenciado	• Recesión de las actividades de la empresa

2.2.2.2 Resultado de la evaluación del Riesgo

En esta parte se va a enunciar las diferentes vulnerabilidades que se tienen asociadas a cada amenaza.

En la tabla 2.10 se muestra las amenazas junto con las vulnerabilidades que pueden ser explotadas.

Tabla 2.10: Amenazas/Vulnerabilidades

TIPO	Nro	AMENAZAS	VULNERABILIDADES
Ambientales	1	Terremotos/Sismos	• El edificio donde se encuentra ubicado MEGADATOS S.A. no es antisísmico • Quito se encuentra ubicado en una zona sísmica • Falta de capacitación al personal ante emergencias
	2	Erupciones Volcánicas	• Quito se encuentra en una zona geográfica que se encuentra rodeada de volcanes • Falta de capacitación del personal ante emergencias
	3	Deslizamientos	• Quito se encuentra asentado sobre valles y quebradas • Falta de capacitación ante emergencias
Humanas	1	Desconfiguración involuntaria del equipo	• No existe una gestión adecuada de claves de configuración y de acceso. • No existe un procedimiento formal de almacenamiento de contraseñas
	2	Desconexión de puerto	• No hay suficiente control en el ingreso al edificio • No existe una política o normativa de cableado y de cambio de cableado periódico. • No existe una protección física pare evitar desconexiones

Tabla 2.10: Amenazas/Vulnerabilidades (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES
Humanas	3	Ingreso a la configuración de equipos por personal no autorizado	• No existe un control adecuando de ingreso a los equipos • No existe una política de claves y de privilegios de acceso • No existe una política de actualización periódica de claves
	4	Ingreso de personal no autorizado a las instalaciones	• No existe el suficiente control de acceso de personas desconocidas • No se cuenta con un registro de las personas que ingresan a la empresa
	5	Suplantación de identidad	• No existe una adecuada gestión de claves de usuarios y éste podría compartirlas o almacenarlas inadecuadamente.
	6	Modificación de información contenida en equipos	• No existe una política formal de autorización de cambios, migraciones o actualizaciones.
	7	Divulgación de información	• A menudo no se pone en práctica el acuerdo de confidencialidad • No se aplican las sanciones especificadas en el acuerdo de confidencialidad • No se da seguimiento a ex funcionarios
	8	Error en la etiquetación de activos	• No se tiene la información clasificada • No todos los activos se encuentran correctamente etiquetados.

Tablas 2.10: Amenazas/Vulnerabilidades (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES
Humanas	9	Mantenimiento inadecuado de equipos	• No se tiene una política de mantenimiento periódico de equipos.
	10	Robo o Pérdida del equipo	• No se cuenta con equipos de backups de todos los servidores. • No existe un control de acceso adecuado.
	11	Inundaciones por falla en tuberías del edificio	• No se conoce como se encuentra la red de agua en el edificio.
	12	Incendios provocados por personal de la empresa	• No se cuenta con un sistema anti incendios. • No existe una capacitación del personal para casos de emergencia.
	13	Respaldos mal realizados	• No existe una política de respaldos.
	14	Pérdida de Información clave contenida en los equipos	• No se tiene una política de claves de acceso y de ingreso a los equipos. • No se realizan respaldos periódicos de la información contenida en los equipos.
	15	Ataques a la red	• No se tiene una política de claves de acceso y de ingreso a los equipos.
	16	Falta de equipos de respaldos	• No se cuenta con una política para disponer de equipos de respaldos.
Tecnológicas	1	Daño de hardware	• No se tienen las piezas necesarias de repuestos.
	2	Daño de software	• Error en las actualizaciones. • Pérdida o borrado de carpetas propias de aplicaciones.

Tablas 2.10: Amenazas/Vulnerabilidades (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES
	3	Inhibición de puerto	• No hay suficiente control en el ingreso al edificio.
	4	Falla eléctrica	• Sobrecarga en las regletas.
	5	Falla en el UPS	• No se tiene conocimiento de los cortes de energía no programados. • No existe una política de mantenimiento periódico de equipos.
	6	Daño en medios de transmisión	• No existen medios alternos para todos los casos. • Falta políticas de cableado estructurado.
	7	Daño en el aire acondicionado	• No existe una política de mantenimiento periódico de equipos
	8	Virus, troyanos, gusanos, etc.	• No existe un monitoreo continuo para detectar posibles ataques. • No existen suficientes seguridades para bloquear amenazas
	9	Software desactualizado	• No se cuenta con planes de migración de SO y de SW de aplicación
	10	Software no licenciado	• No se cuenta con licencias de todos los programas

2.2.2.3 Acciones de Mitigación de Riesgo

Para el grupo de activos “Servidores”, en la tabla 2.11 se indican las amenazas junto con las vulnerabilidades y también se indicara los controles mitigadores existentes para la mitigación cada una de las amenazas. Para los otros grupos de activos, las acciones de mitigación pueden verse en el Anexo 3.

Tabla 2.11: Controles Mitigadores de los activos "Servidores"

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Ambientales	1	Terremotos/Sismos	• El edificio donde se encuentra ubicado MEGADATOS S.A. no es antisísmico • Quito se encuentra ubicado en una zona sísmica	• Daño total o parcial de toda la infraestructura de la empresa	Ninguna
			• Falta de capacitación al personal ante emergencias	• Accidentes e incluso pérdidas humanas.	
	2	Erupciones Volcánicas	• Quito se encuentra en una zona geográfica que se encuentra rodeada de volcanes	• Daño total o parcial de toda la infraestructura de la empresa	Ninguna
			• Falta de capacitación ante emergencias	• Accidentes e incluso pérdidas humanas.	
	3	Deslizamientos	• Quito se encuentra asentado sobre valles y quebradas	• Daño total o parcial de toda la infraestructura de la empresa	Ninguna
			• Falta de capacitación ante emergencias	• Accidentes e incluso pérdidas humanas.	

Tablas 2.11: Controles Mitigadores de los activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Humanas	1	Desconfiguración involuntaria del equipo	• No existe una gestión adecuada de claves de configuración y de acceso. • No existe un procedimiento formal de almacenamiento de contraseñas	• Pérdida total o parcial del servicio que brinda el activo	Ninguna
	2	Desconexión de puerto	• No hay suficiente control en el ingreso al edificio • No existe una política o normativa de cableado y de cambio de cableado periódico. • No existe una protección física pare evitar desconexiones	• Desconexión del servicio para clientes internos	Revisión y cambio periódico del cableado que se está utilizando
	3	Ingreso a la configuración de equipos por personal no autorizado	• No existe un control adecuando de ingreso a los equipos • No existe una política de claves y de privilegios de acceso • No existe una política de actualización periódica de claves	• Cambio no autorizado en la configuración del equipo. Detención de servicio. Robo de información	Ninguna

Tablas 2.11: Controles Mitigadores de los activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Humanas	4	Ingreso de personal no autorizado a las instalaciones	• No existe el suficiente control de acceso de personas desconocidas • No se cuenta con un registro de las personas que ingresan a la empresa	• Falla momentánea en los servicios, robo y/o perdida de equipos y pérdidas económicas	Se pide identificación de cada persona que ingresa al edificio
	5	Suplantación de identidad	• No existe una adecuada gestión de claves de usuarios y éste podría compartirlas o almacenarlas inadecuadamente	• Cambio no autorizado de configuraciones, violación de la confidencialidad de la información. Peligro de robos y ataques.	Cada empleado tiene su identificación con foto y datos personales.
	6	Modificación de información contenida en equipos	• No existe una política formal de autorización de cambios, migraciones o actualizaciones.	• Cambios no autorizados, conflictos entre el personal por desconocimiento de los cambios realizados	Políticas de control de cambio de configuración de equipos

Tabla 2.11: Controles Mitigadores de los activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Humanas	7	Divulgación de información	• A menudo no se pone en práctica el acuerdo de confidencialidad • No se aplican las sanciones especificadas en el acuerdo de confidencialidad • No se da seguimiento a ex funcionarios	• Violación de la confidencialidad de información, mal uso de la información por agentes externos	Ninguna
	8	Error en la etiquetación de activos	• No se tiene la información clasificada • No todos los activos se encuentran correctamente etiquetados	• Información sensible podría verse afectada, pérdida de información crítica.	Ninguna
	9	Mantenimiento inadecuado de equipos	• No se tiene una política de mantenimiento periódico de equipos	• Daño del equipo, afectando al servicio que bridan	Se posee una política para mantenimientos periódicos de equipos.

Tabla 2.11: Controles Mitigadores de los activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Humanas	10	Robo o Pérdida del equipo	• No se cuenta con equipos de backups de todos los servidores • No existe un control de acceso adecuado	• Falla momentánea en los servicios y pérdidas económicas	Ninguna
	11	Inundaciones por falla en tuberías del edificio	• No se conoce como se encuentra la red de agua en el edificio	• Daño de equipos, suspensión temporal de los servicios	La administración del edificio se encarga del mantenimiento del mismo
	12	Incendios provocados por personal de la empresa	• No se cuenta con un sistema anti incendios	• Pérdida total o parcial de todo el edificio y de equipos	En cada piso hay un extintor y el personal sabe que no debe usar fuego dentro de las instalaciones
			• No existe una capacitación del personal para casos de emergencia	• Pérdidas humanas y económicas	
	13	Respaldos mal realizados	• No existe una política de respaldos	• Pérdida de la información almace-nada en el equipo	Ninguna

Tabla 2.11: Controles Mitigadores de los activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Humanas	14	Pérdida de Información clave contenida en los equipos	• No se tiene una política de claves de acceso y de ingreso a los equipos • No se realizan respaldos periódicos de la información contenida en los equipos	• Pérdida total o parcial de los servicio	Ninguna
	15	Ataques a la red	• No se tiene una política de claves de acceso y de ingreso a los equipos	• Pérdida o daños de los equipos. Suspensión total o parcial del servicio que brinda el activo	Se mantiene un monitoreo constante en los equipos para evitar posibles ataques
	16	Falta de equipos de respaldos	• No se cuenta con una política para disponer de equipos de respaldos	• Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna

Tabla 2.11: Controles Mitigadores de los activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Tecnológicas	1	Daño de hardware	• No se tienen las piezas necesarias de repuestos	• Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna
	2	Daño de software	• Error en las actualizaciones • Pérdida o borrado de carpetas propias de aplicaciones	• Daño permanente del equipo. Pérdida total o parcial de la entrega del servicio que brinda el activo	ninguna
	3	Inhibición de puerto	• No hay suficiente control en el ingreso al edificio	• Desconexión del servicio para clientes internos	Ingresan al TELEPUERTO solo el personal autorizado
	4	Falla eléctrica	• Sobrecarga en las regletas	• Daño total o parcial de los equipos	Sistema de UPS

Tablas 2.11: Controles Mitigadores de los activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Tecnológicas	5	Falla en el UPS	• No se tiene conocimiento de los cortes de energía no programados • No existe una política de mantenimiento periódico de equipos	• Pérdida de todo el servicio para usuarios internos y se puede quemar el activo	Se realiza un mantenimiento periódico de los equipos
	6	Daño en medios de transmisión	• No existen medios alternos para todos los casos • Falta políticas de cableado estructurado	• Pérdida temporal del servicio que brinda	Revisión y cambio de medios de transmisión viejos o defectuosos
	7	Daño en el aire acondicionado	• No existe una política de mantenimiento periódico de equipos	• Calentamiento de equipos y posible daño de los mismos	Ninguna
	8	Virus, troyanos, gusanos, etc.	• No existe un monitoreo continuo para detectar posibles ataques.	• Pérdida temporal del servicio que brinda	Se posee un buen antivirus y se lo usa de la manera adecuada
			• No existen suficientes seguridades para bloquear amenazas	• Violación de la seguridad de información	

Tablas 2.11: Controles Mitigadores de los activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/ACCIONES DE AMENAZA	ACCIONES DE MITIGACIÓN
Tecnológicas	9	Software desactualizado	• No se cuenta con planes de migración de SO y de SW de aplicación	• Falla en la prestación de los servicios que ofrece el activo y pérdidas económicas	Ninguna
	10	Software no licenciado	• No se cuenta con licencias de todos los programas	• Recesión de las actividades de la empresa	Se tiene un contrato de licenciamiento

2.2.3 OPCIONES PARA EL TRATAMIENTO DE RIESGO

Para la determinación de las opciones de tratamiento del riesgo se desarrolló los criterios para asumir los riesgos e identificar los niveles de riesgo.

En la tabla 2.12 se muestran los niveles de riesgos.

Tabla 2.12: Niveles del Riesgo[11]

Nivel del Riesgo	Descripción del riesgo y Acciones Necesarias
Alto	Si una observación o hallazgo es evaluado como un riesgo alto, hay una necesidad apremiante de medidas correctivas. Un sistema existente puede continuar operando, pero un plan de acción correctiva debe ponerse en práctica tan pronto sea posible.
Medio	Si una observación es medida como un riesgo medio, son necesarias acciones correctivas y debe ser desarrollado un plan para incorporar estas acciones dentro de un periodo razonable de tiempo.
Bajo	Si una observación es descrita como riesgo bajo, el Administrador del sistema debe determinar si las acciones correctivas son aún requeridas o decidir si se acepta el riesgo.

De acuerdo a la misión y los objetivos que tienen MEGADATOS S.A. los niveles de riesgo aceptables dentro de la empresa en términos generales son Medio y Bajo, se escogió estos dos niveles ya que el objetivo principal de MEGADATOS S.A. es el de brindar un servicio de calidad a los diferentes clientes.

Entre las opciones de tratamiento válidas se mencionan las siguientes:

[11] Fuente: Guía NIST SP 800-30

- **Asunción del riesgo.** Para aceptar el riesgo potencial y continuar operando el sistema TI, o para implementar controles para reducir el riesgo a un nivel aceptable.
- **Evitar el riesgo.** Para evitar el riesgo por la eliminación de la causa del riesgo y/o consecuencia.
- **Limitación del riesgo.** Para limitar el riesgo por la implementación de controles que minimicen el impacto adverso o la explotación de una amenaza sobre una vulnerabilidad.
- **Planeación del riesgo.** Para manejar el riesgo, implementando un plan de mitigación del riesgo que priorice, implemente y mantenga controles.
- **Búsqueda y detección.** Para reducir el riesgo de pérdida por detección de vulnerabilidades o fallas y búsqueda de controles para corregir la vulnerabilidad.
- **Transferencia de riesgo.** Para transferir el riesgo, usando otras opciones para compensar la pérdida, tales como la adquisición de un seguro[12].

Los riegos Bajos se aceptan y/o se ponen a consideración su mitigamiento al criterio de cada administrador de los diferentes activos que se tiene.

A continuación se detallan las opciones de tratamiento inmediatas para mitigar los riesgos medios existentes en cada uno de los 6 grupos de activos que se tiene en MEGADATOS S.A.

Servidores

- Implementar una política de control de cambios, informar al personal de los cambios que se van a realizar en los servidores.
- Implementar una política de cambio periódico de contraseñas para evitar que cualquier persona pueda ingresar a los servidores.

[12] Traducción por el autor, opciones de mitigación del riesgo de la guía NIST SP 800-30: Risk Management Guide for Information Technology Systems.

- Realizar backups periódicos de las diferentes configuraciones contenidas en los servidores que posee la empresa, documentarlas y validar que estén realizados de forma correcta.
- Implementar una política de respaldo de información de los servidores que se tienen en la empresa
- Solicitar presupuesto para poder adquirir equipos que nos sirvan de backups.
- Conseguir un proveedor que esté a la mano en caso de que llegara a fallar cualquiera de las piezas de los servidores.

Equipos de Redes y Comunicación

- Implementar una política de control de cambios, informar al personal de los cambios que se van a realizar en los servidores.
- Implementar una política de cambio periódico de contraseñas para evitar que cualquier persona pueda ingresar a los equipos.
- Realizar backups periódicos de las diferentes configuraciones contenidas en los equipos, documentarlas y validar que estén realizados de forma correcta.
- Solicitar presupuesto para poder adquirir equipos que nos sirvan de backups.
- Implementar una política de actualizaciones periódicas de IOS y de SO de los equipos.

Equipos de escritorio

- Implementar una política de actualización de equipos de escritorio cada cierto periodo de tiempo.
- Implementar una política de backups de equipos, tener a la mano algunos equipos de backups por si acaso llegue a fallar alguno.

Laptops

- Implementar una política de mantenimientos periódicos a las laptops, así se evitará el daño de las diferentes partes y elementos de estos equipos.

- Implementar una política de respaldo de información, enseñarle al usuario que debe respaldar periódicamente su información, puesto que son activos que fácilmente se pueden sustraer.

Equipo Computacional secundario

- Implementar una política de mantenimiento periódico de equipos.

RRHH

- Implementar una política de capacitaciones periódicas a los empleados en los diferentes equipos que se maneja en la empresa.
- Implementar una política de remplazo del personal ausente.

Una vez que se describieron las opciones de tratamiento inmediatas para mitigar los riesgos medios que se tiene en la empresa se va a describir los controles de mitigación que ya se tienen en la empresa establecidos.

