DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA PAVIMENTO UNIVERSAL S.A.

KORINA ISABEL CERVANTES BLANCO

PABLO ANTONIO GALLEGO MERCADO

UNIVERSIDAD DE LA COSTA, C.U.C.

DEPARTAMENTO DE POSTGRADOS

FACULTAD DE CIENCIAS ECONOMICAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN

BARRANQUILLA

2014

2013DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA PAVIMENTO UNIVERSAL S.A.

KORINA ISABEL CERVANTES BLANCO

PABLO ANTONIO GALLEGO MERCADO

Trabajo para optar al título de

Especialista en Auditoria de Sistemas de Información

UNIVERSIDAD DE LA COSTA C.U.C.

DEPARTAMENTO DE POSTGRADOS

FACULTAD DE CIENCIAS ECONOMICAS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN

BARRANQUILLA

2014

DEDICATORIA

Este Proyecto se los dedico a aquellas personas que confiaron en mí y me brindaron su apoyo incondicional y formaron parte de mi etapa de aprendizaje.

Y en especial a mis padres que son parte fundamental en mi enseñanza y a todas las personas que confiaron en mí, he hicieron parte de este proyecto.

PABLO ANTONIO GALLEGO MERCADO

DEDICATORIA

El presente trabajo es dedicado con mucho amor y cariño a quien han puesto todo el empeño, esfuerzo y sacrificio por lograr que yo llegara al nivel donde me encuentro: Mi Familia.

Son tantas las cosas que quiero expresar y no consigo las palabras de cómo describir lo alegre y satisfecho que me siento por haber culminado otra meta más.

Quiero dedicarle este trabajo de Grado en especial a mi madre Diana que me enseño la disciplina y la constancia en los estudios, asumiste el reto de apoyarme y brindarme siempre esa mano amiga al estar conmigo en los momentos más difíciles. Con tu amor y apoyo especial me has animado en los momentos en los que más lo necesitaba. Te pido que me sigas ayudando para poder seguir alcanzo todas las metas que me faltan alcanzar.

KORINA ISABEL CERVANTES BLANCO

AGRADECIMIENTOS

Al Señor Roberto Mario Herrera Jefe de Sistemas de Pavimento Universal S.A. el cual nos brindó todo su apoyo para la elaboración del proyecto.

De igual forma al Sr. Luis Rodríguez Jefe de Dpto. Contabilidad que nos brindó mucha orientación en cada paso del proyecto y a todos a aquellas personas que formaron parte del proceso y aportaron sus conocimientos.

Y a la gerencia de la compañía que sin su apoyo este proyecto no se hubiera llevado a cabo.

PABLO ANTONIO GALLEGO MERCADO

AGRADECIMIENTOS

De manera respetuosa expreso mis más profundos agradecimientos, ante todo a Dios por permitirme realizar el proyecto de grado, que con todo el esfuerzo y dedicación, en aras de continuar con mi crecimiento profesional creando una visión de mujer emprendedora y apta para desempeñar un excelente cargo en el futuro.

De manera complacida pude llevar a cabo; con la valiosa colaboración del profesor Víctor Montaño especialista en Auditoria en Sistemas de Información de la Corporación Universitaria de la Costa CUC, por aportar grandes ideas para el mejoramiento y desarrollo de mi proyecto el cual es de mi completa satisfacción presentarles, no obstante por su pertinente y adecuada asesoría en la elaboración del mismo. De igual forma a mi amado cónyuge Leonardo Reyes Jiménez que desde que se encuentra junto a mí me ha apoyado económica y emocionalmente dándome ánimo y fuerzas cuando ha sido necesario, para poder cumplir con la meta de ser especialista en Auditoria en Sistemas de Información de la prestigiosa Corporación universitaria de la Costa CUC; y en mí rol como madre y esposa de la mejor manera posible durante esta importante etapa de mi vida.

KORINA ISABEL CERVANTES BLANCO

RESUMEN

El presente trabajo de grado, tuvo como propósito identificar los diferentes amenazas a las que se encuentran expuestas las compañías en la actualidad en este caso se utilizaron marcos de trabajo como Cobit y estándares o normas como ISO 24762 o la NISP SP 800-34 en las cuales nos basamos para la elaboración de un plan de recuperación de desastre adecuado para la compañía.

De igual forma se identificaron los activos de la compañía que se encontraban más vulnerables a posibles fallas que podrían interrumpir el normal funcionamiento de todos sus procesos. Estos análisis se llevaron a cabo mediante entrevistas al personal de tecnología y de apoyo de las demás aéreas los cuales arrojaron muchas deficiencias en la seguridad de la información como se puede observar en la matriz de riesgo.

Si la compañía sigue detalladamente la estructura que se propuso para el plan de recuperación de desastres estará más blindada a posibles fallas en su plataforma tecnológica y de seguridad respectivamente.

PALABRAS CLAVE: Identificar amenazas, marcos de trabajo, estándares, matriz de riesgo, normas, plataformas tecnológicas, procesos.

ABSTRACT

This degree work, aimed to identify the various threats that companies are exposed today in this case frameworks and standards such as Cobit or ISO 24762 standards as NISP SP 800-34 or were used in the which we rely for the development of a suitable recovery plan disaster for the company.

Similarly the assets of the company who were more vulnerable to possible failures that could disrupt the normal functioning of all processes were identified. These analyzes were conducted by interviewing staff and technology support from other airlines which threw many deficiencies in the information security as shown in the risk matrix.

If the company continues to detail the structure proposed for disaster recovery plan will be more shielded from possible flaws in its technology platform and security respectively.

KEYWORDS: Identify threats, frameworks, standards, risk matrix, standards, technological platforms, processes.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

INTRODUCCIÓN

En la actualidad un gran porcentaje de las compañías en mayor o menor grado basan toda su operación en plataformas tecnológicas, lo que esto quiere decir que su funcionamiento es gracias a la tecnología lo que conlleva a que estén expuestas a múltiples amenazas en su entorno.

En este caso la compañía PAVIMENTO UNIVERSAL S.A. en su constante actualización en sus diferentes plataformas ha mostrado interés en minimizar sus riesgos tecnológicos.

De igual forma este proyecto detallara un análisis de la situación en que se encuentra la infraestructura tecnológica de la compañía y de igual forma el diseño de un plan de recuperación de desastres adecuado. Se sabe por teoría que un plan de recuperación de desastres es la capacidad que se tiene para responder a cualquier interrupción de las actividades críticas de la compañía.

Para realizar un correcto análisis de la infraestructura tecnológica se utilizara como base la entrevista como un instrumento para obtener información vital para el proyecto. Y en paralelo se utilizaran estándares, guías, normas para el diseño de un plan de recuperación de desastres.

1. PLANTEAMINETO DEL PROBLEMA

Cada compañía debe contar con buenos procedimientos y que se encuentren estandarizados ya que estos son de gran importancia para el entendimiento de cada uno de los procesos, para poder responder oportunamente a cada uno de los incidentes que se presenten como lo son: robos, sabotaje, incendios, inundaciones, accesos no autorizados a la compañía, etc. Que pueden afectar el buen funcionamiento del departamento de sistemas de PAVIMENTO UNIVERSAL S.A.

De igual forma cada compañía debe responder de manera adecuada en cualquier tipo de eventualidad ya sea natural, tecnológica o humana, deberán estar preparadas para enfrentar cualquier emergencia. Para esto existen un conjunto de estándares, guías y normas que se tendrán en cuenta para prevenir este tipo de situaciones.

Este tipo de planes traen buenos beneficios para las compañías como por ejemplo mayor confianza en cada una de las operaciones que estas realicen, competitividad en el mercado, confianza a sus proveedores y clientes.

Lo cual surgen las siguientes interrogantes o premisas:

De acuerdo a la situación actual de la compañía cual sería la estructura de un plan de recuperación de desastres adecuado para PAVIMENTO UNIVERSAL S.A.

Identificar las normas, guías, estándares, buenas prácticas que se pueden utilizar en la realización de un plan de recuperación de desastres.

Identificar los activos tecnológicos que son más vulnerables en la compañía y diseñar un plan de pruebas para el plan de recuperación de desastres para PAVIMENTO UNIVERSAL S.A.