Los controles que se tiene en la empresa son:

- Para evitar que exista problemas con los medio de transmisión en los diferentes equipos de redes y comunicación, en la empresa se realiza un cambio periódico de cableado que se encuentra en mal estado.
- A pesar de poseer un sistema de entradas y salidas caduco, se trata de que todo el personal que ingresa a la empresa se anuncie primero en recepción para evitar que ingrese personal no autorizado.
- La empresa tiene un contrato con un buen antivirus, lo cual hace que todos los equipos de la empresa cuenten con protección para evitar posibles ataques de virus, spam, etc.
- La empresa posee un contrato de licenciamiento con Microsoft, esto permite tener el Software actualizado con las últimas versiones de cada producto.
- Se mantiene monitoreados los equipos para evitar posibles ataques a la red

- En caso de que se llegar a dar un incendio en cada piso hay un extintor y personal que sabe cómo usarlo, adicionalmente el personal sabe que no debe usar fuego dentro de las instalaciones

La empresa debe poner en práctica los controles de mitigación lo antes posible, pues como se puede observar son muy pocos los controles que se tienen implementados, y esto puede ser causante de que alguno de los riesgos lleguen a materializarse y que se tenga algún incidente grave dentro de la compañía.

Luego de realizar el análisis de la Matriz de Riesgos, en la tabla 2.13 se realiza un conteo de los diferentes Niveles del Riesgo que se obtuvieron en cada uno de los 6 grupos de activos.

Tabla 2.13: Resumen del análisis de riesgos

ACTIVOS	Riesgos Altos	Riesgos Medios	Riesgos Bajos
Servidores	--	10	23
Equipos de Redes y de Comunicación	--	6	27
Equipos de Escritorio	--	1	33
Laptops	--	3	30
Equipo Informático Computacional secundario	--	--	33
RRHH	--	2	5

Finalmente y revisando la Matriz de Riesgos y el resumen de la misma se puede recomendar lo siguiente:

- Implementar un sistema de software de entradas y salidas más actualizado y tecnificado debido a que el sistema actual que se tiene es muy caduco y no permite dar los accesos necesarios y adecuados a cada empleado.
- Generar una política de respaldo de la información, pen la que cada usuario pueda tener respaldada toda la data de sus equipos.
- Solicitar el presupuesto necesario para tener equipos de backups.
- Establecer una política de etiquetación de activos.
- Revisar periódicamente los sistemas eléctricos del edificio y los equipos de backups que se tiene en la empresa.

2.3 ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

El Análisis de Impacto del Negocio también conocido como BIA (Business Impact Analisis) es la base para cualquier Plan de Continuidad del Negocio. La elaboración del BIA es un proceso esencial en el desarrollo de un Plan de Continuidad del Negocio.

El Análisis del Impacto del Negocio nos va a permitir conocer cuáles son los procesos y servicios más críticos de la empresa, en otras palabras, el objetivo principal del BIA es determinar y entender qué procesos son esenciales y qué recursos necesitan estos procesos para poder ejecutarse. Al tener conocimiento de todo esto lo que logramos es asegurar la continuidad de las operaciones en la organización. Al especificar qué procesos y servicios son los más críticos, se podría establecer la base para poder realizar en consecuencia una estrategia de recuperación adecuada.

Cabe recalcar que el BIA se aplica solo para riesgos que sean catastróficos.

A la hora de elaborar un Análisis de Impacto del Negocio se tiene cuatro objetivos principales los cuales son:

- Definir los tipos de impacto que se deberían considerar.
- Identificar las funciones o procesos críticos de la empresa y las interdependencias de cada una.
- Identificar cual sería el impacto que cause la interrupción de cada una de las funciones o procesos críticos de la empresa.
- Identificar los recursos mínimos necesarios para la recuperación satisfactoria de las funciones o procesos que se identifican como críticos.

Dentro del análisis de impacto de negocio se puede distinguir las siguientes actividades que se deben llevar a cabo:

- **Identificación de Procesos Críticos:** aquí se va a establecer los procesos críticos del negocio que se realizan en la compañía, así como también los responsables de cada uno de ellos.
- **Identificación de los Recursos que soportan a los procesos críticos:** en esta actividad se va a definir los recursos de hardware y de software que soportan los procesos críticos de la compañía.
- **Identificación de Áreas y Usuarios responsables de los recursos que usan los procesos críticos:** en esta parte se va a identificar las áreas y las personas responsables y/o encargadas de los diferentes recursos que cada proceso crítico usa en la empresa.
- **Valoración de la Criticidad de los Procesos Críticos:** Pueden darse dos valoraciones, una basada en la importancia para la compañía de los procesos cuya ausencia tendría un impacto alto en la actividad de la compañía (valoración cualitativa). La otra, se referiría a las pérdidas económicas por período de tiempo, debido a la ausencia de los procesos (valoración cuantitativa).

- **Período Máximo de Interrupción:** El acumulado de pérdidas suele ir creciendo linealmente a medida que pasan los días manteniendo las actividades interrumpidas. No obstante, a partir de un momento que denominaremos Período Máximo de Interrupción, las pérdidas sufren un aumento significativo y las funciones no podrían ser reasumidas.

2.3.1 IDENTIFICACIÓN DE PROCESOS CRÍTICOS

Una vez que se identificaron todos los procesos que se tiene en la empresa (Sección 1.4), se procede a identificar cuáles de éstos procesos son los procesos críticos y cuáles son los responsables del mismo. Para la obtención de esta información fue necesaria la participación del personal responsable de cada proceso y de aquellos trabajadores que conocen en profundidad los mismos.

En la tabla 2.14 se observar los procesos críticos que se tiene en la empresa.

Tabla 2.14: Procesos Críticos de MEGADATOS S.A.

PROCESOS	DESCRIPCIÓN	FRECUENCIA DE OCURRENCIA	RESPONSABLE
Proceso de gestión comercial	Asesorar y brindar servicios digitales integrados, facilitando el acceso a la información de nuestros clientes, garantizando relaciones a largo plazo.	Diario	Jefe de Ventas

Tabla 3.14: Procesos Críticos de MEGADATOS S.A. (continuación)

PROCESOS	DESCRIPCIÓN	FRECUENCIA DE OCURRENCIA	RESPONSABLE
Proceso de facturación y cobranzas	Administrar y asegurar la facturación y cobranzas de la empresa, de manera que permitan la provisión adecuada de recursos económicos para la organización, con un flujo de ingresos apropiado para la operación y crecimiento de la empresa en beneficio de nuestros clientes y accionistas.	Mensual	Gerente de Auditoria
Proceso de instalación y traslados	Realizar la instalación y el traslado del servicio solicitado por el cliente, siguiendo estándares de calidad y en los tiempos fijados por la Alta Dirección.	Diario	Gerente Nacional de Operaciones
Proceso de cancelación	Realizar la cancelación del servicio adquirido por el cliente, siguiendo los estándares de calidad y en los tiempos fijados por la Alta Dirección.	Diario	Gerente Nacional de Operaciones
Proceso de Adquisiciones	Asegurar que el producto, bien o servicio adquirido cumple los requisitos de compra especificados en base a una adecuada evaluación y selección de Proveedores, cumpliendo los tiempos de entrega establecidos	Diario	Jefe de Adquisiciones

2.3.2 IDENTIFICACIÓN DE LOS RECURSOS QUE SOPORTAN A LOS PROCESOS CRÍTICOS

En este punto se va a definir los recursos que soportan a los procesos críticos de la empresa, en la sección 1.2.2.2 se tiene la información del inventario de hardware (servidores, equipos de redes y comunicación, equipo computacional secundario, etc.) y en la sección 1.2.2.3 el inventarios de software (aplicaciones) que existen en la empresa, esto con el fin de identificar aquellos recursos que den soporte directo a los procesos críticos que se tiene dentro de la empresa.

Los tipos de recursos que se van a analizar son:

- **Hardware,** identificando cada uno de los elementos hardware que soportan los sistemas de información de la compañía.
- **Software Base**, recogiendo todos aquellos componentes de software, incluido todos los asociados al sistema operativo, indispensables para el funcionamiento y optimización del Sistema de Información de la compañía.
- **Software de Aplicaciones**, inventariando las aplicaciones de gestión que son utilizadas en la empresa, es decir los diferentes ERPs que ayudan a realizar los diferentes procesos que se llevan a cabo día a día en la empresa.

2.3.3 IDENTIFICACIÓN DE DEPARTAMENTOS Y USUARIOS RESPONSABLES DE LOS RECURSOS QUE USAN LOS PROCESOS CRÍTICOS

En esta sección lo que se va a realizar es identificar qué departamento y/o usuario maneja o administra los recursos que cada proceso usa, pues, cada uno de los recursos que cada proceso usa, dentro de la empresa está gestionado por un departamento y/o usuario..

2.3.4 VALORACIÓN DE LA CRITICIDAD DE LOS PROCESOS CRÍTICOS

En este ítem se debe realizar una evaluación de los impactos económicos y operacionales. Realizar una valoración de pérdidas no es un asunto sencillo de

realizar ya que existen aspectos que no se pueden tomar en cuenta puesto que son aspectos intangibles tales como la imagen de la organización.

Según el libro “Planes de Contingencia” de Juan Gaspar Martínez[13] existen diversos tipos de impactos dentro de los cuales podemos nombrar a los siguientes:

1. Pérdida de ingresos y beneficios: en empresas cuya razón de ser sea la de generar ingresos y producir beneficios, es muy importante que el flujo de los mismos no se detenga, ya que se pudiera poner en peligro la existencia de la organización.
2. Incremento de costes y/o gastos: la interrupción de ciertas funciones o procesos puede generar el alza de los costes o gastos que tiene la organización, como pérdida de productividad, multas, pérdida de descuentos, defectos o falta de control, etc. Esta valoración debe ser cuantitativa.
3. Peligro para las personas: procesos que si, como consecuencia de un incidente, no se desempeñan de forma adecuada pueden poner en peligro la vida de las personas. Su valoración deberá basarse en criterios los más objetivos posibles y su calificación puede ser cuantitativa o cualitativa.
4. Impacto operacional: procesos que afectan el funcionamiento de la organización y su ausencia puede afectar al correcto funcionamiento de otras funciones.
5. Impacto comercial: si la interrupción de uno de los procesos tiene repercusiones en las relaciones con clientes, en caso de que la interrupción sea muy grave puede ocurrir los siguiente:
    a. Que el cliente se vea forzado a cambiar de proveedor, es decir que se pudiera perder al cliente.
    b. Que las ventas pérdidas durante la interrupción no se recuperen nunca.
    c. Que si la organización presta un servicio público, la falta de este servicio pueda derivar en demandas jurídicas.

[13] MARTINEZ Juan Gaspar, PLANES DE CONTINGENCIA: La Continuidad del Negocio en la Organizaciones, Juan Gaspar Martinez, Ediciones Diaz Santos, S.A., 2004

   d. Que si se trata de un organismo público, pueda generar la desconfianza entre los ciudadanos.
6. Pérdida de calidad: procesos cuya interrupción afecta al control de la calidad de los servicios o productos que se entrega a los clientes. Su presencia puede tener efectos a corto o mediano plazo en la credibilidad de la organización ante sus clientes y esto puede conllevar a un impacto comercial y/o económico.
7. Impacto en la imagen de la organización: procesos que con su interrupción pueden no causar pérdidas inmediatas, pero si un deterioro en la imagen de la organización, que a mediano plazo conllevara a la pérdida de mercado.
8. Incumplimiento de obligaciones jurídicas: procesos que al quedar interrumpidos generan problemas de incumplimiento de obligaciones que pueden acarrear sanciones económicas o administrativas por parte de organismos públicos.
9. Impacto ambiental: procesos cuya interrupción puede causar efectos nocivos en la salud de la población o en el medio ambiente.

En este caso, para el desarrollo del Plan de Continuidad del Negocio de la empresa MEGADATOS S.A. vamos a simplificar esta valoración, por lo tanto se va a realizar una valoración de acuerdo a las prioridades, es decir el proceso más crítico tendrá una mayor prioridad con puntaje de 1 y el menos critico una menor prioridad con un puntaje de 3.

A continuación en la tabla 2.15 y 2.16 se describen los rangos que se van a utilizar para la determinación de la criticidad del software y del hardware.

Tabla 2.15: Rangos de criticidad de Software

RANGOS DE CRITICIDAD DE Software	
1	La organización/departamento no puede funcionar sin el sistema
2	La organización/departamento no puede funcionar parcialmente sin el sistema
3	La organización/departamento puede funcionar sin el sistema

Tabla 2.16: Rangos de criticidad de Hardware

RANGOS DE CRITICIDAD DE Hardware	
1	La organización/departamento no puede funcionar sin el hardware
2	La organización/departamento no puede funcionar parcialmente sin el hardware
3	La organización/departamento puede funcionar sin el hardware

En las tablas 2.19, 2.20, 2.21, 2.22 y 2.23 se puede observar el rango de criticidad que tiene cada proceso.

2.3.5 PERIODO MÁXIMO DE INTERRUPCIÓN

Después de haber establecido los procesos que componen la empresa y conocer la criticidad de cada uno de ellos, se va a establecer los tiempos de recuperación. Teniendo en cuenta que el objetivo principal del Plan de Continuidad de negocio es dar continuidad al negocio tras un incidente o contingencia grave con las menores pérdidas económicas posibles para la empresa, para calcular el período máximo de interrupción se van a tomar en cuenta para cada proceso dos conceptos:

- RPO: (Recovery Point Objective) Punto Objetivo de Recuperación: Es el punto de partida desde el cual se tiene que iniciar la recuperación del proceso. El RPO expresa la cantidad de datos que un proceso puede llegar a perder antes de que esto traiga consecuencias negativas a la organización. Es muy importante saber si es necesario disponer de la información que se tenía justo antes de la catástrofe, o se puede utilizar información previa (hasta qué momento: minutos, horas, días, semanas, etc.).
- RTO: (Recovery Time Objective) Tiempo Objetivo de recuperación: que es el máximo tiempo permitido para que un proceso pueda estar caído como consecuencia de cierto evento, es decir el tiempo que tomara al personal de TI volver a levantar al proceso o volver a ponerlo en línea.

La figura 2.3 muestra una imagen donde explica de mejor manera el RPO y el RTO.

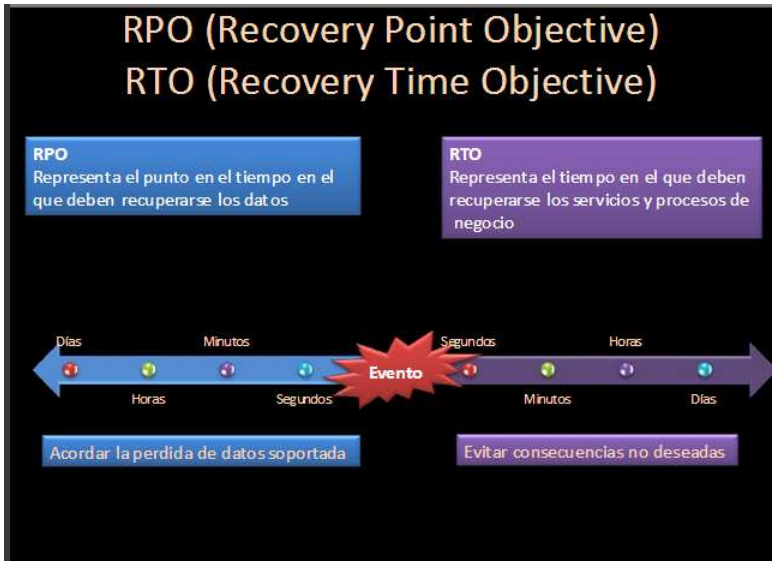


Figura 3.5 RPO Y RTO

FUENTE: http://www.slideshare.net/CarlosFrancavilla/plan-de-continuidad-de-negocios

A continuación, en la tabla 2.17 se definen los diferentes intervalos de tiempo para establecer los niveles de los Tiempos Objetivos de Recuperación.

Tabla 2.17: Niveles de los Tiempos Objetivos de Recuperación

NIVEL RTO	Intervalo de Recuperación
1	Menor a 1 día
2	Entre 1 y 2 días
3	Entre 2 y 3 días
4	Entre 3 días y 1 semana
5	Entre 1 a 2 semanas
6	Más de 2 semanas

Para poder clasificar los niveles de los Puntos Objetivos de Recuperación (RPO) se han definido también una serie de niveles estableciendo los puntos de partida para la restauración de los datos de las diferentes funciones de negocio.

En la tabla 2.18 se describen los diferentes niveles que se han establecido para los Puntos Objetivos de Recuperación.

Tabla 2.18: Niveles de los Puntos objetivos de Recuperación

NIVEL DE RPO	DATOS DE LA RECUPERACIÓN
1	Datos justo antes de la contingencia
2	Máximo 1 día antes de la contingencia
3	Máximo 3 días antes de la contingencia
4	Máximo 1 semana antes de la contingencia
5	Máximo 2 semanas antes de la contingencia
6	Más de 2 semanas

El cálculo del nivel del RPO y del RTO es importante ya que de esto dependerá la selección de la estrategia de respaldo adecuada a las necesidades de la recuperación

Pueden existir procesos en los que el tiempo de recuperación es muy pequeño (horas), así como, también existirán procesos en los cuales su periodo de recuperación será mayor (días o semanas).

Cabe recalcar que lo niveles de RTO y RPO fueron establecidos con cada una de las Gerencias de las diferentes áreas de la empresa, de acuerdo a la criticidad de cada uno de los procesos que se tiene. Estos valores se establecieron de acuerdo a los SLAs que la empresa debe cumplir, los mismos que se encuentran establecidos en la Superintendencia de Telecomunicaciones y también los SLAs propios que tiene la empresa los cuales se encuentran establecidos en el contrato que firma el cliente.

2.3.6 RESULTADOS DEL BIA

En esta sección se va a poner en práctica todo lo mencionado en la sección 2.3, es decir, se va a definir los recursos que necesita cada proceso crítico del negocio, también se va definir cuáles son los responsables o dueños de cada proceso, así como también la criticidad de cada proceso, el RPO y el RTO.