2. JUSTIFICACIÓN

La tendencia a las que están sometidas las compañías tanto climáticas, comerciales, tecnológicas y gubernamentales a diferencia a las de hace unos años todavía siguen expuestas a riesgos que se deberán administrar de manera continua para minimizar el impacto y la probabilidad de que este vuelva a presentarse y de esta manera garantizar una buena continuidad de cada uno de los servicios.

El plan de recuperación de desastres fortalecerá a la compañía y mantendrá un plan de acción actualizado para el momento en que se necesite en el departamento de sistemas.

En el caso de PAVIMENTO UNIVERSAL S.A. es prioritario documentar cada uno de los activos que hacen parte del core el negocio para determinar los pasos para la recuperación ante un desastre.

Para ello se cuentan con marcos de trabajo como COBIT estándares, ISO 24762, NIST SP 800-34, etc. Los cuales podremos tomar para poder combinarlos para obtener un estándar propio los cuales se ajusten a las necesidades de la compañía, para desarrollar eficientemente el plan de recuperación de desastres.

3. DELIMITACIÓN

3.1. DELIMITACIÓN TEMPORAL

Este proyecto se realizara en el periodo comprendido entre Junio y Julio del 2012.

3.2. DELIMITACIÓN ESPACIAL

Este proyecto se realizara en la empresa PAVIMENTO UNIVERSAL S.A. en su oficina principal Barranquilla, Colombia.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

❖ Diseñar un plan de recuperación de desastres conveniente para la compañía PAVIMENTO UNIVERSAL S.A.

4.2. OBJETIVOS ESPECÍFICOS

❖ Identificar los activos que tienen mayor vulnerabilidad en la compañía PAVIMENTO UNIVERSAL S.A.

❖ Diseñar un plan de recuperación de desastres acorde con las necesidades de la compañía PAVIMENTO UNIVERSAL S.A.

❖ Reunir conceptos importantes de los estándares, normas, buenas prácticas o guías para el desarrollo de un plan de recuperación de desastres para la compañía PAVIMENTO UNIVERSAL S.A.

❖ Construir un plan de pruebas para el plan de recuperación de desastres para la compañía PAVIMENTO UNIVERSAL S.A.

5. MARCO TEORICO

5.1. PLAN DE RECUPERACIÓN DE DESASTRES

5.1.1. QUE ES PLAN DE RECUPRACIÓN DE DESASTRES

“Un DRP es un sistema de información centrado en un plan diseñado para restaurar la operatividad del sistema de destino, aplicación o instalación de infraestructura informática en un sitio alterno después de una emergencia.”[1]

Esto quiere decir que toda compañía deberá tener contemplado un plan de recuperación de desastres teniendo en cuenta su ubicación e infraestructura tecnológica para diseñarlo adecuadamente a las necesidades de negocio.

[1]NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems, Pag. 24

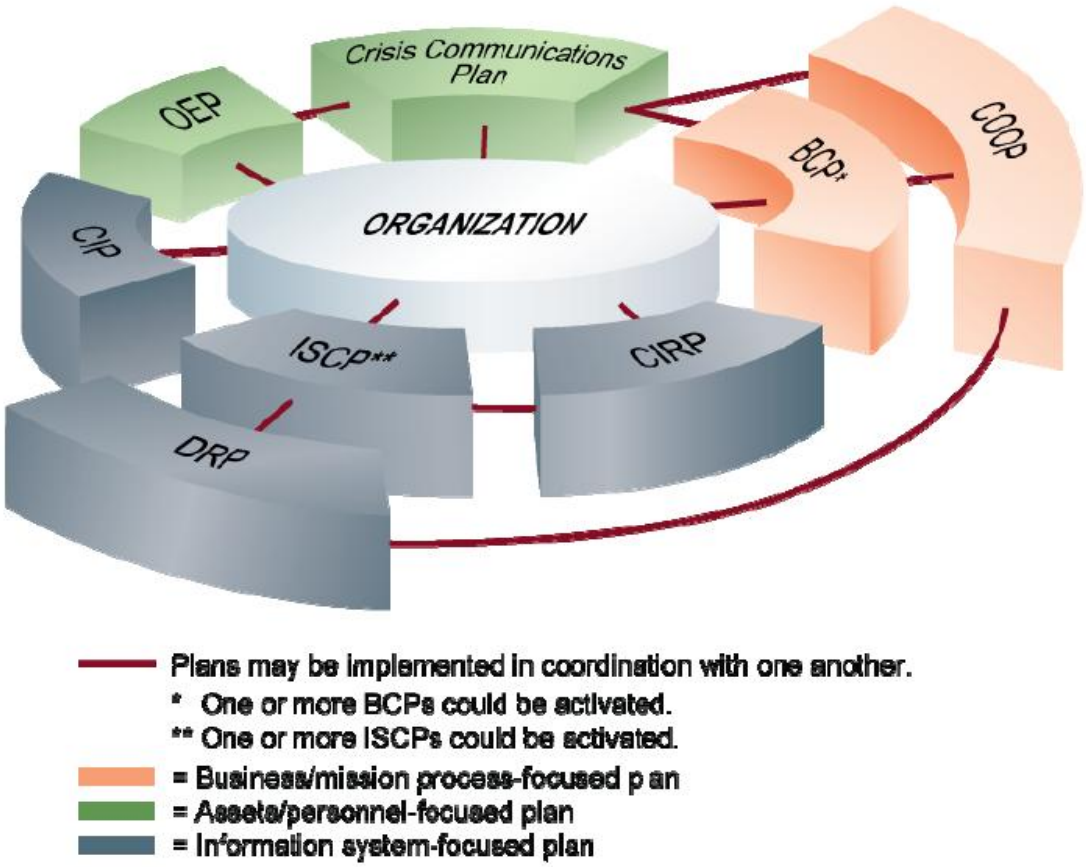

Figura 1: Relaciones con los planes de contingencia

En el anterior grafico de acuerdo NIST 800-34, muestra la interrelación de cada plan a medida que se implementan para responder al evento según corresponda a sus respectivos ámbitos.

5.1.2. IMPORTANCIA DEL PLAN DE RECUPERACIÓN DE DESASTRES

Los últimos acontecimientos mundiales, nos han hecho evaluar fuertemente que aquí en nuestro país son mínimas las previsiones que tomamos para salvaguardar las compañías. Sabemos que las empresas hoy en día son un ente vivo y en continuo cambio es por eso que debemos adoptar una postura de dinámica ante estos cambios.

Para eso es importante que no solo cuenten con los documentos si no que se conviertan en una constante a lo largo de la vida de la compañía, apoyada claro está por la alta gerencia que de igual forma ejercerá control en cada uno de los procesos.

5.2. PROCESOS QUE SE DEBEN SEGUIR EN LOS PLANES DE CONTINGENCIA

"En esta sección se describe el proceso para desarrollar y mantener un sistema eficaz de información sobre el plan de contingencia. El proceso que se presenta es común a todos los sistemas de información"[2]. Los siete pasos en el proceso son:

1. Desarrollar la política de planificación de contingencia

[2]Ibíd. Pág. 27.

2. Llevar a cabo el análisis de impacto en el negocio (BIA)

3. Identificar los controles preventivos

4. Crear estrategias de contingencia

5. Desarrollar un sistema de información del plan de contingencia

6. Plan de pruebas

7. Plan de mantenimiento.

5.3. PLAN PARA LA CONTINUIDAD DEL NEGOCIO

"Inicialmente las empresas consideraron la importancia de poseer planes para garantizar la continuidad del negocio, solamente buscando cumplir con ciertas regulaciones en algunos países del mundo. Pero con el pasar del tiempo y considerando la rapidez con que se necesitan hacer los negocios hoy en día, junto con la complejidad asociado a los sistemas de información, han influido para que la gestión de la contingencia haya llegado a ser una variable muy importante con el fin de lograr que las empresas sobrevivan en un ambiente cada vez más dinámico y con alto riesgo"[3].

Por otra parte, todos sabemos que los desastres pueden ocurrir en cualquier

[3] http://www.sisteseg.com/sindustrial.html

momento, es por eso que se requiere un plan detallado que proteja tanto las personas, como la infraestructura, edificios, aplicaciones, servicios con el fin de poderlos retornar a su normal operación tan pronto como sea posible.

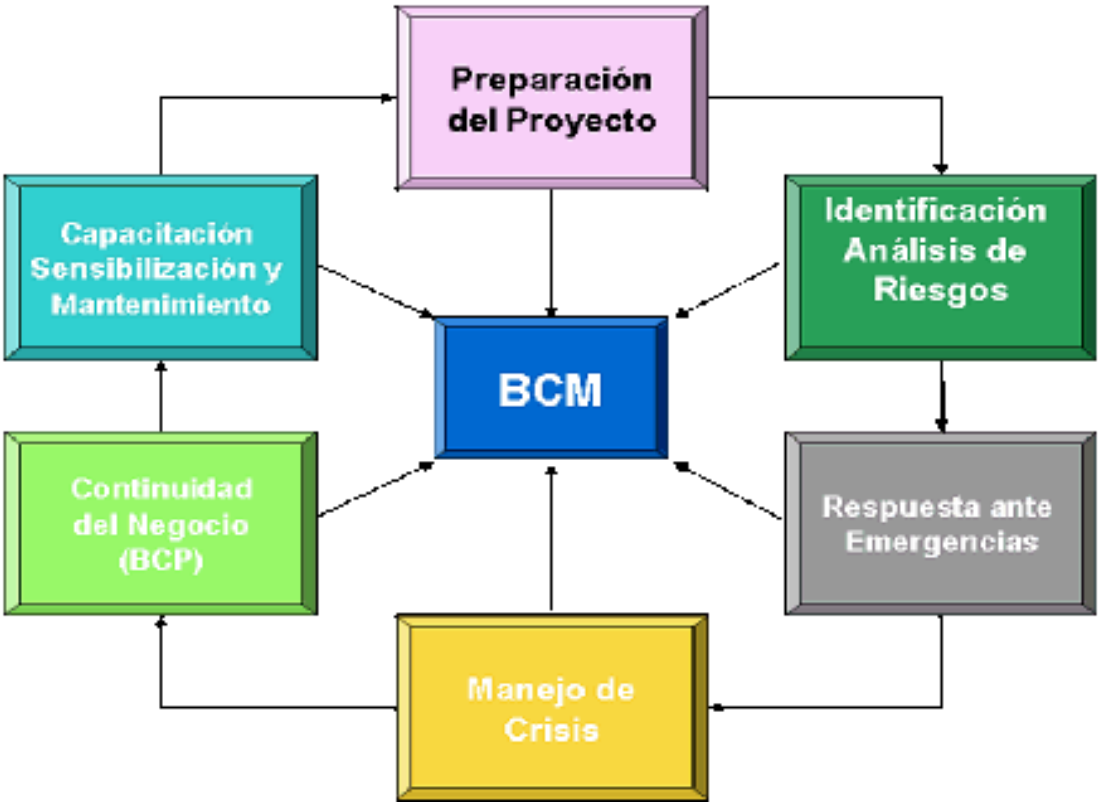

Figura 2: Diferentes fases del plan de continuidad

5.4. FASES DE UN BCP o DRP

Las fases tradicionalmente consideradas de un BCP son:

- Gestión e iniciación del proyecto: Establece un equipo para el proyecto y una estrategia para desarrollar el plan.
- Análisis de impacto sobre el negocio BIA: Identifica los aspectos críticos relacionadas con el máximo tiempo en que un proceso puede estar no disponible.
- Estrategia de recuperación: Identifica y selecciona las apropiadas alternativas de recuperación para lograr los tiempos requeridos definidos en el AIN.
- Diseño del plan y desarrollo: Se trata en esta fase de documentar las estrategias de recuperación.
- Prueba, Mantenimiento, y entrenamiento: La idea es esta fase es probar las estrategias de recuperación anteriormente definidas, manteniendo actualizado el plan y dándolo a conocer a todos los empleados.

5.5. QUÉ ES CONTINUIDAD DEL SERVICIO

"La continuidad del servicio involucra capacidades tácticas y estratégicas pre aprobadas por la dirección de una entidad para responder a incidentes e interrupciones del servicio con el fin de poder continuar con sus operaciones a un nivel aceptable previamente definido"[4].

5.5.1. PRODUCTOS QUE LO COMPONEN

- Business Impact Analysis (Impacto de Análisis del Negocio).
- Risk Assesment (Evaluación o Valoración de Riesgos).
- Estrategias de Continuidad.
- Estructura Organizacional para la Continuidad (Roles, responsabilidades y procedimientos).
- Procesos de Continuidad.
- Plan de Pruebas del Plan de Continuidad.

"Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia

[4]BS25999. Pág. 6

requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias."[5]

Cobit también es un marco de trabajo que nos sirve de referencia para fortalecer controles con respecto a la continuidad del servicio en una organización, en el objetivo de control DS4.1 Marco de Trabajo de Continuidad de TI el trabajo principal de este objetivo es de guiar tanto al plan de recuperación de desastres como también al plan de contingencias. Tomando en cuenta la estructura organizacional de la compañía y los roles y responsabilidades de cada proveedor.

Las etapas que debe contener un plan de recuperación de desastres es el siguiente:

- Identificar y evaluar cada uno de los riesgos
- Priorizar cada una de las aplicaciones
- Establecer los requerimientos de recuperación
- Documentación
- Verificar e implementar el plan de recuperación de desastres
- Mantenimiento del plan

[5]COBIT ® 4.1, IT Governance Institute, DS4.1, Pág. 121.

5.6. CONOCIENDO A LA EMPRESA Y SUS ACTIVOS DE TECNOLOGIA BASICOS

5.6.1. HISTORIA DE LA EMPRESA

En **Pavimento Universal** desde su fundación hemos encaminado todos nuestros esfuerzos para convertirnos en una empresa líder y comprometida con el desarrollo del país, en cuanto a la construcción y administración de proyectos y obras de Ingeniería civil y de urbanismo.

La actividad principal de la empresa consiste en la prestación de servicios profesionales y la ejecución de obras relacionadas con la arquitectura e ingeniería en todas sus ramas, en la producción y optimización de pavimento asfaltico y concreto; el desarrollo de planes de urbanismo para vivienda de todo género, comercio, industria, etc.

Nuestro constante proceso de mejoramiento en cuanto a personal y tecnología, han hecho que Pavimento Universal cumpla con los más altos estándares de calidad en la construcción de vías, producción de mezclas asfálticas; construcción de proyectos urbanísticos y obras institucionales; ingeniería ambiental y desarrollos arquitectónicos en general.

A lo largo de 28 años de servicio al país, **PAVIMENTO UNIVERSAL S.A,** ha diseñado y construido múltiples proyectos viales en Colombia; proyectos que han generado futuro y desarrollo a la población existente en dichos lugares.

Desde el año de 1984 se han construido obras que son gran orgullo para nosotros y muestran la calidad de nuestros productos y servicio.

Es importante mencionar en esta parte que en Pavimento Universal desarrollamos nuestros proyectos arquitectónicos y de ingeniería con maquinaria propia. Brindamos el mejor servicio con procesadores de agregados.

El gran número de obras y proyectos ejecutados nos han permitido además ganar un gran número de clientes los cuales han quedado satisfechos con el servicio y/ o producto ofrecido por nuestro empresa. Entre los principales clientes que podemos resaltar tenemos:

- Agrecon
- Consorcio vía al mar
- Consorcio Ciénaga-Barranquilla
- Envías
- Sociedad Portuaria de Barranquilla
- Roberto Donado Arce y Cía.
- Consorcio Dumar- Sofan
- Gercon.
- Unión Temporal Prosperidad 2011
- Malla vial Departamental

5.6.2. MISIÓN

Pavimento Universal se creó como una necesidad del mercado en la explotación de agregados, producción de concreto asfáltico y construcción de obras de Ingeniería Civil.

Durante la ejecución de estas actividades la organización aporta al desarrollo del país, la calidad de vida de los trabajadores satisfacción de clientes internos y externos.