En las tablas 2.19, 2.20, 2.21, 2.22, 2.23, se realiza el Análisis del Impacto de cada proceso crítico que se tiene en la empresa. En estas tablas se distinguen las actividades que se deben llevar a cabo para el Análisis del Impacto del Negocio descritas en la sección 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.3.5.

En base del análisis realizado y evaluando los resultados obtenidos, se puede concluir lo siguiente:

- El proceso con mayor prioridad es el proceso de facturación el cual no puede estar fuera de servicio entre uno y dos días y los datos que se pueden perder son máximo de tres días antes de la contingencia. Si este proceso llegar a caerse más del tiempo mencionado empezaría a causar pérdidas económicas en la empresa.

- El siguiente proceso importante es el de instalación y traslados, el cual no debe pasar caído más de tres días y los datos que se pueden perder son datos de hasta tres días, es importante ya que su importancia radica en que el proceso de instalaciones y traslados es directamente proporcional a las ganancias que se genera en la empresa.

Tabla 2.19: Análisis del proceso de Gestión Comercial

1. PROCESO DE GESTIÓN COMERCIAL									
SOFTWARE				**HARDWARE**				**RPO**	**RTO**
Nombre	**Descripción**	**Responsable**	**Crit**	**Nombre**	**Descripción de HW**	**Localización**	**Crit**		
Correo electrónico	----	Administrador de Red Interna	3	Servidor de Correo	• SO Windows server 2003 Standar Edition SP2 • Intel Xenon 3.6 GHz • 2 GB DE RAM • 220 GB de Disco Duro	TELEPUERTO	2	4	4
				Servidor de SIT	• SO Red Hat 4.0 • 2.5 GB de RAM • 500 GB de Disco Duro	TELEPUERTO	2		
SIT	Sistema de manejo de clientes, provisioning, y facturación	Departamento de Sistemas de TN	2	Laptop	• Cualquier modelo	Oficinas de TN	3		
				Equipos de comunicación y redes	• Router CISCO 1811 • Switch CISCO WS-C3560-24TS	TELEPUERTO y RACK 2do piso	2		

Tabla 2.20: Análisis del proceso de Facturación y Cobranzas

2. Proceso de facturación y cobranzas									
SOFTWARE				**HARDWARE**				**RPO**	**RTO**
Nombre	**Descripción**	**Responsable**	**Crit**	**Nombre**	**Descripción de HW**	**Localización**	**Crit**		
Correo electrónico	----	Administrador de Red Interna	3	Servidor de Correo	• SO Windows server 2003 Standar Edition SP2 • Intel Xenon 3.6 GHz • 2 GB DE RAM • 220 GB de Disco Duro	TELEPUERTO	2	3	2
SIT	Sistema de manejo de clientes, provisioning, y facturación	Departamento de Sistemas de TN	2	Servidor de SIT	• SO Red Hat 4.0 • 2.5 GB de RAM • 500 GB de Disco Duro	TELEPUERTO	2		
				Servidor de HK	• SO Red Hat 4.0 • Intel Xenon 1.86 GHz. 2 Procesadores • 1.5 GB de RAM • 250 GB de Disco Duro	TELEPUERTO	2		
HK	ERP, maneja clientes servicios, contabilidad, facturación y cobranza	Departamento de Sistemas de TN	2	Laptop	• Cualquier modelo	3er piso	3		
				Equipos de comunicación y redes	• Router CISCO 1811 • Switch CISCO WS-C3560-24TS	TELEPUERTO RACK 2do piso	2		
				Impresora	• Xerox Phaser 3635	Área de Facturación	3		

Tabla 2.21: Análisis del proceso de Instalación y Traslado

3. PROCESO DE INSTALACIÓN Y TRASLADOS									
SOFTWARE				**HARDWARE**				**RPO**	**RTO**
Nombre	**Descripción**	**Responsable**	**Crit**	**Nombre**	**Descripción de HW**	**Localización**	**Crit**		
Correo electrónico	----	Administrador de Red Interna	3	Servidor de Correo	• SO Windows server 2003 Standar Edition SP2 • Intel XeNon 3.6 GHz • 2 GB DE RAM • 220 GB de Disco Duro	TELEPUERTO	2	3	3
SIT	Sistema de manejo de clientes, provisioning, y facturación	Departamento de Sistemas de TN	2	Servidor de SIT	• SO Red Hat 4.0 • 2.5 GB de RAM • 500 GB de Disco Duro	TELEPUERTO	2		
				Laptop	Cualquier modelo	Área de Instalaciones	3		
Aplicación para verificar el status de los enlaces	Sistema de estatus de enlaces	Luis Chang	3	Teléfono	Cualquier modelo	Área de Instalaciones	3		
				Equipos de comunicación y redes	• Router CISCO 1811 • Switch CISCO WS-C3560-24TS	TELEPUERTO y RACK 2do piso	2		
				Impresora	Xerox Phaser 3635	Área de Instalaciones	3		

Tabla 2.22: Análisis del proceso de Cancelaciones

4. PROCESO DE CANCELACIÓN									
SOFTWARE				**HARDWARE**				**RPO**	**RTO**
Nombre	**Descripción**	**Responsable**	**Crit**	**Nombre**	**Descripción de HW**	**Localización**	**Crit**		
Correo electrónico		Administrador de Red Interna	3	Servidor de Correo	• SO Windows server 2003 Standar Edition SP2 • Intel Xeon 3.6 GHz • 2 GB DE RAM • 220 GB de Disco Duro	TELEPUERTO	2	4	4
SIT	Sistema de manejo de clientes, provisioning, y facturación	Departamento de Sistemas de TN	2	Servidor de SIT	• SO Red Hat 4.0 • 2.5 GB de RAM • 500 GB de Disco Duro	TELEPUERTO	2		
				Laptop	Cualquier modelo	Área de Instalaciones	3		
Aplicación para verificar el estatus de los enlaces	Sistema de estatus de enlaces	Luis Chang	3	Teléfono	Cualquier modelo	Área de Instalaciones	3		
				Equipos de comunicación y redes	• Router CISCO 1811 • Switch CISCO WS-C3560-24TS	TELEPUERTO y RAC 2do piso	2		
				Impresora	Xerox Phaser 3635	Área de Instalaciones	3		

Tabla 2.23: Análisis del proceso de Adquisiciones

5. Proceso de adquisiciones									
SOFTWARE				**HARDWARE**				**RPO**	**RTO**
Nombre	**Descripción**	**Responsable**	**Crit**	**Nombre**	**Descripción de HW**	**Localización**	**Crit**		
Correo electrónico		Administrador de Red Interna	3	Servidor de Correo	• SO Windows server 2003 Standar Edition SP2 • Intel Xenon 3.6 GHz • 2 GB DE RAM • 220 GB de Disco Duro	TELEPUERTO	2	2	3
				Servidor de HK	• SO Red Hat 4.0 • Intel Xenon 1.86 GHz. 2 Procesadores • 1.5 GB de RAM • 250 GB de Disco Duro	TELEPUERTO	2		
HIPERK	Sistema de manejo de clientes, provisioning, y facturación	Departamento de Sistemas de TN	3	Laptop		Bodega	3		
				Teléfono		Bodega	3		
				Equipos de comunicación y redes	• Router CISCO 1811 • Switch CISCO WS-C3560-24TS	TELEPUERTO y RACK 2do piso	2		
				Impresora	Lexmark X738 de	Bodega	3		

3 DESARROLLO DEL PLAN DE CONTINUIDAD DE NEGOCIO

3.1 INTRODUCCIÓN

Este proyecto está enfocado en la realización de un Plan de Continuidad de Negocio o BCP (Business Continuity Planning) para la empresa MEGADATOS S.A. Este plan establece como objetivo el recuperar y restaurar las principales funciones críticas que han sido parcial o totalmente interrumpidas después de una contingencia o desastre de una organización.

Para la realización del mismo, se ha utilizado como referencia el estándar de la Norma BS25999 Gestión de Continuidad de Negocio. Esta norma incorpora la Gestión de Continuidad de Negocio dentro de un proceso de mejora continua "PDCA" (Planear, Hacer, Verificar, Actuar), ver figura 3.1, haciendo que el Plan de continuidad esté permanentemente actualizado ante la posible ocurrencia de un incidente.

Figura 3.1 Esquema del Modelo PDCA

3.1.1 LA NORMA BS 25999

EL BS-25999 es un estándar Británico, es un documento que fue desarrollado por un amplio grupo de expertos, que actúa tanto como un código de Práctica así como de especificación.

La norma BS 25999 consta de dos partes y fue publicada por la British Standards Institution, la primera parte es el código de prácticas que fue publicada en noviembre del 2006 y la segunda parte es la especificación que fue publicada en noviembre del 2007.

La primera parte, el código de buenas prácticas, proporciona unas recomendaciones de buenas prácticas en cuanto a la Gestión de la Continuidad de Negocio (BCM), este documento es simplemente un documento guía.

La segunda parte, la especificación, proporciona los requisitos de un Sistema de Gestión de Continuidad de Negocio (SGCN) basado en las mejores prácticas de BCM. Aquí se describen cuáles son los requisitos auditables para la implementación de un Sistema de Gestión de la Continuidad de Negocio.

El ciclo de vida de la Gestión de la Continuidad de Negocio consta de 5 etapas, las mismas que son:

- Programa de Gestión de la Continuidad del Negocio.
- Comprensión de la organización.
- Determinar la estrategia de la continuidad o recuperación.
- Desarrollo e implementación de la respuesta BCM.
- Validación, mantenimiento y revisión.

En la figura 3.2 se muestra el ciclo de vida del SGCN.

Figura 3.2: Ciclo de Vida del BCM

FUENTE: Http://www.mariourenacuate.com/wp-content/uploads/2010/03/222-Implementaci%C3%B3n-BS25999-Mure%C3%B1a-2010-03-02.pdf

La Gestión de la Continuidad del Negocio (BCM) consiste en la mejora proactiva de la resistencia de la organización frente a diversas contingencias que se pueden presentar dentro de la misma.

3.1.2 DEFINICIÓN DE BCP

A continuación se va a dar algunas definiciones del Plan de Continuidad de Negocio:

"El BCP es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos del negocio generando un impacto mínimo o nulo ante una contingencia" [14]

[14] www.acis.org.co/fileadmin/Conferencias/ConferenciaBCP.pdf

"Un plan de Continuidad de Negocio es un proceso que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para construir y reforzar la capacidad de dar una respuesta efectiva que salvaguarde los intereses, la imagen y el valor de las actividades realizadas por la misma".[15]

En otras palabras se puede decir que un Plan de Continuidad de Negocio nos ayuda a conocer los diferentes activos que se tiene en la organización y la manera o estrategias para salvaguardarlos ante cualquier situación de contingencia que se puede presentar en la organización para garantizar la continuidad de las operaciones y/o la entrega de servicios.

En la figura 3.3 se muestra una figura de la Continuidad de Negocio

Figura 3.3 Continuidad de Negocio

FUENTE: http://www.sia.es/noticias/bcp.pdf

3.1.3 OBJETIVOS DEL BCP

Para la realización del Plan de Continuidad de Negocio para la empresa MEGADATOS S.A. es necesario establecer los objetivos que se desean alcanzar con dicho plan los cuales son los siguientes:

- Mantener el nivel de servicio

[15] MARTINEZ Juan Gaspar, PLANES DE CONTINGENCIA: La Continuidad del Negocio en la Organizaciones, Juan Gaspar Martinez, Ediciones Diaz Santos, S.A., 2004

- Establecer los tiempos máximos de inactividad de los activos de la empresa.
- Garantizar la reanudación de los servicios y procesos críticos en el menor tiempo posible, dentro de los tiempos tolerables.
- Proteger al personal y a los diferentes activos que se tiene en la empresa.
- Optimizar las acciones a realizar en caso de desastre.
- Reducir los efectos negativos producidos en el caso de que se dé una contingencia.
- Cumplir con requerimientos Legales / Contractuales /Gubernamentales
- Reducir al máximo los niveles de dependencia de personas o grupos específicos en el proceso de continuidad.
- Eliminar la necesidad de desarrollar nuevos procedimientos durante la contingencia.
- Minimizar la posibilidad de pérdida de información crítica para el negocio.

En otras palabras, este proyecto consiste en la realización de un análisis y estudio de las posibles vulnerabilidades que existen en la empresa, así como también los requerimientos necesarios para establecer una serie de procedimientos y estrategias para poder actuar en caso de que se presente alguna incidencia o algún desastre.

3.2 DESARROLLO DEL BCP

En este capítulo se va a desarrollar todo el Plan de Continuidad del Negocio. El desarrollo del Plan de Continuidad del Negocio se lo realizara en base a las fases descritas en la metodología de la norma BS25999 según el DRI (Disaster Reccovery Institute Internacional), las mismas que son:

1. Inicio y gestión del proyecto
2. Evaluación y Gestión de Riesgos
3. Análisis de Impacto del Negocio (BIA)
4. Desarrollo de Estrategias para la Continuidad del Negocio
5. Respuestas ante Emergencias

6. Desarrollo del BCP

En la figura 3.4 se indican las diferentes fases del BCP.

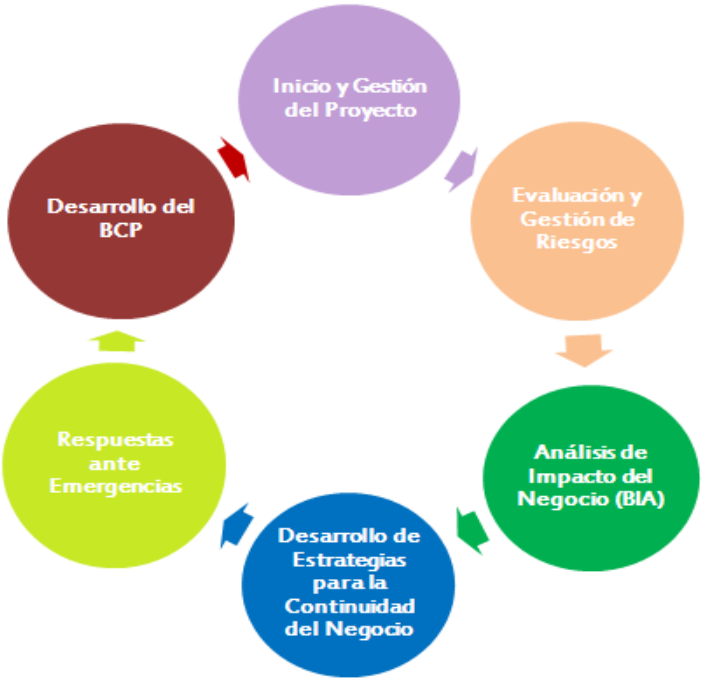


Figura 3.4 Fases del BCP

3.2.1 INICIO Y GESTIÓN DEL PROYECTO

La fase inicial del Plan de Continuidad del Negocio para la empresa MEGADATOS S.A., se basa principalmente en un proceso de concientización dirigido principalmente a las gerencias de MEGADATOS S.A., sobre la importancia de que la organización pueda responder ante incidentes e interrupciones que se presenten, los mismos que pueden afectar los servicios que brinda la MEGADATOS S.A. con el fin de que la empresa pueda continuar sus operaciones a un nivel aceptable para evitar el colapso total de la misma.

El encargado de realizar esta concientización será el Administrador de la Red Interna previo la autorización y aprobación del Gerente Nacional de Operaciones.

Después de realizar el proceso de concientización a las distintas gerencias y luego de considerar la importancia de la implementación de un Plan de Continuidad del Negocio en MEGADATOS S.A., es necesario la generación de un documento escrito y firmado por parte del Gerente General de MEGADATOS S.A., quien es la máxima autoridad de la empresa, donde se respalde la ejecución y elaboración del BCP.

En esta fase también se va a establecer un Comité responsable del BCP, este comité será el encargado de evaluar el BCP a lo largo de su desarrollo. Se describirá las responsabilidades que cada miembro va a tener y los recursos que van a necesarios durante la ejecución del BCP.

A continuación se listan todas las tareas que hay que realizar para poner en práctica el BCP.

1. Inicio y gestión del proyecto
    - Concientización
    - Formación del Comité Responsable
    - Definición de recursos necesarios
    - Revisión
2. Evaluación y Gestión de Riesgos
    - Caracterización del sistema
    - Identificación de amenazas
    - Identificación de la vulnerabilidad
    - Análisis de Controles
    - Determinación de la probabilidad
    - Análisis del Impacto
    - Determinación del Riesgo
    - Recomendaciones de control
    - Documentación de Resultados

- Revisión

3. Análisis de Impacto del Negocio (BIA)
    - Obtención de la relación de Procesos
    - Obtención de la relación de Aplicaciones
    - Relación de Departamentos y Usuario
    - Valoración de la Criticidad de los procesos
    - Periodo máximo de Interrupción
    - Revisión
4. Desarrollo de Estrategias para la Continuidad del Negocio
    - Elección de la Estrategia
    - Revisión
5. Respuestas ante Emergencias
    - Desarrollo de las Respuestas para emergencias
    - Revisión

3.2.1.1 Concientización

Es importante el desarrollo de un plan de continuidad de negocio ya que ninguna empresa u organización se encuentra exenta de algún desastre o de cualquier eventualidad que pueda causar un daño tal que pueda causar la quiebra o la paralización total de la organización.

El no poseer un Plan de Continuidad del Negocio pone en riesgo todos los activos de la empresa incluyendo el más importante como es la información, es por eso que se requiere realizar un análisis detallado de todos los activos de la empresa como son recurso humano, software, hardware, aplicaciones, etc.