5.6.3. VISIÓN

Alcanzar reconocimiento a nivel nacional en la prestación de servicios de Ingeniería Civil y a su vez incrementar el desarrollo de obras de urbanismo manteniendo el cumplimiento de los requisitos de calidad y otros especificados por el cliente en las obras de ingeniería civil y en el suministro de concreto asfáltico.

5.6.4. ORGANIGRAMA

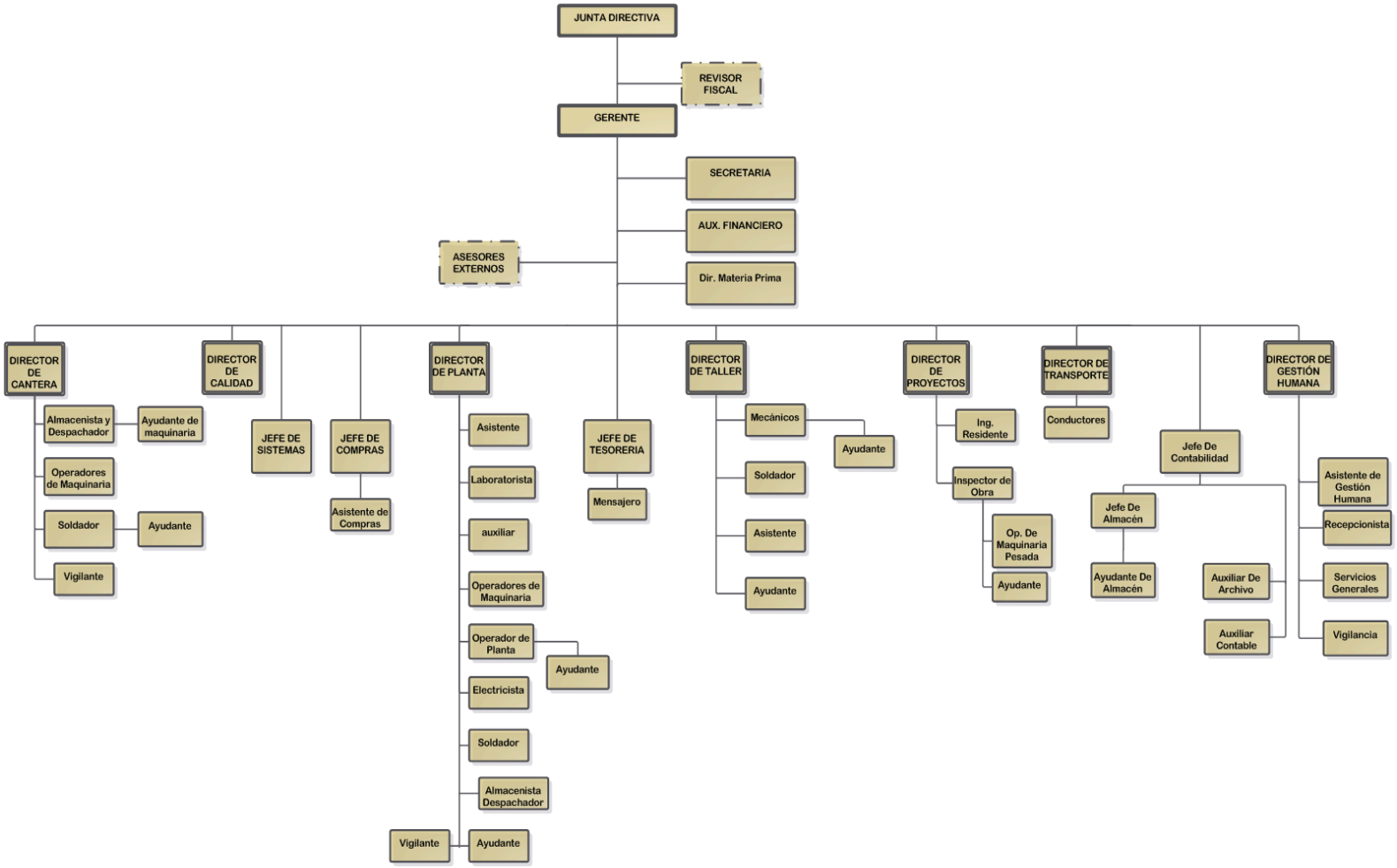

Figura 3: Organigrama General

5.6.5. MAPA DE RED

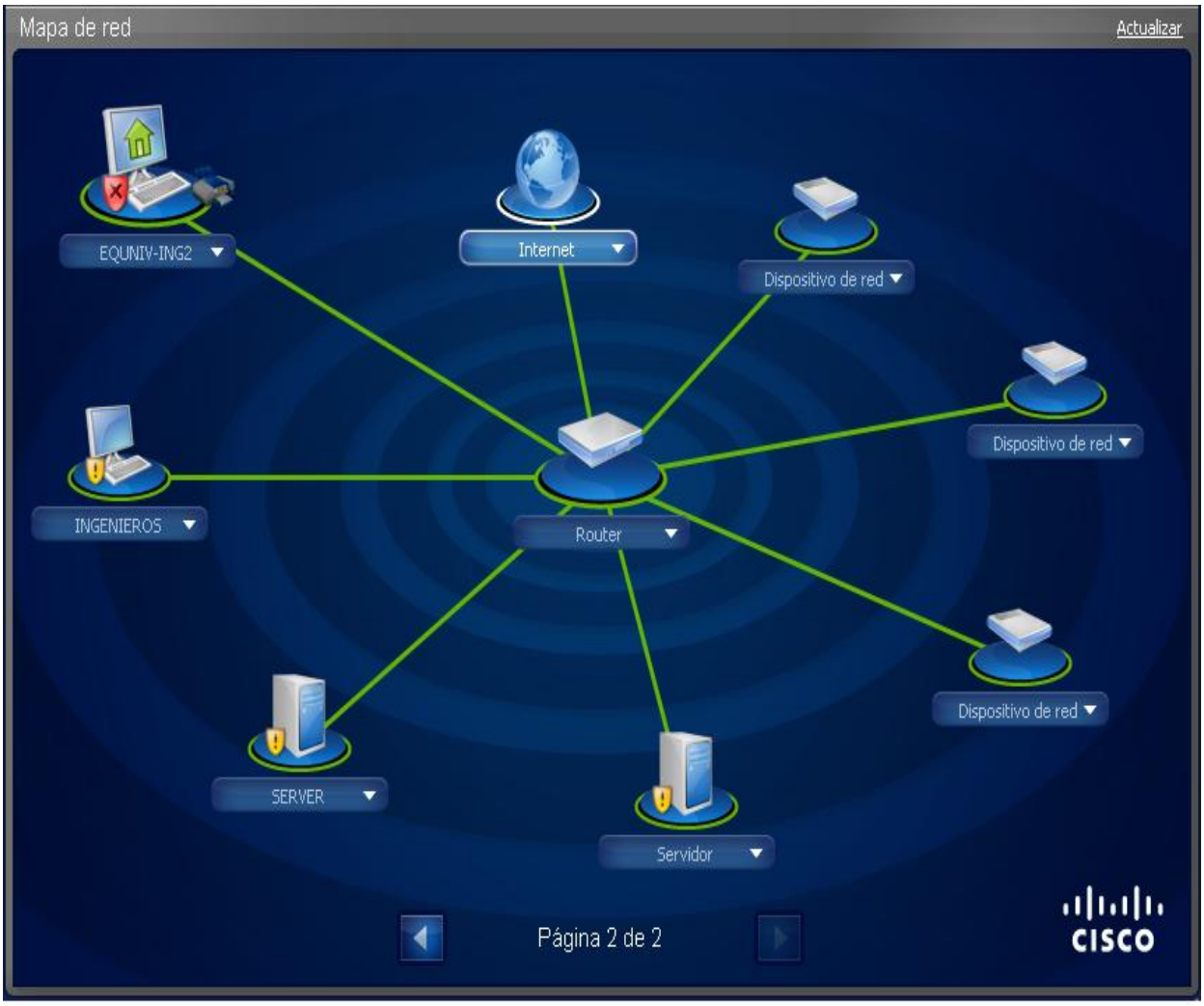

Figura 4: Mapa de red de los servidores

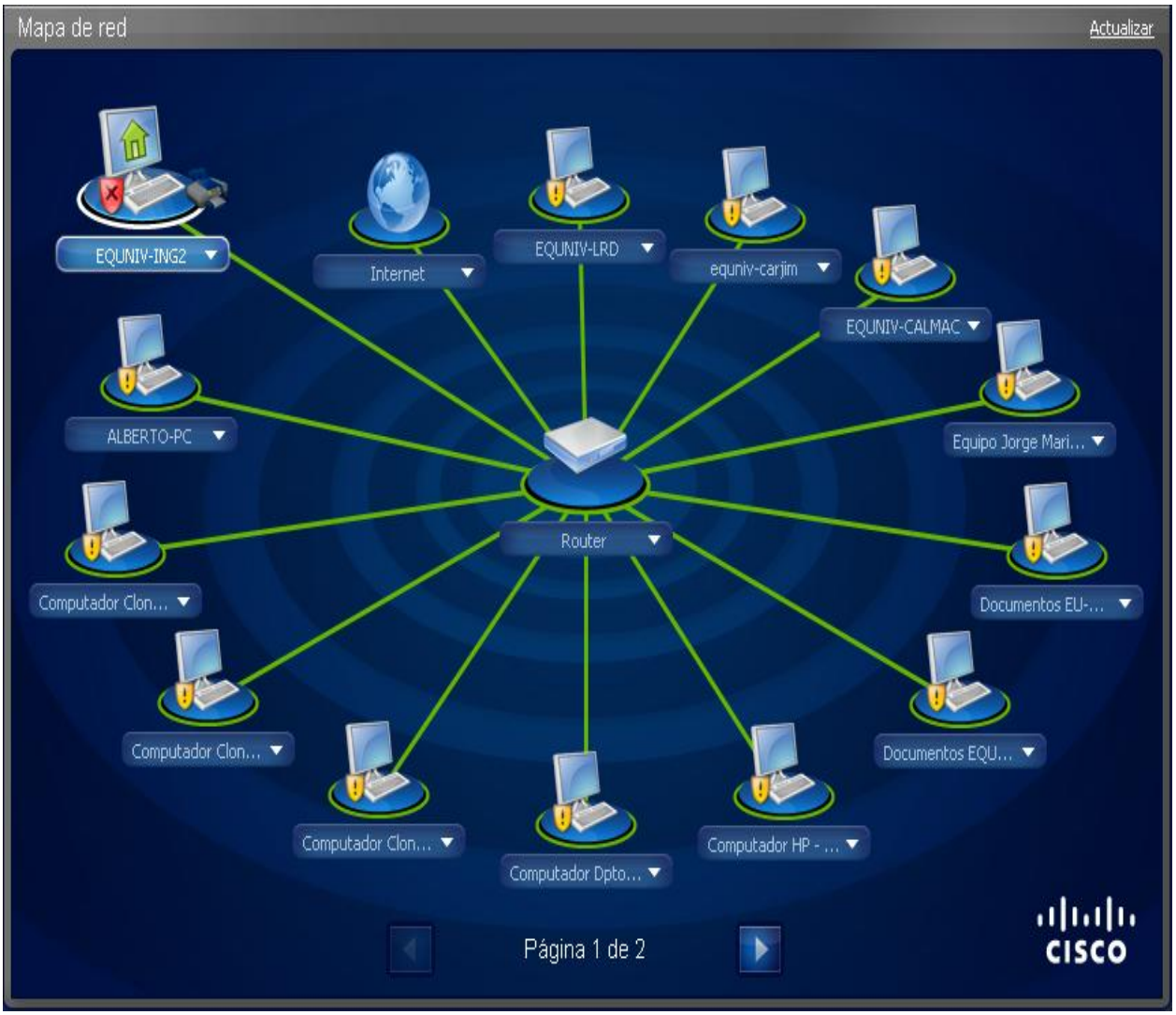

Figura 5: Mapa de red de usuarios

6. MARCO CONCEPTUAL

Amenazas: La fuente de daño potencial o una situación que potencialmente cause pérdidas.

Arquitectura de Información: es la ciencia encargada de efectuar la planeación estratégica para la creación de un sistema de información contemplando desde los diagramas estructurales de la infraestructura utilizada según la necesidad, sistema de navegación, usabilidad, carga y satisfacción de la necesidad de un negocio especifico.

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

Factores de Riesgo: Manifestaciones o características medibles u observables de un proceso que indican la presencia de Riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Impacto: Es el efecto del riesgo sobre la organización (ingresos, reputación, satisfacción de clientes, emisión de la información, etc.). Se expresa cualitativa o cuantitativamente, sea este una pérdida, perjuicio o desventaja.

Incidente: La fuente de daño potencial o una situación que potencialmente cause pérdidas.

Infraestructura tecnológica: Es el conjunto de hardware y software sobre el que se asientan los diferentes recursos que la compañía necesita tener en funcionamiento para poder llevar a cabo toda su actividad.

Plan de Contingencia: Parte del plan de manejo de riesgos que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la entidad.

Riesgo: Riesgo se refiere a un hecho, una acción u omisión que podría afectarla capacidad de una Entidad para lograr sus objetivos de proceso, de negocio, o estrategias. Considerar la ocurrencia latente o potencial de acontecimientos negativos o inesperados así como la ausencia o sub-aprovechamiento de oportunidades.

Valoración del Riesgo: Es el resultado de confrontar la evaluación del riesgo con los controles existentes.

Vulnerabilidad: hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

7. DISEÑO METODOLOGICO

7.1. TIPO DE ESTUDIO

Descriptivo

Este proyecto es de tipo descriptivo porque en él se describen características fundamentales de fenómenos homogéneos.

7.2. METODO DE ESTUDIO

Deductivo – Inductivo

Deductivo por qué parte del conocimiento que se inicia por la observación de fenómenos de carácter general con el propósito de llegar a conclusiones de carácter particular

Inductivo por qué parte del conocimiento que se inicia por la observación de fenómenos particulares con el propósito de llegar a conclusiones y premisas de carácter general que pueden ser aplicadas a situaciones similares.

7.3. TECNICAS DE RECOLECCIÓN DE INFORMACIÓN

7.3.1. Técnica de recolección de la información primaria

Se trabajó con la observación directa producto de la realidad**.**

7.3.2. Técnica de recolección de la información secundaria

Se trabajó con las fuentes de segunda mano tales como libros, revistas, Internet.

7.4. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

7.4.1. Instrumentos de recolección de información primaria

El instrumento a utilizar es la entrevista.

7.4.2. Instrumentos de recolección de información secundaria

Como instrumento de recolección de información secundaria el trabajo se soportó en los siguientes estándares, buenas prácticas, normas, y/o guías

8. PROPUESTA

PLAN DE RECUPERACIÓN DE DESASTRES PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA PAVIMENTO UNIVERSA S.A.

De acuerdo a los estándares establecidos para la continuidad del negocio se diseñó el siguiente plan de recuperación de desastres para la empresa PAVIMENTO UNIVERSAL S.A. basados en el estándar Contingency Planning Guide for Federal Information Systems (NIST) y The Institute For Continuity Management(DRII), el cual proponemos la siguiente estructura:

- Análisis del ambiente interno
- Análisis de riesgo
- Análisis de impacto
- Elección de estrategias para la recuperación
- Documentación de procesos
- Plan de prueba
- Socialización
- Mantenimiento

A continuación representamos gráficamente cada uno de los pasos y/o actividades que se deben seguir para implementar de manera efectiva un plan de recuperación de desastres para la compañía.

Figura 6: Estructura propuesta para un plan de recuperación de desastres.

8.1. ANÁLISIS DEL AMBIENTE INTERNO

Para conocer mejor cada una de las actividades que cumple cada miembro del Dpto. de Sistemas y los componentes tecnológicos con que cuenta la compañía lo detallaremos a continuación.