La implementación de un Plan de Continuidad de Negocio basado en la norma BS 25999 brinda a las organizaciones, a sus clientes y a las diferentes partes interesadas la confianza en que sí se está preparado para responder ante situaciones calamitosas que afectan la prestación de servicios o el suministro de productos.

Para llevar a cabo la tarea de concientización, dentro de la empresa se van a dar charlas a todo el personal sobre la importancia del BCP, estas charlas deberán ser coordinadas previamente con cada Jefe de Área y con Recursos Humanos.

Los temas a tratar en estas charlas serán:

- Concepto del BCP.
- Importancia del BCP.
- Objetivos del BCP.
- Como se va a dessarollar el BCP en la empresa.
- Qué recursos materiales son necesarios.
- Qué personas están implicadas en el cumplimiento del plan.

Todo el personal de MEGADATOS S.A. debe conocer el Plan de Continuidad del Negocio y su respectiva función dentro de él, una vez se haya realizado su aprobación.

3.2.1.2 Autorización

Se obtiene la autorización de la Alta Gerencia, la misma que se plasma en una carta, en la misma se autoriza el desarrollo del Plan de Continuidad de Negocio para la empresa MEGADATOS S.A., esta carta se encuentra en el Anexo 2.

3.2.1.3 Formación Del Comité

Para el desarrollo de Plan de Continuidad del Negocio se va a definir un comité, los integrantes de dicho comité, serán los encargados de poner en práctica el Plan de Continuidad del Negocio que se va a desarrollar.

El comité contará con el apoyo del Gerente Nacional de Operaciones, él es quien va a definir el alcance, las pautas y va a ser el primero en evaluar el Plan de Continuidad del Negocio.

En la tabla 3.1 se puede observar la formación de dicho comité.

Tabla 3.1 Integrantes del Comité del BCP

ACTIVIDAD	RECURSO	DESCRIPCIÓN
Desarrollo del Plan de Continuidad del Negocio	Administrador de Red Interna.	Desarrolladores del BCP
Información y Apoyo dentro de MEGADATOS S.A.	Gerente Nacional de Operaciones	Revisión de BCP.
	Coordinador de Sistemas	Desarrollo y Administración de ERP´s
	Encargado del Sistema Eléctrico	Administrador y monitoreo del Sistema eléctrico

3.2.1.4 Definición de Recursos

En la tabla 3.2 se definen los recursos necesarios durante el desarrollo del Plan de Continuidad del Negocio.

Tabla 3.2: Recursos para la realización el BCP

TIPO	RECURSO
Materiales de Oficina	• Papel
Medios de Comunicación	• Correo • Teléfono • Internet • Intranet
Hardware	• 1 PC • 1 Laptop • 1 Impresora
Software	• Microsoft Office

3.2.2 EVALUACIÓN Y GESTIÓN DE RIESGO

En las secciones 2.1 y 2.2 se realizó el análisis y evaluación de riesgos.

Las tareas que se llevaron a cabo para el análisis y gestión el riesgo son:

- Caracterización del sistema
- Identificación de amenazas
- Identificación de la vulnerabilidad
- Análisis de Controles
- Determinación de la probabilidad
- Análisis del Impacto
- Determinación del Riesgo
- Recomendaciones de control
- Documentación de Resultados

En la tabla 3.3, la misma que es una copia de la tabla 2.13, se muestra un resumen del análisis de riesgos que se realizó en las secciones antes mencionadas.

Tabla 3.3: Resumen del análisis de riesgos

ACTIVOS	Riesgos Altos	Riesgos Medios	Riesgos Bajos
Servidores	--	10	23
Equipos de Redes y de Comunicación	--	6	27
Equipos de Escritorio	--	1	33
Laptops	--	3	30

Tabla 3.3: Resumen del Análisis de Riesgos (continuación)

ACTIVOS	Riesgos Altos	Riesgos Medios	Riesgos Bajos
Equipo Informático Computacional secundario	--	--	33
RR.HH.	--	2	5

Una vez que se ha realizado el análisis de riesgos con su respectiva matriz y revisando el resumen de la misma, se puede decir en general que los controles a implementar son los siguientes:

- Implementación de un sistema de entradas y salidas más actualizado y tecnificado debido a que el sistema actual está obsoleto y no permite dar los accesos necesarios y adecuados a cada empleado.
- Tener más cuidado con las diferentes personas que ingresan a las instalaciones de la empresa y velar por que cada usuario tenga su tarjeta de identificación para poderlo distinguir de una mejor manera.
- Establecer una política de etiquetación de activos.
- Revisión periódica de los sistemas eléctricos del edificio y de los equipos de backups que se tiene en la empresa.

3.2.3 ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

El Análisis de Impacto de Negocio se lo desarrollo en la sección 2.3.

Para la realización de Análisis de Impacto del Negocio se desarrolló las siguientes tareas:

- **Identificación de Procesos Críticos:** aquí se estableció los procesos críticos del negocio que se realizan en la compañía, así como también los responsables de cada uno de ellos.
- **Identificación de los Recursos que soportan a los procesos críticos:** en esta actividad se definieron los recursos de hardware y de software que soportan los procesos críticos de la compañía.
- **Identificación de Áreas y Usuarios responsables de los recursos que usan los procesos críticos:** en esta parte se identificó las áreas y las personas responsables y/o encargadas de los diferentes recursos que cada proceso crítico usa en la empresa.
- **Valoración de la Criticidad de los Procesos Críticos:** se estableció una valoración cuantitativa de acuerdo a las prioridades de cada proceso, en la tabla 2.15 y 2.16 se puede observar los rangos de criticidad establecidos.
- **Período Máximo de Interrupción:** se establecieron los tiempos de recuperación de cada proceso crítico, para el cálculo de estos tiempos se tomó en cuenta dos factores: el RPO y el RTO, en las tablas 2.17 y 2.18 se muestran los niveles de estos dos factores.

En las tablas 2.19, 2.20, 2.21, 2.22 y 2.13 se puede observar el análisis de Impacto del Negocio que se realizó por cada proceso crítico del negocio.

En base del análisis realizado en la sección 2.3 y evaluando los resultados obtenidos, se puede concluir lo siguiente:

- El proceso con mayor prioridad es el proceso de facturación el cual no puede estar fuera de servicio entre uno y dos días y los datos que se pueden perder son máximo de 3 días antes de la contingencia. Si este proceso llegar a caerse más del tiempo mencionado empezaría a causar pérdidas económicas en la empresa.
- El siguiente proceso importante es el de instalación y traslados, el cual no debe pasar caído más de tres días y los datos que se pueden perder son

datos de hasta tres días, es importante ya que su importancia radica en que el proceso de instalaciones y traslados es directamente proporcional a las ganancias que se genera en la empresa.

3.2.4 DESARROLLO DE ESTRATEGIAS PARA LA CONTINUIDAD DEL NEGOCIO

Una vez realizado el análisis de riesgos y el análisis del impacto del negocio, es necesario desarrollar las estrategias para la continuidad del negocio en caso de que, por efecto de una catástrofe o contingencia se paralicen uno o más procesos del negocio de la organización.

Las estrategias de recuperación son una serie de alternativas las cuales tienen como objetivo la recuperación de los recursos de la información entre las cuales se elige aquella que será aceptable en el coste de recuperación y razonable en el impacto que se determinó en el BIA.

Para ello, se contempla una serie de alternativas de instalaciones de procesamiento de datos (CPDs centro de procesamiento de datos), que se analizarán, y entre las cuales se elegirá una de ellas.

Centro de procesamiento de datos (CPD): un centro de procesamiento de datos es un conjunto de recursos físicos, lógicos y humanos necesarios para la realización, organización y control de las diferentes actividades informáticas y para tener acceso a la información que tiene la organización.

Entre los diferentes centros de procesamiento de datos tenemos los siguientes:

1. Hotsite
2. Warmsite
3. Coldsite
4. Mirrorsite
5. Sitios móviles

6. Acuerdos recíprocos con otras organizaciones

3.2.4.1 ALTERNATIVAS DE RECUPERACIÓN

Las estrategias de recuperación que vamos a ver a continuación serán usadas solo en casos de desastres en los sistemas y que su recuperación sea de larga duración, y que este acontecimiento afecte a las funciones o procesos fundamentales de la empresa.

Hotsite

Es una segunda ubicación de procesamiento que está configurado y suficientemente actualizado pudiendo incluir si se desea hasta personal alterno, para poder restaurar los servicios correctamente en tan sólo unos pocos segundos o minutos después de la ocurrencia de la interrupción de dichos servicios.

Los costes son elevados, es la opción más costosa, pero permiten alcanzar los tiempos establecidos en el Análisis de Impacto del Negocio.

Los costes podrían ser:

- Coste básico de suspensión
- Cuotas mensuales
- Cargos de pruebas
- Costes de activación (emergencia real)
- Cargos por uso por hora o por día (dependencia del proveedor)

Warmsite

Es una segunda ubicación de procesamiento, con una configuración adecuada pero que no está suficientemente actualizada como para poder restaurar los servicios sin perder datos. Por tanto, sería necesaria una actualización antes de proceder a una restauración de los servicios en este centro de procesamiento.

Los costes son elevados, pero menores que el Hotsite, ya que el mantenimiento y las pruebas se realizan con menor frecuencia.

Coldsite

Es una segunda ubicación que contiene los elementos físicos para establecer un centro de procesamiento si fuera necesario (cableado eléctrico, aire acondicionado, etc.), pero que no contiene ni las maquinas ni los componentes de hardware necesarios para poder levantar los servicios en caso de desastre, es decir no está adecuada para operar.

Para poner a operar esta ubicación se debe realizar un gran esfuerzo, por lo cual se va a necesitar una cantidad de tiempo bastante considerable.

Los costes serian netamente inferiores a los costes para las estrategias anteriores. Son la opción más económica de todas.

Mirrorsite

Es una segunda ubicación con los recursos necesarios, correctamente configurados y actualizados, donde se realizan las distintas transacciones de cada servicio en paralelo con el centro de procesamiento principal.

Esta alternativa supone la necesidad de realizar pruebas periódicas que garanticen la sincronía entre el centro principal y el de respaldo. Debe existir también una correspondencia equitativa de capacidad de trabajo entre ambos centros.

Se trata de una alternativa muy costosa, además de ser muy necesario el uso de recursos informáticos y de personal que garantice la viabilidad de este método.

Sitios móviles

Es una segunda ubicación móvil, por ejemplo un remolque, que contiene los elementos necesarios para instalar un centro de procesamiento alternativo.

Pueden ser útiles en caso de desastre expandido para construir áreas de trabajo donde situar PC´s y terminales de trabajo.

A continuación en la tabla xx se indica una comparación entre los 5 sitios antes mencionados

Tabla 3.4: Comparación de las Estrategias de Recuperación

SITIO	COSTO	HARDWARE	TELECOMUNICACIONES	TIEMPO	LOCALIZACION
Hotsite	Alto	Completo	Parcial	Corto	Fijo
Warmsite	Medio	Parcial	Parcial	Medio	Fijo
Coldsite	Bajo	No	Ninguno	Largo	Fijo
Mirrorsite	Muy Alto	Completo	Completo	Minimo	Fijo
Sitio Movil	Alto	Variable	Variable	Variable	No Fijo

FUENTE:http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_PLAN_RECUPERACION_ANTE_DESASTRES_DRP.pdf

Acuerdos recíprocos con otras organizaciones

Son acuerdos suscritos con otras organizaciones (normalmente cuyas sedes se encuentran cerca geográficamente) para proveerse mutuamente de tiempo de CPU e incluso de espacio para poder instalar a algunos trabajadores de forma temporal después de una catástrofe.

Este método supone una dificultad de conseguir una configuración y actualización adecuadas para poder reanudar los servicios críticos al poco tiempo de producirse dicho desastre.

El coste de esta alternativa sería el más bajo de todas las alternativas vistas anteriormente.

Almacenamiento en nube

El Almacenamiento en nube o Cloud Storage es un modelo de almacenamiento empresarial en red, este tipo de almacenamiento fue ideado en los años 1960, aquí

los datos de encuentran alojados o se alojan en espacios de almacenamiento virtualizados y por lo general están alojados por terceros.

Las compañías que brindan el servicio de alojamiento operan grandes centros de procesamiento de datos y los usuarios que requieren de este servicio compran o alquilan la capacidad de almacenamiento que requieran. En el fondo lo que los centros de procesamiento de datos hacen es virtualizar los recursos de acuerdo a los requerimientos que el cliente necesite, y solo muestran o exhiben los entornos con los recursos solicitados y es el cliente quien administra el almacenamiento y funcionamiento de archivos, datos y/o aplicaciones. Físicamente el recurso puede estar o extenderse a lo largo de varios servidores y estar en múltiples sitios, además es responsabilidad de las empresas de alojamiento la seguridad de los archivos.

El acceso a los servicios de almacenamiento en la nube se los puede hacer de algunas formas y medios, pude ser a través de una interfaz de programación de aplicaciones de servicios web (API), interface web de usuario o alguna otra seleccionada por el cliente.

Servicios en la Nuibe

Al hablar de servicios en la nube se puede elegir entre tres opciones o modelos de servicio que brinda, los cuales son:

1. SaaS (Software as a Service)
2. PaaS (Platform as a Service)
3. IaaS (Infraestructures as a Service)

- **SaaS o Software as a Service:** el cliente que opte por este tipo de servicio podrá hacer uso de las aplicaciones que contrate al proveedor. Es decir, si cierta empresa contrata una aplicación de correo para cierto número de empleados, la aplicación no podrá ser modificada por la empresa ni por los usuarios a excepción de posibles configuraciones de usuario o

personalizaciones que le permita el proveedor. En este tipo de servicio el usuario no tiene ningún control de las aplicaciones.

- **PaaS o Platform as a Service:** en este tipo de servicio el cliente estará contratando un servicio el cual le permite alojar y desarrollar sus propias aplicaciones en una plataforma que dispone de herramientas de desarrollo para que el usuario pueda elaborar la solución que necesite. En este modelo el proveedor ofrece el uso de su plataforma que a su vez se encuentra alojada en sus infraestructuras. Por lo que el usuario no tiene control sobre la plataforma ni las infraestructuras pero si sobre sus aplicaciones.
- **IaaS o Infraestructures as a Service**: aquí el cliente estará contratando únicamente las infraestructuras tecnológicas (capacidad de procesamiento, de almacenamiento y / o de comunicaciones). Sobre dicha IaaS alojará él sus aplicaciones y plataformas; sobre estas últimas tendrá él el control pero no sobre las infraestructuras.

  Un cliente puede adoptar uno o más de estos modelos según sus necesidades. La decisión vendrá condicionada por dónde desea centrar sus esfuerzos y expertise: en las aplicaciones, en las plataformas y/o en las infraestructuras tecnológicas. Qué elementos le aportan valor a su negocio y por lo tanto quiere seguir implicado más de cerca en su evolución y cuales no le suponen un valor diferencial y prefiere contratar a un proveedor especializado.

3.2.4.2 ESTRATEGIA DE RECUPERACIÓN ELEGIDA

Una vez que se analizaron las diferentes alternativas de recuperación se llegó a la conclusión de que la mejor estrategia de recuperación es la de hacer uso de los convenios que se tiene con la empresa aliada que es TELCONET.

La estrategia elegida es la de “Acuerdos Recíprocos entre organizaciones”; el haber elegido esta estrategia se debe a que el costo de este tipo de CPD es el más barato para nuestra empresa y también porque se debe aprovechar la alianza estratégica

que se tiene con la empresa aliada “TELCONET”. Pues dicho acuerdo permite compartir los diferentes recursos que se tienen en las 2 empresas como son: recurso de Hardware de Software y de RR.HH.

Las ventajas que se tiene al elegir esta estrategia son:

- Menor costo: esto en cuanto a que se comparte el know how del recursos humano que se tiene entre las 2 empresa.
- Se albergan equipos en otras ciudades, como en Guayaquil pues nuestra empresa aliada tiene su Data Center en dicha ciudad, esto es muy bueno para la empresa pues en caso de que llegue a pasar algo en la ciudad local a los equipos que tenemos hospedados ahí, no les pasaría nada.

Las desventajas que se pueden tener serian:

- Generalmente no es exigible: muchas de las veces, solo se utiliza la capacidad de procesamiento sobrante de la otra parte del acuerdo.
- Las diferencias en la configuración del equipo de la otra parte, normalmente, exige cambios a programas a fin de operar eficazmente.

3.2.5 RESPUESTAS ANTE EMERGENCIAS

Luego de haber elegido la estrategia de recuperación para casos de desastres de larga duración, es necesario diseñar una serie de procedimientos de cómo se debe actuar para las situaciones de contingencia.

Para cada situación de contingencia se describirán las medidas o pasos a seguir para proceder a la restauración de sistema.

Se distinguen las siguientes situaciones de contingencia:

1. Fallo de Hardware (sin daños a la información)
2. Dañado o borrado lógico de la configuración

3. Dañado o borrado de software
4. Destrucción total de alguno de los sistemas.
5. Problemas de energía eléctrica

3.2.5.1 FALLO DE HARDWARE (SIN DAÑOS A LA INFORMACIÓN)

Se va a describir el procedimiento a seguir en caso de avería o destrucción de los siguientes equipos de hardware:

- Servidores
- Switch
- Router
- Equipos Inalámbricos

El procedimiento a seguir debe ser el siguiente:

1. Se notifica al responsable de los equipos (Departamento de Soporte de MEGADATOS S.A.)
2. El Departamento de Soporte revisará el equipo para determinar el tipo y gravedad del daño.
3. Se verifica si el equipo está en garantía
    a. Si el equipo está en garantía o tiene algún acuerdo suscrito de soporte se notifica al proveedor sobre daño de dicho equipo.
    b. Si el equipo no está en garantía, el Departamento de Soporte procederá a comprar la parte que se necesite o se lo transfiere al proveedor para su reparación (con costo) lo más rápido como le sea posible.
4. Si el tiempo de la sustitución o reparación de equipo o de la parte del equipo es muy largo, se procede a la sustitución del equipo por otro que esté disponible, siempre y cuando sea posible.