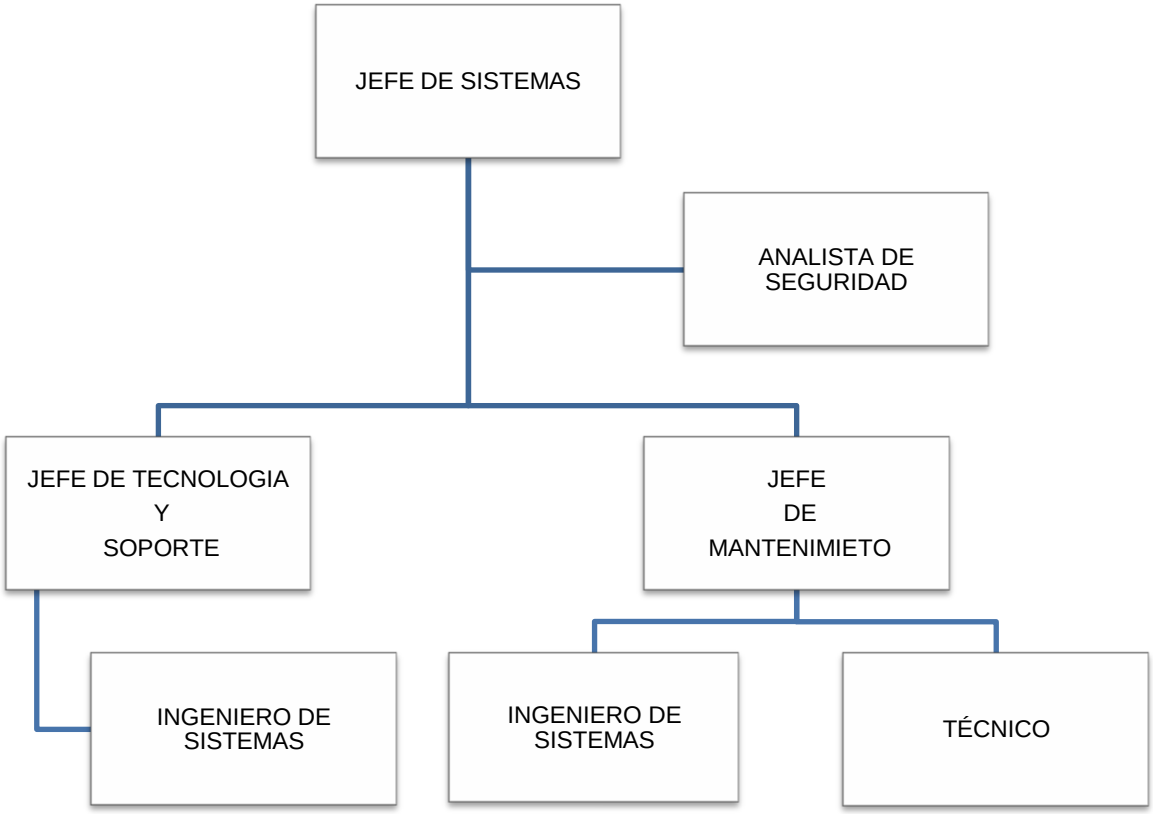

Figura 7: Organigrama General del Dpto. de Sistemas.

A continuación detallaremos los componentes tecnológicos tanto hardware y software con que cuenta la compañía actualmente.

- Cuentan con dos servidores situados en la sede principal de la compañía.

- Se cuentan con 17 terminales de trabajo ubicadas en sus diferentes aéreas tanto administrativas y de producción.
- Se cuentan con dos bases de datos del fabricante ORACLE y son utilizadas en las aplicaciones principales de la compañía.
- Actualmente se está utilizando un ERP de la compañía OFIMATICA S.A. y un sistemas de vigilancia Detektor GPS para el Monitoreo y controlde la compañía TRACKER DE COLOMBIA el cual es una aplicación web con un tercero.

8.2. ANÁLISIS DE RIESGO

Para este proyecto se realizara un análisis de cada una de las amenazas con sus respectivas vulnerabilidades que puedan materializarse en el Dpto. de sistemas de la compañía.

"En la siguiente figura se muestra las diferentes amenazas que puede afrontar una compañía de acuerdo al factor que lo inicia ya sean humanas o por factores naturales y ambientales"[6].

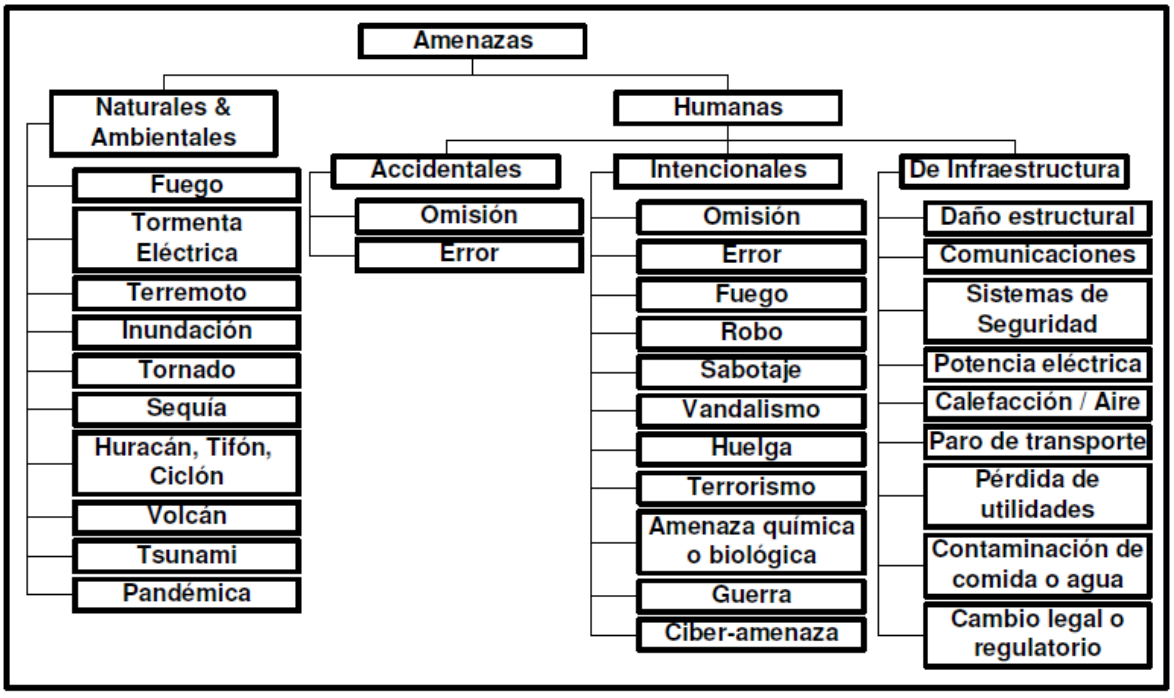

Figura 8: Tipos de amenazas.

[6]Ing. Rodrigo, Ferrer V. Plan de Continuidad para el Negocio.Sisteseg, 2009. P. 21

“En el numeral A.5.3.2 La identificación del riesgo debe incluir la siguientes tipos de riesgos potenciales. Esta lista no es exhaustiva, pero refleja las categorías generales que deben ser evaluadas en la identificación de los peligros”[7].

(1) De origen natural peligros que pueden ocurrir sin la influencia de las personas y tienen un impacto potencial directo o indirecto en la entidad (personas, los bienes, el medio ambiente), como el siguiente:

(A) Los riesgos geológicos (no incluye los asteroides, los cometas, meteoros)

i.Terremoto

ii.Tsunami

iii.Volcán

iv. Deslizamientos de tierra, lodo, hundimientos

v glaciar, iceberg

(B) los riesgos meteorológicos

i. Inundaciones, crecidas repentinas, marejada

ii. Sequía

iii. Fuego (bosque, campo, urbano, forestal, urbano interfaz)

[7]NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, Pág.11

iv. Nieve, hielo, granizo, aguanieve, la avalancha de

v Tormentas, ciclones tropicales, huracanes, tornados, chorro de agua, polvo / arena tormenta

VI. Las temperaturas extremas (calor, frío)

vii. Los rayos

VIII. Hambre

IX. Tormenta geomagnética

(C) Los riesgos biológicos

i. Las enfermedades emergentes de impacto que los seres humanos o animales [Peste, la viruela, el ántrax, virus del Nilo Occidental, la fiebre aftosa, el SARS, la enfermedad pandémica, La encefalopatía espongiforme bovina (enfermedad de las vacas locas)]

ii. Animales o insectos plaga o daño

(2) eventos causados por el hombre tales como los siguientes:

(A) accidental

i. De materiales peligrosos (líquidos explosivos, inflamables, gases inflamables, sólidos inflamables, oxidantes, veneno, radiológica, corrosivo) derrame o liberación

ii. Explosión / incendio

iii. Transporte de accidentes

iv. Construcción / estructura de colapso

v de energía / potencia / utilidad de fracaso

VI. Combustible / recurso escasez

vii. Aire / contaminación del agua, la contaminación

VIII. Estructura de control de agua / presa / el fracaso del dique

IX. Las cuestiones financieras, la depresión económica, la inflación, colapso del sistema financiero

x. Sistemas de comunicaciones interrupciones

XI. Desinformación

(B) intencional

i. Terrorismo (explosivos, armas químicas, biológicas, radiológicas, nuclear, cibernético)

ii. Sabotear

iii. Disturbios civiles, disturbios públicos, histeria de masas, motín

iv. Ataque enemigo, la guerra

v Insurrección

VI. Huelga o conflicto laboral

vii. Desinformación

VIII. La actividad criminal (vandalismo, incendio, robo, el fraude, la malversación, el robo de datos)

IX. Impulso electromagnético

x. La seguridad física o la información incumplimiento

XI. Violencia en el trabajo

xii. Producto defectuoso o contaminación

xiii. Acoso

XIV. Discriminación

(3) Eventos Tecnológico-causados que pueden no estar relacionadas con eventos naturales o causados por el hombre, tales como las siguientes: (A) una computadora central, mainframe, el software, o la aplicación (Interna / externa)

(B) el equipo de apoyo auxiliar

(C) Telecomunicaciones

(D) La energía / servicios públicos

DEPARTAMENTO DE SISTEMAS						
Código Amenaza	**Descripción Amenaza**	**Código Vulnerabilidad**	**Descripción Vulnerabilidad**	**Probabilidad**	**Impacto**	**Valoración**
A01	Acceso físico no autorizado	V1	Construcción deficiente de edificios (v.gr. protección inadecuada de puertas, ventanas, etc.)	Bajo	Medio	Bajo
		V14	Acceso no supervisado a las oficinas/edificios/instalaciones de la compañía	Bajo	Medio	Bajo
		V22	Administración indebida de mecanismos de acceso físico a las instalaciones de la compañia (v.gr. copias de tarjetas de acceso, uso compartido de tarjetas de acceso, etc.)	Bajo	Alto	Bajo
		V48	Ausencia de mecanismos de control de acceso físico a áreas restringidas de la compañia (v.gr. centros de cómputos, cuartos de cableado, operaciones, etc.).	Alto	Alto	Alto
		V49	Ausencia de mecanismos de control de acceso físico a las instalaciones(v.gr. edificio, instalaciones, oficinas, etc.)	Bajo	Alto	Bajo
		V56	Ausencia de personal de seguridad física (vigilancia)	Bajo	Bajo	Bajo
		V63	Falta de mecanismos de protección física de las instalaciones(v. gr. edificio, puertas y ventanas)	Alto	Alto	Alto
		V121	Personal de seguridad física no capacitado	Bajo	Bajo	Bajo

		V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)	Alto	Alto	Alto
		V159	Falta de supervisión de mecanismos de monitoreo	Alto	Medio	Alto
		V244	Procedimientos de control de acceso físico deficientes	Bajo	Bajo	Bajo
		V185	Inexistencia de bitácoras de acceso a las instalaciones y áreas restringidas de la compañía.	Bajo	Bajo	Bajo
		V178	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información	Alto	Alto	Alto
		V282	Uso inadecuado o descuidado del control de acceso físico al edificio y oficinas.	Bajo	Bajo	Bajo
A02	Ausencia / Interrupción total o parcial del aire acondicionado	V140	Falla del aire acondicionado	Bajo	Medio	Bajo
		V144	Fallas de mantenimiento	Bajo	Bajo	Bajo
		V157	Falta de mecanismos de control de fluctuaciones de energía	Alto	Alto	Alto
		V167	Fluctuaciones Eléctricas	Alto	Alto	Alto
		V197	Los equipos de control ambiental no reciben mantenimiento preventivo adecuado y suficiente (v.gr. componentes de TI, sistemas contra incendios, de suministro de energía, etc.).	Bajo	Bajo	Bajo

		V202	Mantenimiento insuficiente a la red de energía y tableros de control	Bajo	Alto	Bajo
		V203	Mantenimiento insuficiente de controles medioambientales	Bajo	Bajo	Bajo
		V204	Mantenimiento insuficiente de las instalaciones	Bajo	Bajo	Bajo
		V255	Red energética inestable	Alto	Alto	Alto
		V264	Susceptibilidad de los recursos de TI a variaciones de temperatura	Alto	Alto	Alto
		V265	Susceptibilidad de los equipos a variaciones de voltaje	Alto	Alto	Alto
		V271	Uniones deficientes de cables de energía	Bajo	Bajo	Bajo
		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Bajo	Alto	Bajo
A03	Ausencia / Interrupción total o parcial en el suministro eléctrico	V138	Falla de elementos de soporte (UPS)	Bajo	Bajo	Bajo
		V144	Fallas de mantenimiento	Bajo	Bajo	Bajo
		V157	Falta de mecanismos de control de fluctuaciones de energía	Alto	Alto	Alto
		V167	Fluctuaciones Eléctricas	Alto	Alto	Alto
		V197	Los equipos de control ambiental no reciben mantenimiento preventivo adecuado y suficiente (v.gr. componentes de TI, sistemas contra incendios, de suministro de energía, etc.).	Bajo	Bajo	Bajo

		V202	Mantenimiento insuficiente a la red de energía y tableros de control	Bajo	Medio	Bajo
		V203	Mantenimiento insuficiente de controles medioambientales	Bajo	Medio	Bajo
		V204	Mantenimiento insuficiente de las instalaciones	Bajo	Medio	Bajo
		V255	Red energética inestable	Alto	Alto	Alto
		V265	Susceptibilidad de los equipos a variaciones de voltaje	Alto	Alto	Alto
		V271	Uniones deficientes de cables de energía	Bajo	Bajo	Bajo
		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Bajo	Bajo	Bajo
A04	Ausencia / Interrupción total o parcial en el suministro telecomunicaciones	V138	Falla de elementos de soporte (UPS)	Bajo	Bajo	Bajo
		V141	Falla del hardware	Bajo	Alto	Bajo
		V144	Fallas de mantenimiento	Bajo	Alto	Bajo
		V157	Falta de mecanismos de control de fluctuaciones de energía	Medio	Bajo	Bajo
		V167	Fluctuaciones Eléctricas	Alto	Alto	Alto
		V197	Los equipos de control ambiental no reciben mantenimiento preventivo adecuado y suficiente (v.gr. componentes de TI, sistemas contra incendios, de suministro de energía, etc.).	Bajo	Bajo	Bajo
		V202	Mantenimiento insuficiente a la red de energía y tableros de control	Bajo	Bajo	Bajo

		V203	Mantenimiento insuficiente de controles medioambientales	Bajo	Bajo	Bajo
		V204	Mantenimiento insuficiente de las instalaciones	Bajo	Bajo	Bajo
		V205	Mantenimiento insuficiente de los recursos de TI y/o seguridad	Bajo	Alto	Bajo
		V255	Red energética inestable	Bajo	Medio	Bajo
		V265	Susceptibilidad de los equipos a variaciones de voltaje	Alto	Alto	Alto
		V271	Uniones deficientes de cables de energía	Bajo	Bajo	Bajo
		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Bajo	Bajo	Bajo
		V283	Conexión deficiente de los cables de red	Bajo	Bajo	Bajo
A05	Funcionamiento inadecuado de la infraestructura de TI (v.gr. hardware, software, etc.)	V19	Administración inadecuada de los componentes de la infraestructura de TI	Bajo	Medio	Bajo
		V141	Falla del hardware	Medio	Alto	Alto
		V144	Fallas de mantenimiento	Bajo	Bajo	Bajo
		V204	Mantenimiento insuficiente de las instalaciones	Bajo	Bajo	Bajo
		V205	Mantenimiento insuficiente de los recursos de TI y/o seguridad	Bajo	Alto	Bajo
		V261	Subvaloración de un incidente de seguridad de la información	Bajo	Alto	Bajo
		V263	Susceptibilidad de equipos a humedad, polvo	Alto	Alto	Alto