Nota: En el caso de que uno de los daños se dé en alguno de los equipos de los que los Administra el Departamento de Sistemas de la empresa aliada

TELCONET, se notificará inmediatamente a dicho departamento y ellos procederán de acuerdo a su método de recuperación.

3.2.5.2 DAÑADO O BORRADO LÓGICO DE LA CONFIGURACIÓN

A continuación se va a describir el procedimiento a seguir en caso de que los activos que se mencionaron anteriormente resulten dañados o con sus configuraciones modificadas.

1. Se notifica al responsable de los equipos, Departamento de Soporte de MEGADATOS S.A.
2. Se valora que tan grave es el daño y que porcentaje de información se ha perdido, y si se puede realizar una replicación de las configuraciones iniciales.
3. Se procede a revisar si se tiene los respaldos necesarios para realizar una replicación de los datos o de las base de datos dependiendo de la información que se perdió.
4. Si se tiene los respaldos necesarios y con la aprobación del Departamento de Soporte se procede a realizar dicho proceso.
5. Se valida si la dicho proceso requiere una parada en producción del equipo:
    a. Sí se requiere una parada en la producción, se notifica a los usuarios sobre el servicio que será detenido y la duración que tomará dicho proceso.
    b. Caso contrario se realiza la replicación en caliente.
6. Una vez que se ha acabado de realizar el proceso de la copia o replicación, se verifica y se comprueba que este proceso ha obtenido los resultados deseados es decir que la copia o la réplica se ha realizado correctamente.
7. Se procede a realizar las pruebas respectivas para verificar que todo esté funcionando correctamente.
    a. Si todo se encuentra correcto, se guardan los cambios realizados y se pone en producción nuevamente al equipo
    b. De lo contrario se da marcha atrás, volviendo al estado anterior del comienzo del proceso de copia o de replicación. El proceso quedara en

espera o cancelado dependiendo de la decisión del Departamento de Soporte. Finalmente se procede a llamar a expertos en el tema, dependiendo del equipo que tuvo el problema.

3.2.5.3 DAÑADO O BORRADO DE SOFTWARE

Para el caso de dañado borrado de software, se describen aquellos procesos que serían necesarios realizar en caso de que existan daños más o menos graves en las aplicaciones o en el sistema operativo de las maquinas o de los servidores de la organización.

Se van a diferenciar los siguientes casos, cada uno va a tener un tratamiento diferente:

- **Daño o borrado en el software de aplicación de un computador de un técnico**
    1. Se notifica del daño o de la aplicación borrada al Departamento de Soporte (Helpdesk)
    2. Dicho departamento procederá a revisar e instalar el Software borrado o dañado.
    3. Se realizan las pruebas de que dicho software funcione correctamente y se entrega el computador al técnico.

- **Daño o borrado del Sistema Operativo de un computador de un técnico**

    Si se trata de daños en el sistema operativo de un computador de un técnico se seguirá el siguiente procedimiento:

    1. Se comunica al Departamento de Soporte (Helpdesk).
    2. Se valora la gravedad de los daños y se verifica si es posible la recuperación del Sistema Operativo.

a. Si es posible se procede a realizar la reparación o recuperación del Sistema Operativo
b. Si no es posible realizar la recuperación del Sistema Operativo, si el daño es muy grave (no se puede iniciar el sistema operativo) se realizará las siguientes acciones:
    i. Se realiza un respaldo de la información del disco de ser posible.
    ii. Se procede al formateo de los discos duros del PC.
    iii. Posteriormente, se realiza la copia de la información respaldada y se procede a la instalación de todas las aplicaciones que necesite el técnico.

- **Daño o borrado del software de aplicación de uno de los servidores**

Los pasos a seguir en estos casos son:

1. Se comunicará al Departamento de Soporte.
2. Dicho Departamento procederá a instalar o reinstalar los productos o aplicaciones necesarias en el servidor.

Cabe recalcar que en la empresa no se cuenta con una política de respaldos de servidores, el único servidor que tiene respaldo es el servidor de correo.

En el caso del servidor de correo el procedimiento a seguir seria solamente iniciar el servidor de respaldo, el mismo que esta virtualizado en el BLADE.

- **Daño o borrado del Sistema Operativo en uno de los servidores**

Los procedimientos a seguir en caso de fallo del sistema operativo en alguno de los servidores es el siguiente:

1. Se notifica al Departamento de soporte.

2. Se intenta la recuperación del Sistema operativo. Si el daño es suficientemente grave (no se puede iniciar el sistema operativo) se procede de la siguiente manera:
    a. En caso de ser el servidor de correo o el BLADE, se procede a notificar a las empresas que nos brindan soporte con dichos servidores.
        i. Se esperara a los técnicos y se supervisara el proceso de recuperación.
        ii. Una vez que el proceso termine se verifica que todo funcione correctamente.
    b. Si se trata de los demás servidores se procede a realizar un respaldo de toda la información del disco duro del servidor, de ser posible se respalda las configuraciones de los diferentes programas instalados.
    c. Se procede al formateo del disco duro del Servidor.
    d. Posteriormente, se realiza la instalación de todas las aplicaciones teniendo en cuenta las configuraciones anteriores.
3. Se pone en marcha el servidor y se verifica su correcto funcionamiento.

Nota: En el caso de que sea uno de los servidores de TELCONET, el Departamento de Sistemas de dicha empresa será el responsable de realizar todo el procedimiento que sea necesario para la recuperación del servidor que se encuentre dañado.

3.2.5.4 DESTRUCCIÓN TOTAL DE ALGUNO DE LOS SISTEMAS.

Los servidores que se pueden ver afectados son los siguientes:

- Servidor de Archivos
- Servidor de Máquinas Virtuales
- Servidor de Diagramas de Red
- Servidor de Antivirus
- Servidor de Correo

- Servidor de Pagina de Calidad
- Firewall
- Servidor BLADE
- Servidor de Monitoreo TN
- Servidor de Monitoreo TN 2

A continuación se describe el procedimiento a seguir en caso de que alguno de los servidores esté gravemente dañado, sin posibilidad de arranque.

1. Se notificara al departamento de Soporte de MEGADATOS S.A..
2. Se procede a verificar la documentación que se tiene y se verifica si se tienen respaldos de configuraciones, de bases de datos, etc.
3. Se procede a preparar un nuevo servidor, tratando en lo que sea posible de instalar las mismas versiones de SW y con las mismas aplicaciones que se tenía.
4. Luego se procederá a configurar nuevamente el servidor usando los respaldos que se tenía.
5. Se pone en marcha el nuevo servidor y se verifica que esté funcionando correctamente y se realizan las pruebas necesarias para descartar cualquier error que se pudiera tener si se pone a producción dicho servidor.
6. Luego de realizar las pruebas y si todo funciona correctamente se pondrá en producción el nuevo servidor.

3.2.5.5 PROBLEMAS DE ENERGÍA ELÉCTRICA

En MEGADATOS S.A. se tiene los siguientes UPS:

1. UPS FERRUPS 18KVA FERRORESONANTE (Banco externo de baterías 12Vdc/75Ah)
2. UPS FERRUP 10KVA FERRORESONANTE(Banco externo de baterías 12Vdc/75Ah)

Estos UPS distribuyen la energía eléctrica desde el Subsuelo 3 hasta el Piso 8 a través de 2 tableros independientes para alimentar a los *racks* en el TELEPUERTO.

La carga eléctrica está distribuida entre ambos UPS y señalizado en cada rack a que UPS se conectaran.

El Ing. Eléctrico encargado que pertenece a la empresa aliada TELCONET se encargara de aprobar el ingreso o retiro de cualquier equipo que forma parte de la infraestructura de energía eléctrica.

El TELEPUERTO consta de 2 sistemas de energía eléctrica, por seguridad de los equipos:

1. Alimentación de energía eléctrica a través de la red eléctrica suministrada por la Empresa Eléctrica Quito, la cual se conecta a un tablero de transferencia y luego a los UPS.
2. Alimentación de energía eléctrica a través de un generador de 75KW de propiedad del Edificio Torres del Puente, el cual ingresa en operación 2 minutos. luego de cualquier corte de energía. Esto se debe a que el tablero de transferencia tiene un PLC (controlador lógico programable), el cual conmuta automáticamente en caso de cortes de energía y activa el funcionamiento del generador generando la energía inmediatamente conmutándola hacia los UPS.

En el caso de que el daño sea masivo y de que no funcionen los UPS se seguirán las siguientes acciones:

1. El monitoreo del TELEPUERTO Quito se lo realiza a través del IP Contac Center de TELCONET el cual opera en la modalidad de 24x7 (24 horas x 7 días)
2. En caso de falla en la parte eléctrica se notificará al encargado de las conexiones eléctricas. Ing. Eléctrico (Jefe Eléctrico).
3. Se revisa los equipos y se verifica en donde y por qué se produjo la falla.

4. Se procede a reparar la falla si fuera el caso en el UPS o en el generador.
5. Una vez que se haya solventado el problema eléctrico, el Departamento de Soporte procederá a revisar que todos los equipos tanto de redes y comunicación, así como los servidores se encuentren funcionando correctamente.
6. El informe será entregado por el IP Contac Center de acuerdo a la información que entregue el Ing. Electrico (Jefe Eléctrico)

El tiempo de respaldo de los UPS es 15 minutos, actualmente están con una carga del 70% cada uno de ellos.

El tiempo de respaldo del generador es 8 horas con tanque lleno de diesel. (La Administración del generador está a cargo del Edificio)

3.2.6 CRONOGRAMA DE IMPLANTACIÓN DEL BCP

La implementación del Plan de Continuidad de Negocio será ejecutada de acuerdo con las necesidades de la empresa, es decir el plan no será aplicado de forma inmediata por la empresa MEGADATOS S.A., por tal razón se procede a realizar dentro del presente capitulo un cronograma donde se describen todas y cada una de las actividades que se deben realizar para la implantación del plan propuesto.

Las actividades descritas serán las que se deben poner en práctica en caso de que la empresa decida implementar el mencionado plan.

En la tabla 3.4, se muestra las actividades con los tiempos de cada una y con los responsables de las mismas.

Tabla 3.4 Cronograma de implantación del BCP

TAREAS	DURACIÓN	RESPONSABLES
DESARROLLO DEL BCP	**200 horas**	
Inicio y gestión del proyecto	**32 horas**	
Concientización	8 horas	Administrador de Red Interna
Formación del Comité Responsable	8 horas	Administrador de Red Interna
Definición de recursos necesarios	8 horas	Administrador de Red Interna
Revisión	8 horas	Gerente Nacional de Operaciones, Administrador de Red Interna
Evaluación y Gestión de Riesgos	**88 horas**	
Caracterización del sistema	8 horas	Administrador de Red Interna
Identificación de amenazas	8 horas	Administrador de Red Interna
Identificación de la vulnerabilidad	8 horas	Administrador de Red Interna
Análisis de Controles	8 horas	Administrador de Red Interna
Determinación de la probabilidad	8 horas	Administrador de Red Interna
Análisis del Impacto	8 horas	Administrador de Red Interna
Determinación del Riesgo	8 horas	Administrador de Red Interna
Recomendaciones de control	8 horas	Administrador de Red Interna
Documentación de Resultados	16 horas	Administrador de Red Interna
Revisión	8 horas	Gerente Nacional de Operaciones, Administrador de Red Interna
Análisis de Impacto del Negocio (BIA)	**48 horas**	
Obtención de la relación de Procesos	8 horas	Administrador de Red Interna
Obtención de la relación de Aplicaciones	8 horas	Administrador de Red Interna
Relación de Departamentos y Usuario	8 horas	Administrador de Red Interna
Valoración de la Criticidad de los procesos	8 horas	Administrador de Red Interna
Periodo máximo de Interrupción	8 horas	Administrador de Red Interna

Tabla 3.5 Cronograma de implantación del BCP (continuación)

TAREAS	DURACIÓN	RESPONSABLES
Revisión	8 horas	Gerente Nacional de Operaciones, Administrador de Red Interna
Desarrollo de Estrategias para la Continuidad del Negocio	**16 horas**	
Elección de la Estrategia	8 horas	Administrador de Red Interna
Revisión	8 horas	Gerente Nacional de Operaciones, Encargado de Sistema Eléctrico, Administrador de Red Interna
Respuestas ante Emergencias	**16 horas**	
Desarrollo de las Respuestas para emergencias	8 horas	Administrador de Red Interna
Revisión	8 horas	Gerente Nacional de Operaciones, Encargado de Sistema Eléctrico, Administrador de Red Interna

4 EVALUACIÓN DE LA APLICABILIDAD DEL BCP

Es importante realizar un análisis de la aplicabilidad del BCP, de esta forma se podrá saber el costo y/o inversión de la implementación del mismo y si es aplicable de acuerdo a la leyes que están rigiendo actualmente en el país y en el caso de ponerlo en práctica cual serian el recurso humano que se necesitaría para poder aplicarlo.

Por este motivo se va a realizar una evaluación de la aplicabilidad del BCP desde tres aspectos diferentes como son:

- En el aspecto económico
- En el aspecto legal
- En el aspecto organizacional

4.1 EN EL ASPECTO ECONÓMICO

Para realizar la evaluación en este aspecto se establecerá el recurso humano que llevaría a cabo la implementación del Plan, el costo por hora de cada recurso y el número de horas que se necesiten para la implementación del BCP, también se va a tomar en cuenta los recursos de hardware y de oficina que se utilicen para poder realizar dicho plan.

La evaluación se va a llevar a cabo bajo las siguientes consideraciones:

- La implementación del BCP se lo realizará fuera del horario laborable.
- Se va a trabajar 2 horas diarias por fuera del horario laboral.
- El costo de los recursos de hardware y de papelería será de acuerdo a lo que le cuesta a la empresa.

Es importante saber cuánto necesita la empresa invertir en la implementación del BCP.

Los involucrados en la implementación del BCP se indican en la tabla 4.1

Tabla 4.1: Involucrados en la Implementación del BCP

Nombre	Costo x hora
Gerente Nacional de Operaciones	$ 7,50
Administrador de Red Interna	$ 5,50
Encargado de Sistema Eléctrico	$ 6,00

En la tabla 3.4 se realizó la calendarización de la implementación del Plan de Continuidad de Negocio, en el mismo se describieron las diferentes actividades que se debe llevar a cabo y los encargados de cada actividad, en la calendarización anteriormente realizada se determinó que para la realización del plan se necesitan 200 horas.

Como se mencionó anteriormente, se va a trabajar 2 horas diarias en este proyecto, en base a esto dentro de la tabla 4.2 se describe el costo del recurso humano que va a realizar la implementación de acuerdo al número de horas que se indica en la tabla 3.4 que cada involucrado va a trabajar.

Tabla 4.2: Costo de RR.HH. en la implementación del BCP

EMPLEADO	TIEMPO (H)	COSTO HORA	TOTAL
Gerente Nacional de Operaciones,	40	$ 7,5	$ 300
Encargado de Sistema Eléctrico	16	$ 6	$ 96
Administrador de Red Interna	200	$ 5,5	$ 1100
		Total Costo	**$ 1496**

Para la implementación del Plan de Continuidad de Negocio se necesitara los siguientes recursos de hardware y papelería.

- Laptop con acceso a Internet y con Office
- Impresiones blanco y negro y a color.

Tabla 4.3: Costo de recurso de HW y papelería

RECURSO	COSTO	# DE HORAS Y HOJAS	TOTAL ($)
Laptop	0.25ctv. x hora	200 horas	$ 50
Impresión color	0.10 ctvs. x hoja	50	$ 5
Impresión blanco y negro	0.03 ctvs. x hoja	300	$ 9
		Total Costo	$ 64

El costo total que se necesita para la implementación del BCP se sacara con la siguiente formula:

Costo total = Costo de RR.HH. + Costo de recurso de HW y Papeleria

Costo total = $ 1496 + $ 64

Costo Total = $ 1563

CONCLUSIÓN

MEGADATOS S.A. requiere una inversión de $ 1563 dólares americanos para implementar el Plan de Continuidad de Negocio.

La empresa cuenta con estos recursos económicos y también se cuenta con la aprobación de las autoridades por lo que el Plan de Continuidad de Negocio es aplicable en el aspecto económico.

4.2 EN EL ASPECTO LEGAL

Se va a revisar las leyes y/o reglamentos bajo los cuales la empresa se encuentra regida. Se va a enunciar los artículos competentes al desarrollo del Plan de Continuidad del Negocio.

REGLAMENTO GENERAL A LA LEY ESPECIAL DE TELECOMUNICACIONES REFORMADA

Artículo 76. El contrato de concesión como mínimo deberá contener:

i) Potestad del Estado de revocar la concesión cuando el servicio no sea prestado de acuerdo con los términos del contrato y a asumir su prestación expresamente para mantener la continuidad de los servicios públicos de telecomunicaciones;

Artículo 77. El contrato de concesión podrá ser renovado de conformidad con lo estipulado en dicho instrumento, a solicitud del concesionario.

De no renovarse la concesión, el CONATEL tomará las medidas pertinentes para asegurar la continuidad de los servicios concesionados.

La renegociación de los contratos de concesión se iniciará con por lo menos cinco años de anticipación a la terminación del mismo. Para el caso de que las partes no se hayan puesto de acuerdo en los términos de la renegociación en el plazo de dos años, el CONATEL convocará a un procedimiento público competitivo en el cual podrá participar el concesionario saliente.

El valor que deberá cancelar el nuevo adjudicatario de la concesión al saliente por los activos tangibles e intangibles será determinado por una firma evaluadora de

reconocido prestigio y experiencia en el sector de telecomunicaciones. Antes de la terminación de la concesión, el concesionario saliente, a su costo, procederá a contratar a la firma evaluadora antes mencionada mediante concurso público. El valor determinado por la firma evaluadora servirá como base para la licitación de la nueva concesión, monto que se le entregará al concesionario saliente por la transferencia de los bienes tangibles e intangibles al nuevo concesionario, en caso de que el concesionario saliente no fuese el nuevo adjudicatario.

En los casos de terminación anticipada del plazo de vigencia del título habilitante, para cumplir con la continuidad del servicio, el Estado intervendrá a través del organismo competente. El tratamiento de los activos del concesionario saliente deberá observar el mismo procedimiento previsto en la terminación de la concesión por cumplimiento del plazo.

REGLAMENTO DE ABONADOS

Que, el artículo 39 de la Ley Especial de Telecomunicaciones y sus reformas, establece que todo usuario tiene derecho a recibir el servicio en las condiciones contractuales estipuladas con el proveedor de servicio, y a que dichas condiciones no sean modificadas unilateralmente sin su consentimiento, salvo por fuerza mayor, a ser indemnizados por el incumplimiento a dichos términos contractuales por parte del proveedor del servicio, garantizando el Estado el derecho al secreto y a la privacidad del contenido de las telecomunicaciones y quedando prohibido interceptar, interferir, publicar o divulgar sin consentimiento previo de las partes la información cursada mediante los servicios de telecomunicaciones, bajo las sanciones previstas en la ley para la violación de correspondencia. Los operadores de redes y proveedores de servicios deberán adoptar las medidas necesarias, técnica y económicamente aceptables, para garantizar la inviolabilidad de las telecomunicaciones. El Estado determinara, a través del reglamento de la ley, los mecanismos para que los derechos de los usuarios sean garantizados y satisfechos, incluyendo las modalidades para la solución de reclamos, mediante procedimientos arbitrales o de medición, sin perjuicio de lo establecido en la Ley de Defensa del

Consumidor y el Usuario. Además, las tarifas reflejarán los costos de eficiencia basados en los parámetros internacionales y se facturaran por tiempo efectivo de uso, establecido en horas, minutos y segundos, según corresponda. Los ajustes tarifarios se realizaran de manera gradual.

Que, el artículo 88 del Reglamento General a la Ley Especial de Telecomunicaciones Reformada, en las letras b, c y d señala que corresponde al CONATEL regular la prestación de los servicios de telecomunicaciones y dictar las medidas necesarias para que los servicios de telecomunicaciones se presten con niveles apropiados de calidad y eficiencia, así como el dictar normas para la protección de los derechos de los prestadores de servicios de telecomunicaciones y usuarios.

Artículo 16.- Condiciones Contractuales

16.5 A que se mantengan las condiciones de prestación de servicios, conforme los establecidos en los contratos; los cambios unilaterales en los contratos de prestación de servicios, se considerarán como nulos y no tendrán ningún valor.

16.7 Recibir los servicios contratados conforme las obligaciones relativas a calidad que deben ser cumplidas por el prestador del servicio.

Artículo 18.- Atención y reclamos

18.1 Presentar quejas y reclamos a los prestadores de servicios por fallas en la prestación de los servicios contratados, que pueden ser relacionados con la calidad del servicio, atención en el servicio y trato al abonado/cliente-usuario, facturación, suspensión y reactivación del servicio, reparaciones, averías y demás aspectos relacionados con la prestación del servicio.

18.4 Presentar sus quejas, recursos y reclamos ante los organismos competentes, por incumplimientos y la prestación deficiente de servicios.

CONCLUSIÓN

El desarrollo del Plan de Continuidad de Negocio no afecta a ninguno de los artículos anteriormente mencionados, por el contrario ayudará a que se cumpla lo estipulado en los artículos mencionados.

4.3 EN EL ASPECTO ORGANIZACIONAL

Aquí se va a definir el recurso humano que se necesitará para la implementación del plan, se va a analizar si en la empresa existe el RR.HH. necesario para llevar a cabo la implementación y de no ser así se propondrá cuales profesionales deberán ser las personas encargadas de la implementación del mismo.

Dentro de la empresa MEGADATOS S.A. existen creadas brigadas de emergencia, las mismas que ayudan en algunos aspectos dentro de la empresa. Cada brigada está conformada por 5 integrantes y estos integrantes son afines a la rama de cada brigada.

Las brigadas de emergencia que se tiene en la empresa son:

- Incendios
- Primeros Auxilios
- Contingencia
- Comunicación
- Evacuación

La brigada de “contingencia” es la que se encarga de desarrollar los diferentes procedimientos en caso de darse alguna contingencia en la empresa.

CONCLUSIÓN

Actualmente la empresa cuenta con el recurso necesario para la implementación del Plan de Continuidad de Negocio, por tal motivo no se necesita contratar personal

adicional al existente, en caso de que alguno de los involucrados llegara a faltar por algún motivo, los que podrían hacer este trabajo serían los miembros de la brigada de “contingencia”.

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

En base del análisis realizado para el desarrollo del proyecto, se puede obtener las siguientes conclusiones:

- El Plan de Continuidad de Negocio se ha desarrollado para que pueda cubrir las situaciones de contingencia probables que puedan darse dentro de la empresa.
- El planteamiento de las situaciones de contingencia servirá para determinar cuáles son las alternativas viables de recuperación.
- El tener conocimiento de los posibles riesgos a los que puede estar expuesta la empresa y el contar con las estrategias para minimizar los mismos, permite aplicar medidas correctivas para de esta manera evitar pérdida de dinero y evitar que estos riesgos lleguen a materializarse.
- El que la empresa posea un Plan de Continuidad de Negocio aporta mayor confianza dentro de la misma, puesto que esto evita que se hagan improvisaciones, las cuales pueden afectar incluso más que el propio incidente que llegue a darse.
- Se estableció cuáles son los procesos críticos del negocios que deben ser recuperados de forma inmediata y cuáles pueden ser recuperados en un periodo de tiempo más prolongado.
- El Plan de Continuidad que se desarrolló proporciona una respuesta rápida y apropiada ante cualquier incidente imprevisto, lo cual hace que se reduzca el impacto en situaciones de trabajo.

5.2 RECOMENDACIONES

- Tomar conciencia de la necesidad de un plan de continuidad del negocio, puesto que este ayuda a la reanudación de la operación en caso de que ocurra una contingencia.
- Determinar cuánto se necesita invertir para recuperarse ante un desastre asi como determinar el máximo tiempo de inactividad tolerable ante las diferentes situaciones de contingencia.
- Mantener actualizado el plan, revisarlo periódicamente para contemplar los cambios que se hayan producido en la empresa, y probar la eficacia del plan diseñado. Se recomienda a la Alta Dirección de la empresa colocar fechas para la revisión.
- Comprometer a los directivos para definir un equipo que mantenga actualizado el plan y pueda cubrir las necesidades que se vayan incorporando, el equipo determinado tendrá la responsabilidad de repetir la última fase del plan: actualizar y probar, sólo así podrán confiar en su eficacia.

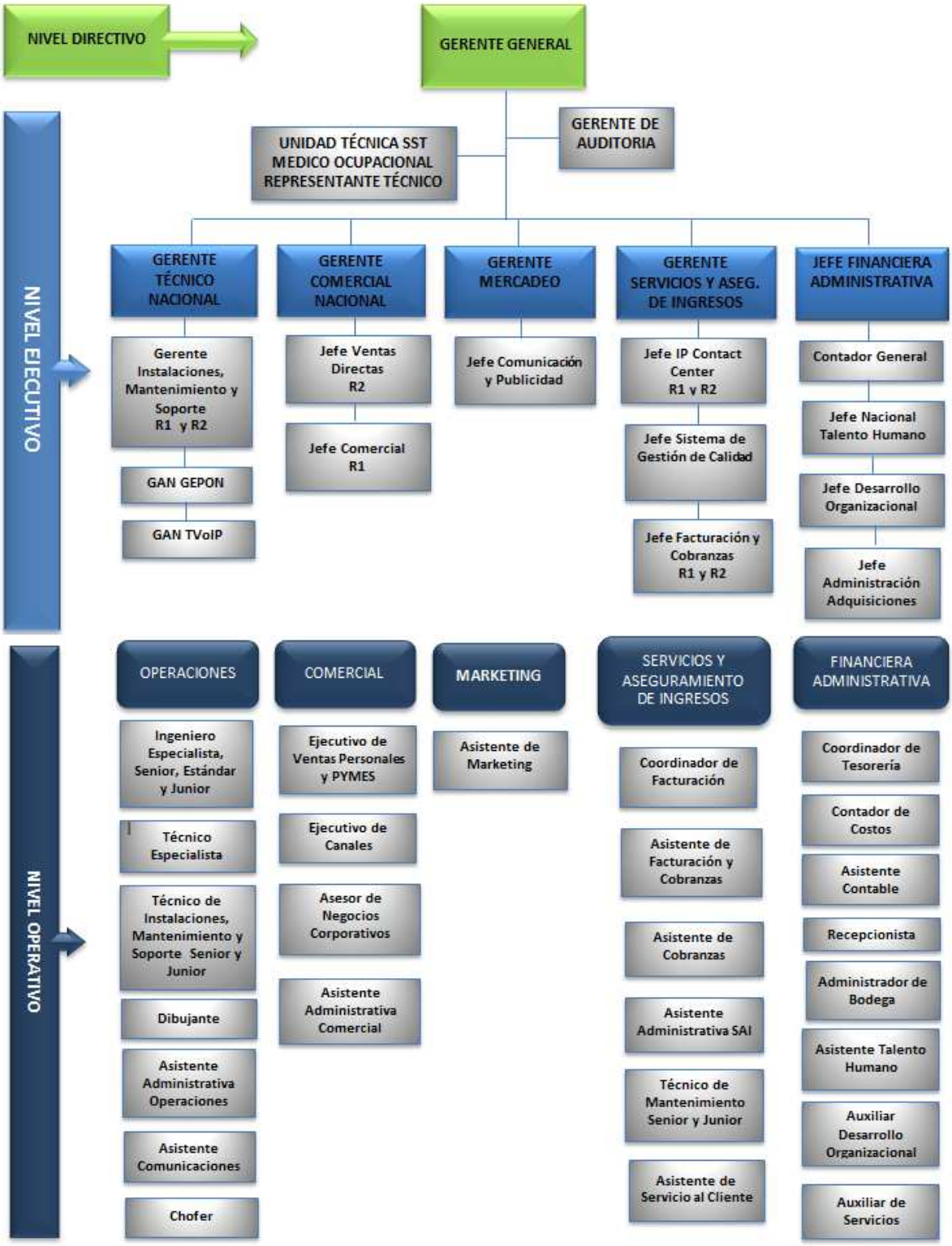
BIBLIOGRAFÍA

- GARCIA FORT Javier, MADRID, Julio 2010. PLAN DE CONTINUIDAD DEL NEGOCIO DE UNA TIC. http://es.scribd.com/doc/63042328/26/CAPITULO-4-ANALISIS-DE-IMPACTO-DEL-NEGOCIO. Mayo 2013.
- GONZALEZ Roció, VASQUEZ Andres, REYES Rene, RAMIREZ Diana, ARIAS Marlon. 23 de Septiembre de 2009. BS 25999 GESTION DE LA CONTINUIDAD DE NEGOCIO. https://docs.google.com/viewer?a=v&q=cache:fF98zKruArMJ:scc2008.webs.com/Desarrollo/BS%252025999.docx+secciones+de+la+norma+bs25999&hl=es&gl=ec&pid=bl&srcid=ADGEEShAoBGRuU2JBvvRROlMXTwLh4v2NvMx5i70LaJ4DPf2pkW6aqYZSvNr_7OfXASYrIj_-x0EEm0uOObHr7ctZ-qYjy6rAkot-lX9Q_JOsAFM_n1AERC6Po4cnhLvds7GcjPHBMDr&sig=AHIEtbQM_YWPqDCUSD3Rrfoneskxjc7Ozg. Junio 2013.
- CONATEL, RESOLUCIÓN TEL-477-16-CONATEL-2012.
- CONGRESO NACIONAL, Ley de comercio electrónico, firmas electrónicas y
- mensajes de datos
- MARTINEZ Juan Gaspar, PLANES DE CONTINGENCIA: La Continuidad del Negocio en la Organizaciones, Juan Gaspar Martinez, Ediciones Diaz Santos, S.A., 2004.
- STONEBURNER Gary, GOGUEN Alice and FERINGA Alexis (Julio 2002), Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30
- Revista Tecnológica ESPOL – RTE, Vol. XX, N. XX, pp-pp, (Mes, 200X), Desarrollo de un Plan de Continuidad del Negocio de una empresa Industrial productora de Electrodos, en el Área de Producción, en la ciudad de Guayaquil, para el período 2009
- ARANJO, Jeferson (Manizales 2010), BCM Business continuity management, BS 25999, BCI (Business continuityinstitute)

- BUSINESS CONTINUITY INSTITUTE: MANUAL DE BUENAS PRACTICAS 2007. Guia para instaurar Buenas Practicas Globales en Gestion de Continuidad de Negocio.
- CARVAJAL ARMANDO (2007), Como hacer un BIA, la base fundamental del BCP,
- RODRIGUEZ Edith, CORREA Deisy. PLAN DE CONTINUIDAD BS25999.

ANEXOS

ANEXO 1: ORGANIGRAMA



ANEXO 2: CARTA DE AUTORIZACIÓN

Quito, 1 de marzo de 2012

Yo Washington Francisco Balarezo Pozo en calidad de representante legal de la empresa MEGADATOS S.A con RUC número 1791287541001 autorizo a la Srta. Glenda Soraya Tixi Cali con cedula de identidad número 0604173328 a utilizar información de la compañía con uso exclusivo para fines académicos para la realización de su Proyecto de Titulación de Tesis el cual lo está realizando en la empresa. Si esta información fuera difundida más allá de los fines académicos la Srta. Glenda Soraya Tixi Cali como usuaria de la información se someterá a las penalidades correspondientes en el Reglamento Interno, tanto como Políticas Organizacionales y la pena civil si fuera el caso.

Atentamente

_____

Francisco Balarezo

ANEXO 3: MATRIZ DEL RIESGO

Tabla 6.1: Matriz del Riesgo de los Activos "Servidores"

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Ambientales	1	Terremotos/ Sismos	El edificio donde se encuentra ubicado MEGADATOS S.A. no es antisísmico	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Quito se encuentra ubicado en una zona sísmica					
			Falta de capacitación al personal ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	2	Erupciones Volcánicas	Quito se encuentra en una zona geográfica que se encuentra rodeada de volcanes	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	3	Deslizamientos	Quito se encuentra asentado sobre valles y quebradas	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo

Tabla: 6.1: Matriz del Riesgo de los Activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	1	Desconfiguración involuntaria del equipo	No existe una gestión adecuada de claves de configuración y de acceso.	Pérdida total o parcial del servicio que brinda el activo	Ninguna	Baja	Media	Bajo
			No existe un procedimiento formal de almacenamiento de contraseñas					
	2	Desconexión de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Revisión y cambio periódico del cableado que se está utilizando	Baja	Media	Bajo
			No existe una política o normativa de cableado y de cambio de cableado periódico.					
			No existe una protección física pare evitar desconexiones					

Tabla: 6.1: Matriz del Riesgo de los Activos "Servidores" (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	3	Ingreso a la configuración de equipos por personal no autorizado	No existe un control adecuando de ingreso a los equipos	Cambio no autorizado en la configuración del equipo. Detención de servicio. Robo de información	Ninguna	Baja	Media	Bajo
			No existe una política de claves y de privilegios de acceso		Ninguna			
			No existe una política de actualización periódica de claves		Ninguna			
	4	Ingreso de personal no autorizado a las instalaciones	No existe el suficiente control de acceso de personas desconocidas	Falla momentánea en los servicios, robo y/o perdida de equipos y pérdidas económicas	Se pide identificación de cada persona que ingresa al edificio	Media	Media	Medio
			No se cuenta con un registro de las personas que ingresan a la empresa					
	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios y éste podría compartirlas o almacenarlas inadecuadamente	Cambio no autorizado de configuraciones, violación de la confidencialidad de la información. Peligro de robos y ataques.	Cada empleado tiene su identificación con foto y datos personales.	Media	Media	Medio

Tabla: 6.1: Matriz del Riesgo de los Activos "Servidores" (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	6	Modificación de información contenida en equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados, conflictos entre el personal por desconocimiento de los cambios realizados	Políticas de control de cambio de configuración de equipos	Media	Media	Medio
	7	Divulgación de información	A menudo no se pone en práctica el acuerdo de confidencialidad No se aplican las sanciones especificadas en el acuerdo de confidencialidad No se da seguimiento a ex funcionarios	Violación de la confidencialidad de información, mal uso de la información por agentes externos	Ninguna	Media	Media	Medio
	8	Error en la etiquetación de activos	No se tiene la información clasificada No todos los activos se encuentran correctamente etiquetados	Información sensible podría verse afectada, pérdida de información crítica.	Ninguna	Media	Media	Medio

Tabla: 6.1: Matriz del Riesgo de los Activos "Servidores" (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	9	Mantenimiento inadecuado de equipos	No se tiene una política de mantenimiento periódico de equipos	Daño del equipo, afectando al servicio que bridan	Se posee una política para mantenimientos periódicos de equipos.	Baja	Media	Bajo
	10	Robo o Pérdida del equipo	No se cuenta con equipos de backups de todos los servidores No existe un control de acceso adecuado	Falla momentánea en los servicios y pérdidas económicas	Ninguna	Baja	Alto	Bajo
	11	Inundaciones por falla en tuberías del edificio	No se conoce como se encuentra la red de agua en el edificio	Daño de equipos, suspensión temporal de los servicios	La administración del edificio se encarga del mantenimiento del mismo	Baja	Media	Bajo

Tabla: 6.1: Matriz del Riesgo de los Activos "Servidores" (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	12	Incendios provocados por personal de la empresa	No se cuenta con un sistema anti incendios	Pérdida total o parcial de todo el edificio y de equipos	En cada piso hay un extintor y el personal sabe que no debe usar fuego dentro de las instalaciones	Baja	Alto	Bajo
			No existe una capacitación del personal para casos de emergencia	Pérdidas humanas y económicas		Baja	Media	Bajo
	13	Respaldos mal realizados	No existe una política de respaldos	Pérdida de la información almacenada en el equipo	Ninguna	Baja	Media	Bajo
	14	Pérdida de Información clave contenida en los equipos	No se tiene una política de claves de acceso y de ingreso a los equipos	Pérdida total o parcial de los servicio	Ninguna	Media	Media	Medio
			No se realizan respaldos periódicos de la información contenida en los equipos					

Tabla: 6.1: Matriz del Riesgo de los Activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	15	Ataques a la red	No se tiene una política de claves de acceso y de ingreso a los equipos	Pérdida o daños de los equipos. Suspensión total o parcial del servicio que brinda el activo	Se mantiene un monitoreo constante en los equipos para evitar posibles ataques	baja	Media	Bajo
	16	Falta de equipos de respaldos	No se cuenta con una política para disponer equipos de respaldos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	Media	Media	Medio
Tecnológicas	1	Daño de hardware	No se tienen las piezas necesarias de repuestos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	Baja	Media	Bajo

Tabla: 6.1: Matriz del Riesgo de los Activos “Servidores” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	2	Daño de software	Error en las actualizaciones Pérdida o borrado de carpetas propias de aplicaciones	Daño permanente del equipo. Pérdida total o parcial de la entrega del servicio que brinda el activo	ninguna	Baja	Media	Bajo
	3	Inhibición de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Ingresan al TELEPUERTO solo el personal autorizado	Baja	Media	Bajo
	4	Falla eléctrica	Sobrecarga en las regletas	Daño total o parcial de los equipos	Sistema de UPS	Media	Alto	Medio
	5	Falla en el UPS	No se tiene conocimiento de los cortes de energía no programados No existe una política de mantenimiento periódico de equipos	Pérdida de todo el servicio para usuarios internos y se puede quemar el activo	Se realiza un mantenimiento periódico de los equipos	Baja	Alto	Bajo

Tabla: 6.1: Matriz del Riesgo de los Activos "Servidores" (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	6	Daño en medios de transmisión	No existen medios alternos para todos los casos Falta políticas de cableado estructurado	Pérdida temporal del servicio que brinda	Revisión y cambio de medios de transmisión viejos o defectuosos	Baja	Media	Bajo
	7	Daño en el aire acondicionado	No existe una política de mantenimiento periódico de equipos	Calentamiento de equipos y posible daño de los mismos	Ninguna	Baja	Baja	Bajo
	8	Virus, troyanos, gusanos, etc.	No existe un monitoreo continuo para detectar posibles ataques. No existen suficientes seguridades para bloquear amenazas	Pérdida temporal del servicio que brinda Violación de la seguridad de información	Se posee un buen antivirus y se lo usa de la manera adecuada	Baja	Media	Bajo
	9	Software desactualizado	No se cuenta con planes de migración de SO y de SW de aplicación	Falla en la prestación de los servicios que ofrece el activo y pérdidas económicas	Ninguna	Media	Alto	Medio

Tabla: 6.1: Matriz del Riesgo de los Activos "Servidores" (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	10	Software no licenciado	No se cuenta con licencias de todos los programas	Recesión de las actividades de la empresa	Se tiene un contrato de licenciamiento	Media	Alto	Medio

Tabla 6.2: Matriz del Riesgo de los Activos "Equipos de redes y comunicación"

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Ambientales	1	Terremotos/Sismos	El edificio donde se encuentra ubicado MEGADATOS S.A. no es antisísmico	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Quito se encuentra ubicado en una zona sísmica					
			Falta de capacitación al personal ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo

Tabla 6.2: Matriz del Riesgo de los Activos “Equipos de redes y comunicación” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Ambientales	2	Erupciones Volcánicas	Quito se encuentra en una zona geográfica que se encuentra rodeada de volcanes	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	3	Deslizamientos	Quito se encuentra asentado sobre valles y quebradas	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
Humanas	1	Desconfiguración involuntaria del equipo	No existe una gestión adecuada de claves de configuración y de acceso. No existe un procedimiento formal de almacenamiento de contraseñas	Pérdida total o parcial del servicio que brinda el activo	Ninguna	Baja	Media	Bajo

Tabla 6.2: Matriz del Riesgo de los Activos “Equipos de redes y comunicación” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	2	Desconexión de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Revisión y cambio periódico del cableado que se está utilizando	Baja	Media	Bajo
			No existe una política o normativa de cableado y de cambio de cableado periódico.					
			No existe una protección física pare evitar desconexiones					
	3	Ingreso a la configuración de equipos por personal no autorizado	No existe un control adecuando de ingreso a los equipos	Cambio no autorizado en la configuración del equipo. Detención de servicio. Robo de información	Ninguna	Media	Media	Medio
			No existe una política de claves y de privilegios de acceso		Ninguna			
			No existe una política de actualización periódica de claves		Ninguna			

Tabla 6.2: Matriz del Riesgo de los Activos “Equipos de redes y comunicación” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	4	Ingreso de personal no autorizado a las instalaciones	No existe el suficiente control de acceso de personas desconocidas No se cuenta con un registro de las personas que ingresan a la empresa	Falla momentánea en los servicios y pérdidas económicas	Se pide identificación de cada persona que ingresa al edificio	Media	Media	Medio
	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios y éste podría compartirlas o almacenarlas inadecuadamente	Cambio no autorizado de configuraciones, violación de la confidencialidad de la información. Peligro de robos y ataques.	Cada empleado tiene su identificación con foto y datos personales.	Media	Media	Medio
	6	Modificación de información contenida en equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados, conflictos entre el personal por desconocimiento de los cambios realizados	Políticas de control de cambio de configuración de equipos	Baja	Media	Bajo

Tabla 6.2: Matriz del Riesgo de los Activos “Equipos de redes y comunicación” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	7	Divulgación de información	A menudo no se pone en práctica el acuerdo de confidencialidad	Violación de la confidencialidad de información, mal uso de la información por agentes externos.	Ninguna	Media	Media	Medio
			No se aplican las sanciones especificadas en el acuerdo de confidencialidad					
			No se da seguimiento a ex funcionarios					
	8	Error en la etiquetación de activos	No se tiene la información clasificada	Información sensible podría verse afectada, pérdida de información crítica.	Ninguna	Baja	Media	Bajo
			No todos los activos se encuentran correctamente etiquetados					
	9	Mantenimiento inadecuado de equipos	No se tiene una política de mantenimiento periódico de equipos	Daño del equipo, afectando al servicio que bridan	Se posee una política para mantenimientos periódicos de equipos.	Baja	Media	Bajo

Tabla 6.2: Matriz del Riesgo de los Activos “Equipos de redes y comunicación” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	10	Robo o Pérdida del equipo	No ese cuenta con respaldos de todos los equipos No existe un control de acceso adecuado	Falla momentánea en los servicios y Pérdidas económicas	Ninguna	Baja	Media	Bajo
	11	Inundaciones por falla en tuberías del edificio	No se conoce como se encuentra la red de agua en el edificio	Daño de equipos, suspensión temporal de los servicios	La administración del edificio se encarga del mantenimiento adecuado del edificio	Baja	Media	Bajo
	12	Incendios provocados por personal de la empresa	No se cuenta con un sistema anti incendios	Pérdida total o parcial de todo el edificio y de equipos	En cada piso existe un extintor y se capacita al personal para que no use fuego dentro de las instalaciones	Baja	Alto	Bajo
			No existe una capacitación del personal para casos de emergencia	Pérdidas humanas y económicas		Baja	Media	Bajo

Tabla 6.2: Matriz del Riesgo de los Activos “Equipos de redes y comunicación” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	13	Respaldos mal realizados	No existe una política de respaldos	Pérdida de la información almacenada en el equipo	Ninguna	Baja	Media	Bajo
	14	Pérdida de Información clave contenida en los equipos	No se tiene una política de claves de acceso y de ingreso a los equipos No se realizan respaldos periódicos de la información contenida en los equipos	Pérdida total o parcial de los servicio	Ninguna	Baja	Media	Bajo
	15	Falta de equipos de respaldos	No se cuenta con una política para disponer equipos de respaldos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	Media	Media	Medio

Tabla 6.2: Matriz del Riesgo de los Activos “Equipos de redes y comunicación” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	16	Ataques a las red	No se tiene una política de claves de acceso y de ingreso a los equipos	Pérdida o daños de los equipos. Suspensión total o parcial del servicio que brinda el activo	Se mantiene un monitoreo constante en los equipos para evitar posibles ataques	baja	Media	Bajo
Tecnológicas	1	Daño de hardware	No se tienen las piezas necesarias de repuestos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	Baja	Media	Bajo
	2	Daño de software	Error en las actualizaciones	Daño permanente del equipo. Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	Baja	Media	Bajo
			Pérdida o borrado de carpetas propias de aplicaciones					

Tabla 6.2: Matriz del Riesgo de los Activos “Equipos de redes y comunicación” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	3	Inhibición de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Ingresan al TELEPUERTO solo el personal autorizado	Baja	Media	Bajo
	4	Falla eléctrica	Sobrecarga en las regletas	Daño total o parcial de los equipos	Se tiene un sistema de UPS	Baja	Media	Bajo
	5	Falla en el UPS	No se tiene conocimiento de los cortes de energía no programados No existe una política de mantenimiento periódico de equipos	Pérdida de todo el servicio para usuarios internos y se puede quemar el activo	Se realiza un mantenimiento periódico de los equipos	Baja	Media	Bajo
	6	Daño en medios de transmisión	No existen medios alternos para todos los casos Falta políticas de cableado estructurado	Pérdida temporal del servicio que brinda	Revisión y cambio de medios de transmisión viejos o defectuosos	Baja	Media	Bajo

Tabla 6.2: Matriz del Riesgo de los Activos "Equipos de redes y comunicación" (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	7	Daño en el aire acondicionado	No existe una política de mantenimiento periódico de equipos	Calentamiento de equipos y posible daño de los mismos	Ninguna	Baja	Baja	Bajo
	8	Virus, troyanos, gusanos, etc.	No existe un monitoreo continuo para detectar posibles ataques.	Pérdida temporal del servicio que brinda	Se posee un buen antivirus en la empresa y se lo usa de la mejor manera	Baja	Media	Bajo
			No existen suficientes seguridades para bloquear amenazas	Violación de la seguridad de información				
	9	Software desactualizado	No se cuenta con planes de migración de SO y de SW de aplicación	Falla en la prestación de los servicios que ofrece el activo y pérdidas económicas	Ninguna	Media	Media	Medio
	10	Software no licenciado	No se cuenta con licencias de todos los programas	Recesión de las actividades de la empresa	Se tiene un contrato de licenciamiento	Media	Alto	Medio

Tabla 6.3: Matriz del Riesgo de los Activos "Equipos de Escritorio"

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Ambientales	1	Terremotos /Sismos	El edificio se encuentra ubicado MEGADATOS S.A. no es antisísmico	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Quito se encuentra ubicado en una zona sísmica					
			Falta de capacitación al personal ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	2	Erupciones Volcánicas	Quito se encuentra en una zona geográfica que se encuentra rodeada de volcanes	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	3	Deslizamientos	Quito se encuentra asentado sobre valles y quebradas	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	1	Desconfiguración involuntaria del equipo	No existe una gestión adecuada de claves de configuración y de acceso. No existe un procedimiento formal de almacenamiento de contraseñas	Pérdida total o parcial del servicio que brinda el activo	Ninguna	Baja	Baja	Bajo
	2	Desconexión de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Revisión y cambio periódico del cableado que se está utilizando	Media	Baja	Bajo
			No existe una política o normativa de cableado y de cambio de cableado periódico.					
			No existe una protección física pare evitar desconexiones					

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	3	Ingreso a la configuración de equipos por personal no autorizado	No existe un control adecuando de ingreso a los equipos	Cambio no autorizado en la configuración del equipo. Detención de servicio. Robo de información	Ninguna	Media	Baja	Bajo
			No existe una política de claves y de privilegios de acceso		Ninguna			
			No existe una política de actualización periódica de claves		Ninguna			
	4	Ingreso de personal no autorizado a las instalaciones	No existe el suficiente control de acceso de personas desconocidas	Falla momentánea en los servicios y pérdidas económicas	Se pide identificación de cada persona que ingresa al edificio	Media	Baja	Bajo
			No se cuenta con un registro de las personas que ingresan a la empresa					

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios y éste podría compartirlas o almacenarlas inadecuadamente	Cambio no autorizado de configuraciones, violación de la confidencialidad de la información. Peligro de robos y ataques.	Cada empleado tiene su identificación con foto y datos personales.	Media	Baja	Bajo
	6	Modificación de información contenida en equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados, conflictos entre el personal por desconocimiento de los cambios realizados	Políticas de control de cambio de configuración de equipos	Media	Baja	Bajo

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	7	Divulgación de información	A menudo no se pone en práctica el acuerdo de confidencialidad No se aplican las sanciones especificadas en el acuerdo de confidencialidad No se da seguimiento a ex funcionarios	Violación de la confidencialidad de información, mal uso de la información por agentes externos.	Ninguna	Media	Baja	Bajo
	8	Error en la etiquetación de activos	No se tiene la información clasificada No todos los activos se encuentran correctamente etiquetados	Información sensible podría verse afectada, pérdida de información crítica.	Ninguna	Baja	Baja	Bajo
	9	Mantenimiento inadecuado de equipos	No se tiene una política de mantenimiento periódico de equipos	Daño del equipo, afectando al servicio que bridan	Se posee una política para mantenimientos periódicos de equipos.	Baja	Baja	Bajo

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	10	Robo o Pérdida del equipo	No ese cuenta con respaldos de todos los servidores No existe un control de acceso adecuado	Falla momentánea en los servicios y Pérdidas económicas	Ninguna	Baja	Baja	Bajo
	11	Inundaciones por falla en tuberías del edificio	No se conoce como se encuentra la red de agua en el edificio	Daño de equipos, suspensión temporal de los servicios	La administración del edificio se encarga del mantenimiento adecuado del edificio	Baja	Baja	Bajo
	12	Incendios provocados por personal de la empresa	No se cuenta con un sistema anti incendios	Pérdida total o parcial de todo el edificio y de equipos	En cada piso existe un extintor y se capacita al personal para que no use fuego dentro de las instalaciones	Baja	Baja	Bajo
			No existe una capacitación del personal para casos de emergencia	Pérdidas humanas y económicas		Baja	Baja	Bajo

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	13	Respaldos mal realizados	No existe una política de respaldos	Pérdida de la información almacenada en el equipo	Ninguna	Baja	Baja	Bajo
	14	Pérdida de Información clave contenida en los equipos	No se tiene una política de claves de acceso y de ingreso a los equipos No se realizan respaldos periódicos de la información contenida en los equipos	Pérdida total o parcial de los servicio	Ninguna	Baja	Baja	Bajo
	15	Falta de equipos de respaldos	No se cuenta con una política para disponer equipos de respaldos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	baja	Baja	Bajo

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	16	Ataques a las red	No se tiene una política de claves de acceso y de ingreso a los equipos	Pérdida o daños de los equipos. Suspensión total o parcial del servicio que brinda el activo	Se mantiene un monitoreo constante en los equipos para evitar posibles ataques	baja	Media	Bajo
Tecnológicas	1	Daño de hardware	No se tienen las piezas necesarias de repuestos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	baja	Baja	Bajo
	2	Daño de software	Error en las actualizaciones	Daño permanente del equipo. Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	Baja	Baja	Bajo
			Pérdida o borrado de carpetas propias de aplicaciones					

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	3	Inhibición de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Ingresan al TELEPUERTO solo el personal autorizado	Baja	Baja	Bajo
	4	Falla eléctrica	Sobrecarga en las regletas	Daño total o parcial de los equipos	Se tiene un sistema de UPS	Baja	Baja	Bajo
	5	Falla en el UPS	No se tiene conocimiento de los cortes de energía no programados No existe una política de mantenimiento periódico de equipos	Pérdida de todo el servicio para usuarios internos y se puede quemar el activo	Se realiza un mantenimiento periódico de los equipos	Baja	Baja	Bajo
	6	Daño en medios de transmisión	No existen medios alternos para todos los casos Falta políticas de cableado estructurado	Pérdida temporal del servicio que brinda	Revisión y cambio de medios de transmisión viejos o defectuosos	Media	Baja	Bajo

Tabla 6.3: Matriz del Riesgo de los Activos “Equipos de Escritorio” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACION	Prob	Imp	NR
Tecnológicas	7	Daño en el aire acondicionado	No existe una política de mantenimiento periódico de equipos	Calentamiento de equipos y posible daño de los mismos	Ninguna	Baja	Baja	Bajo
	8	Virus, troyanos, gusanos, etc.	No existe un monitoreo continuo para detectar posibles ataques.	Pérdida temporal del servicio que brinda	Se posee un buen antivirus en la empresa y se lo usa de la mejor manera	Baja	Baja	Bajo
			No existen suficientes seguridades para bloquear amenazas	Violación de la seguridad de información				
	9	Software desactualizado	No se cuenta con planes de migración de SO y de SW de aplicación	Falla en la prestación de los servicios que ofrece el activo y pérdidas económicas	Ninguna	Media	Baja	Bajo
	10	Software no licenciado	No se cuenta con licencias de todos los programas	Recesión de las actividades de la empresa	Se tiene un contrato de licenciamiento	Media	Baja	Bajo

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops”

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Ambientales	1	Terremotos /Sismos	El edificio donde se encuentra ubicado MEGADATOS S.A. no es antisísmico	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Quito se encuentra ubicado en una zona sísmica					
			Falta de capacitación al personal ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	2	Erupciones Volcánicas	Quito se encuentra en una zona geográfica que se encuentra rodeada de volcanes	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	3	Deslizamientos	Quito se encuentra asentado sobre valles y quebradas	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	1	Desconfiguración involuntaria del equipo	No existe una gestión adecuada de claves de configuración y de acceso. No existe un procedimiento formal de almacenamiento de contraseñas	Pérdida total o parcial del servicio que brinda el activo	Ninguna	Baja	Media	Bajo
	2	Desconexión de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Revisión y cambio periódico del cableado que se está utilizando	Media	Baja	Bajo
			No existe una política o normativa de cableado y de cambio de cableado periódico.					
			No existe una protección física pare evitar desconexiones					

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	3	Ingreso a la configuración de equipos por personal no autorizado	No existe un control adecuando de ingreso a los equipos	Cambio no autorizado en la configuración del equipo. Detención de servicio. Robo de información	Ninguna	Media	Baja	Bajo
			No existe una política de claves y de privilegios de acceso		Ninguna			
			No existe una política de actualización periódica de claves		Ninguna			
	4	Ingreso de personal no autorizado a las instalaciones	No existe el suficiente control de acceso de personas desconocidas	Falla momentánea en los servicios y pérdidas económicas	Se pide identificación de cada persona que ingresa al edificio	Media	Baja	Bajo
			No se cuenta con un registro de las personas que ingresan a la empresa					

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios y éste podría compartirlas o almacenarlas inadecuadamente	Cambio no autorizado de configuraciones, violación de la confidencialidad de la información. Peligro de robos y ataques.	Cada empleado tiene su identificación con foto y datos personales.	Media	Baja	Bajo
	6	Modificación de información contenida en equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados, conflictos entre el personal por desconocimiento de los cambios realizados	Políticas de control de cambio de configuración de equipos	Media	Media	Medio

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	7	Divulgación de información	A menudo no se pone en práctica el acuerdo de confidencialidad	Violación de la confidencialidad de información, mal uso de la información por agentes externos.	Ninguna	Media	Media	Medio
			No se aplican las sanciones especificadas en el acuerdo de confidencialidad					
			No se da seguimiento a ex funcionarios					
	8	Error en la etiquetación de activos	No se tiene la información clasificada	Información sensible podría verse afectada, pérdida de información crítica.	Ninguna	Baja	Baja	Bajo
			No todos los activos se encuentran correctamente etiquetados					
	9	Mantenimiento inadecuado de equipos	No se tiene una política de mantenimiento periódico de equipos	Daño del equipo, afectando al servicio que bridan	Se posee una política para mantenimientos periódicos de equipos.	Baja	Media	Bajo
						Media	Media	Medio

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	10	Robo o Pérdida del equipo	No ese cuenta con máquinas de backups	Falla momentánea en los servicios y Pérdidas económicas	Ninguna	Media	Media	Medio
			No existe un control de acceso adecuado					
	11	Inundaciones por falla en tuberías del edificio	No se conoce como se encuentra la red de agua en el edificio	Daño de equipos, suspensión temporal de los servicios	La administración del edificio se encarga del mantenimiento adecuado del edificio	Baja	Baja	Bajo
	12	Incendios provocados por personal de la empresa	No se cuenta con un sistema anti incendios	Pérdida total o parcial de todo el edificio y de equipos	En cada piso existe un extintor y se capacita al personal para que no use fuego dentro de las instalaciones	Baja	Baja	Bajo
			No existe una capacitación del personal para casos de emergencia	Pérdidas humanas y económicas		Baja	Baja	Bajo

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	13	Respaldos mal realizados	No existe una política de respaldos	Pérdida de la información almacenada en el equipo	Ninguna	Baja	Media	Bajo
	14	Pérdida de Información clave contenida en los equipos	No se tiene una política de claves de acceso y de ingreso a los equipos No se realizan respaldos periódicos de la información contenida en los equipos	Pérdida total o parcial de los servicio	Ninguna	Baja	Media	Bajo
	15	Falta de equipos de respaldos	No se cuenta con una política para disponer equipos de respaldos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Se mantiene un monitoreo constante en los equipos para evitar posibles ataques	baja	Baja	Bajo

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	16	Ataques a las red	No se tiene una política de claves de acceso y de ingreso a los equipos	Pérdida o daños de los equipos. Suspensión total o parcial del servicio que brinda el activo	Ninguna	baja	Media	Bajo
Tecnológicas	1	Daño de hardware	No se tienen las piezas necesarias de repuestos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	baja	Baja	Bajo
	2	Daño de software	Error en las actualizaciones	Daño permanente del equipo. Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	baja	Baja	Bajo
			Pérdida o borrado de carpetas propias de aplicaciones					
	3	Inhibición de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Ingresan al TELEPUERTO solo el personal autorizado	Baja	Baja	Bajo

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	4	Falla eléctrica	Sobrecarga en las regletas	Daño total o parcial de los equipos	Se tiene un sistema de UPS	Baja	Baja	Bajo
	5	Falla en el UPS	No se tiene conocimiento de los cortes de energía no programados No existe una política de mantenimiento periódico de equipos	Pérdida de todo el servicio para usuarios internos y se puede quemar el activo	Se realiza un mantenimiento periódico de los equipos	Baja	Baja	Bajo
	6	Daño en medios de transmisión	No existen medios alternos para todos los casos Falta políticas de cableado estructurado	Pérdida temporal del servicio que brinda	Revisión y cambio de medios de transmisión viejos o defectuosos	Media	Baja	Bajo
	7	Daño en el aire acondicionado	No existe una política de mantenimiento periódico de equipos	Calentamiento de equipos y posible daño de los mismos	Ninguna	Baja	Baja	Bajo

Tabla 6.4: Matriz del Riesgo de los Activos “Laptops” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	8	Virus, troyanos, gusanos, etc.	No existe un monitoreo continuo para detectar posibles ataques.	Pérdida temporal del servicio que brinda	Se posee un buen antivirus en la empresa y se lo usa de la mejor manera	Baja	Baja	Bajo
			No existen suficientes seguridades para bloquear amenazas	Violación de la seguridad de información				
	9	Software desactualizado	No se cuenta con planes de migración de SO y de sw de aplicación	Falla en la prestación de los servicios que ofrece el activo y pérdidas económicas	Ninguna	Media	Baja	Bajo
	10	Software no licenciado	No se cuenta con licencias de todos los programas	Recesión de las actividades de la empresa	Se tiene un contrato de licenciamiento	Media	Baja	Bajo

Tabla 6.5: Matriz del Riesgo de los Activos "Equipo Computacional Secundario"

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Ambientales	1	Terremotos /Sismos	El edificio donde se encuentra ubicado MEGADATOS S.A. no es antisísmico	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Quito se encuentra ubicado en una zona sísmica					
			Falta de capacitación al personal ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	2	Erupciones Volcánicas	Quito se encuentra en una zona geográfica que se encuentra rodeada de volcanes	Daño total o parcial de toda la infraestructura de la empresa	Ninguno	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo
	3	Deslizamientos	Quito se encuentra asentado sobre valles y quebradas	Daño total o parcial de toda la infraestructura de la empresa	Ninguna	Baja	Alto	Bajo
			Falta de capacitación ante emergencias	Accidentes e incluso pérdidas humanas.		Baja	Media	Bajo

Tabla 6.5: Matriz del Riesgo de los Activos “Equipo Computacional Secundario” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	1	Desconfiguración involuntaria del equipo	No existe una gestión adecuada de claves de configuración y de acceso. No existe un procedimiento formal de almacenamiento de contraseñas	Pérdida total o parcial del servicio que brinda el activo	Ninguna	Media	Baja	Bajo
	2	Desconexión de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Revisión y cambio periódico del cableado que se esta utilizando	Baja	Baja	Bajo
			No existe una política o normativa de cableado y de cambio de cableado periódico.					
			No existe una protección física pare evitar desconexiones					

Tabla 6.5: Matriz del Riesgo de los Activos “Equipo Computacional Secundario” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	3	Ingreso a la configuración de equipos por personal no autorizado	No existe un control adecuando de ingreso a los equipos	Cambio no autorizado en la configuración del equipo. Detención de servicio. Robo de información	Ninguna	Baja	Baja	Bajo
			No existe una política de claves y de privilegios de acceso		Ninguna			
			No existe una política de actualización periódica de claves		Ninguna			
	4	Ingreso de personal no autorizado a las instalaciones	No existe el suficiente control de acceso de personas desconocidas	Falla momentánea en los servicios y pérdidas económicas	Se pide identificación de cada persona que ingresa al edificio	Media	Baja	Bajo
			No se cuenta con un registro de las personas que ingresan a la empresa					

Tabla 6.5: Matriz del Riesgo de los Activos "Equipo Computacional Secundario" (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	5	Suplantación de identidad	No existe una adecuada gestión de claves de usuarios y éste podría compartirlas o almacenarlas inadecuadamente	Cambio no autorizado de configuraciones, violación de la confidencialidad de la información. Peligro de robos y ataques.	Cada empleado tiene su identificación con foto y datos personales.	Baja	Baja	Bajo
	6	Modificación de información contenida en equipos	No existe una política formal de autorización de cambios, migraciones o actualizaciones.	Cambios no autorizados, conflictos entre el personal por desconocimiento de los cambios realizados	Políticas de control de cambio de configuración de equipos	Baja	Baja	Bajo

Tabla 6.5: Matriz del Riesgo de los Activos “Equipo Computacional Secundario” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	7	Divulgación de información	A menudo no se pone en práctica el acuerdo de confidencialidad No se aplican las sanciones especificadas en el acuerdo de confidencialidad No se da seguimiento a ex funcionarios	Violación de la confidencialidad de información, mal uso de la información por agentes externos.	Ninguna	Baja	Baja	Bajo
	8	Error en la etiquetación de activos	No se tiene la información clasificada No todos los activos se encuentran correctamente etiquetados	Información sensible podría verse afectada, pérdida de información crítica.	Ninguna	Baja	Baja	Bajo
	9	Mantenimiento inadecuado de equipos	No se tiene una política de mantenimiento periódico de equipos	Daño del equipo, afectando al servicio que bridan	Se posee una política para mantenimientos periódicos de equipos.	Baja	Baja	Bajo

Tabla 6.5: Matriz del Riesgo de los Activos “Equipo Computacional Secundario” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	10	Robo o Pérdida del equipo	No ese cuenta con respaldos de todos los servidores No existe un control de acceso adecuado	Falla momentánea en los servicios y Pérdidas económicas	Ninguna	Baja	Baja	Bajo
	11	Inundaciones por falla en tuberías del edificio	No se conoce como se encuentra la red de agua en el edificio	Daño de equipos, suspensión temporal de los servicios	La administración del edificio se encarga del mantenimiento adecuado del edificio	Baja	Baja	Bajo
	12	Incendios provocados por personal de la empresa	No se cuenta con un sistema anti incendios	Pérdida total o parcial de todo el edificio y de equipos	En cada piso existe un extintor y se capacita al personal para que no use fuego dentro de las instalaciones	Baja	Baja	Bajo
			No existe una capacitación del personal para casos de emergencia	Pérdidas humanas y económicas		Baja	Baja	Bajo

Tabla 6.5: Matriz del Riesgo de los Activos “Equipo Computacional Secundario” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	13	Respaldos mal realizados	No existe una política de respaldos	Pérdida de la información almacenada en el equipo	Ninguna	Baja	Baja	Bajo
	14	Pérdida de Información clave contenida en los equipos	No se tiene una política de claves de acceso y de ingreso a los equipos No se realizan respaldos periódicos de la información contenida en los equipos	Pérdida total o parcial de los servicio	Ninguna	Baja	Baja	Bajo
	15	Falta de equipos de respaldos	No se cuenta con una política para disponer equipos de respaldos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Se mantiene un monitoreo constante en los equipos para evitar posibles ataques	Baja	Baja	Bajo

Tabla 6.5: Matriz del Riesgo de los Activos “Equipo Computacional Secundario” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	16	Ataques a las red	No se tiene una política de claves de acceso y de ingreso a los equipos	Pérdida o daños de los equipos. Suspensión total o parcial del servicio que brinda el activo	Ninguna	Baja	Baja	Bajo
Tecnológicas	1	Daño de hardware	No se tienen las piezas necesarias de repuestos	Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	Baja	Baja	Bajo
	2	Daño de software	Error en las actualizaciones Pérdida o borrado de carpetas propias de aplicaciones	Daño permanente del equipo. Pérdida total o parcial de la entrega del servicio que brinda el activo	Ninguna	Baja	Baja	Bajo
	3	Inhibición de puerto	No hay suficiente control en el ingreso al edificio	Desconexión del servicio para clientes internos	Ingresan al TELEPUERTO solo el personal autorizado	Baja	Baja	Bajo

Tabla 6.5: Matriz del Riesgo de los Activos “Equipo Computacional Secundario” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	4	Falla eléctrica	Sobrecarga en las regletas	Daño total o parcial de los equipos	Se tiene un sistema de UPS	Baja	Baja	Bajo
	5	Falla en el UPS	No se tiene conocimiento de los cortes de energía no programados No existe una política de mantenimiento periódico de equipos	Pérdida de todo el servicio para usuarios internos y se puede quemar el activo	Se realiza un mantenimiento periódico de los equipos	Baja	Baja	Bajo
	6	Daño en medios de transmisión	No existen medios alternos para todos los casos Falta políticas de cableado estructurado	Pérdida temporal del servicio que brinda	Revisión y cambio de medios de transmisión viejos o defectuosos	Baja	Baja	Bajo
	7	Daño en el aire acondicionado	No existe una política de mantenimiento periódico de equipos	Calentamiento de equipos y posible daño de los mismos	Ninguna	Baja	Baja	Bajo

Tabla 6.5: Matriz del Riesgo de los Activos “Equipo Computacional Secundario” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Tecnológicas	8	Virus, troyanos, gusanos, etc.	No existe un monitoreo continuo para detectar posibles ataques.	Pérdida temporal del servicio que brinda	Se posee un buen antivirus en la empresa y se lo usa de la mejor manera	Baja	Baja	Bajo
			No existen suficientes seguridades para bloquear amenazas	Violación de la seguridad de información				
	9	Software desactualizado	No se cuenta con planes de migración de SO y de software de aplicación	Falla en la prestación de los servicios que ofrece el activo y pérdidas económicas	Ninguna	Baja	Baja	Bajo
	10	Software no licenciado	No se cuenta con licencias de todos los programas	Recesión de las actividades de la empresa	Se tiene un contrato de licenciamiento	Baja	Baja	Bajo

Tabla 6.6: Matriz del Riesgo de los Activos “RR.HH.”

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Ambientales	1	Terremotos /Sismos	El edificio donde se encuentra ubicado MEGADATOS S.A. no es antisísmico	Muerte de funcionarios o accidentados	Ninguna	Media	Media	Medio
			Falta de capacitación ante emergencias					
			Quito está en una zona sísmica					
	2	Erupciones Volcánicas	Falta de capacitación ante emergencias	Muerte de funcionarios o accidentados	Ninguna	Baja	Media	Bajo
			Quito se encuentra en una zona geográfica rodeado de volcanes					
	3	Deslizamientos	Falta de capacitación ante emergencias	Muerte de funcionarios o accidentados	Ninguna	Baja	Media	Bajo
			Quito se encuentra asentado en valles y quebradas					

Tabla 6.6: Matriz del Riesgo de los Activos “RR.HH.” (continuación)

TIPO	Nro	AMENAZAS	VULNERABILIDADES	IMPACTO/Acciones de Amenaza	ACCIONES DE MITIGACIÓN	Prob	Imp	NR
Humanas	1	Ausencia de Salida de Emergencias	El edificio no dispone de salidas de emergencia No existe una señalización adecuada de por dónde evacuar en caso de una emergencia	Muerte/accidentes de personal clave	Ninguna	Media	Media	Medio
	2	Muerte o ausencia del personal	No se tiene una política respaldos de personal	Corte temporal en los servicios que dan los equipos debido a que nadie sabe su funcionamiento	Ninguna	Baja	Media	Bajo
	3	Calamidades domesticas	Nadie esta excepto de que se pueda tener alguna eventualidad	Mal funcionamiento de equipos manejados por el empleado	Alguien mas realiza las funciones	Baja	Baja	Bajo
	4	Falta de capacitación al personal	No se tienen una política de capacitaciones periódicas	Desactualización	Ninguna	Media	Baja	Bajo