		V264	Susceptibilidad de los recursos de TI a variaciones de temperatura	Alto	Alto	Alto
		V99	Desbordamiento de memoria (búfer overflow)	Bajo	Alto	Bajo
		V265	Susceptibilidad de los equipos a variaciones de voltaje	Alto	Alto	Alto
		V117	Estrategias de recuperación desactualizadas	Bajo	Alto	Bajo
		V139	Falla de la copia de respaldo (backup)	Bajo	Bajo	Bajo
		V153	Falta de esquemas de crecimiento y escalabilidad de la plataforma	Medio	Alto	Alto
		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Bajo	Alto	Bajo
		V254	Punto única de falla	Bajo	Bajo	Bajo
		V188	Inexistencia de planes de recuperación de desastres y/o los procesos y procedimientos que los soportan	Alto	Alto	Alto
		V267	Ausencia de supervisión sobre los trabajos realizados por personal externo (v.gr. Limpieza, etc.)	Bajo	Alto	Bajo
		V284	Uso incorrecto de software y hardware	Bajo	Bajo	Bajo
		V285	Ausencia de un eficiente control de cambios	Medio	Alto	Alto
A06	Accidente importante que afecta la instalación	V66	Ausencia de señalización adecuada al interior de las instalaciones.	Medio	Alto	Alto

		V84	Construcción deficiente de edificios (v.gr. protección inadecuada de puertas, ventanas, etc.)	Medio	Medio	Medio
		V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)	Alto	Medio	Alto
		V159	Falta de supervisión de mecanismos de monitoreo	Bajo	Alto	Bajo
		V178	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información	Alto	Alto	Alto
		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Bajo	Medio	Bajo
		V268	Ubicación de las instalaciones en sector de alto riesgo (v.gr. inundación, terremoto, etc.)	Alto	Alto	Alto
		V269	Ubicación inadecuada de equipos	Alto	Alto	Alto
A07	Situaciones de Contaminación ambiental (v.gr. polvo, etc.)	V123	Error de controles medio ambientales	Bajo	Alto	Bajo
		V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)	Alto	Medio	Alto
		V159	Falta de supervisión de mecanismos de monitoreo	Bajo	Alto	Bajo

		V160	Falta de personal de limpieza	Bajo	Bajo	Bajo
		V161	Falta de políticas de escritorio y pantalla limpia	Medio	Alto	Alto
		V197	Los equipos de control ambiental no reciben mantenimiento preventivo adecuado y suficiente (v.gr. componentes de TI, sistemas contra incendios, de suministro de energía, etc.).	Medio	Alto	Alto
		V203	Mantenimiento insuficiente de controles medioambientales	Bajo	Bajo	Bajo
		V263	Susceptibilidad de equipos a humedad, polvo	Bajo	Alto	Bajo
		V290	Ausencia de protección física de la edificación, puertas y ventanas	Bajo	Bajo	Bajo
A08	Fenómeno Climáticos	V66	Ausencia de señalización adecuada al interior de las instalaciones.	Medio	Alto	Alto
		V159	Falta de supervisión de mecanismos de monitoreo	Bajo	Bajo	Bajo
		V178	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información	Medio	Alto	Alto
		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Bajo	Medio	Bajo
		V188	Inexistencia de planes de recuperación de desastres y/o los procesos y procedimientos que los soportan	Alto	Alto	Alto

		V268	Ubicación de las instalaciones en sector de alto riesgo (v.gr. inundación, terremoto, etc.)	Medio	Alto	Alto
		V269	Ubicación inadecuada de equipos	Medio	Alto	Alto
A09	Fenómeno sísmico (v.gr. terremoto)	V84	Construcción deficiente de edificios (v.gr. protección inadecuada de puertas, ventanas, etc.)	Bajo	Bajo	Bajo
		V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)	Bajo	Alto	Bajo
		V159	Falta de supervisión de mecanismos de monitoreo	Bajo	Alto	Bajo
		V178	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información	Bajo	Alto	Bajo
		V268	Ubicación de las instalaciones en sector de alto riesgo (v.gr. inundación, terremoto, etc.)	Bajo	Bajo	Bajo
		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Medio	Alto	Alto
		V188	Inexistencia de planes de recuperación de desastres y/o los procesos y procedimientos que los soportan	Medio	Alto	Alto
		V269	Ubicación inadecuada de equipos	Bajo	Alto	Bajo

A10	Fenómeno volcánicos	V268	Ubicación de las instalaciones en sector de alto riesgo (v.gr. inundación, terremoto, etc.)	Bajo	Bajo	Bajo
		V188	Inexistencia de planes de recuperación de desastres y/o los procesos y procedimientos que los soportan	Bajo	Medio	Bajo
		V269	Ubicación inadecuada de equipos	Bajo	Medio	Bajo
A11	Incendio	V84	Construcción deficiente de edificios (v.gr. protección inadecuada de puertas, ventanas, etc.)	Bajo	Bajo	Bajo
		V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)	Medio	Alto	Alto
		V159	Falta de supervisión de mecanismos de monitoreo	Bajo	Alto	Bajo
		V197	Los equipos de control ambiental no reciben mantenimiento preventivo adecuado y suficiente (v.gr. componentes de TI, sistemas contra incendios, de suministro de energía, etc.).	Bajo	Bajo	Bajo
		V206	Materiales inflamables empleados en la construcción y acabado de las instalaciones	Bajo	Medio	Bajo
		V207	Materiales inflamables en inmediaciones	Bajo	Bajo	Bajo
		V259	Sistemas insuficientes contra incendios	Medio	Alto	Alto
		V264	Susceptibilidad de los recursos de TI a variaciones de temperatura	Bajo	Medio	Bajo

		V265	Susceptibilidad de los equipos a variaciones de voltaje	Bajo	Alto	Bajo
		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Alto	Medio	Alto
		V188	Inexistencia de planes de recuperación de desastres y/o los procesos y procedimientos que los soportan	Alto	Alto	Alto
		V269	Ubicación inadecuada de equipos	Bajo	Bajo	Bajo
		V203	Mantenimiento insuficiente de controles medioambientales	Bajo	Bajo	Bajo
A12	Inundación (v.gr. sabotaje en tuberías, etc.)	V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)	Medio	Alto	Alto
		V159	Falta de supervisión de mecanismos de monitoreo	Bajo	Alto	Bajo
		V178	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información	Bajo	Medio	Bajo
		V268	Ubicación de las instalaciones en sector de alto riesgo (v.gr. inundación, terremoto, etc.)	Medio	Alto	Alto

		V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan	Medio	Alto	Alto
		V188	Inexistencia de planes de recuperación de desastres y/o los procesos y procedimientos que los soportan	Medio	Alto	Alto
		V269	Ubicación inadecuada de equipos	Bajo	Bajo	Bajo
		V292	Falta de mantenimiento de instalaciones hidráulicas y sanitarias	Bajo	Medio	Bajo
A13	Ataque terrorista	V270	Ubicación susceptible a disturbios, robos o vandalismo.	Alto	Alto	Alto
		V262	Suplantación de funcionarios de la compañía (v.gr. Mediante el uso de cuentas y contraseñas de acceso a los recursos informáticos, etc.)	Bajo	Medio	Bajo
		V260	Situación social inestable (v.gr. manifestaciones políticas, sindicales, ideológicas, etc.).	Bajo	Medio	Bajo
		V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)	Alto	Alto	Alto
		V159	Falta de supervisión de mecanismos de monitoreo	Medio	Alto	Alto
		V14	Acceso no supervisado a las oficinas/edificios/instalaciones de la compañía	Bajo	Medio	Bajo

		V188	Inexistencia de planes de recuperación de desastres y/o los procesos y procedimientos que los soportan	Alto	Alto	Alto
		V121	Personal de seguridad física no capacitado	Bajo	Bajo	Bajo
A14	Ladrón	V01	Acceso de personal no autorizado a la información almacenada en copias de respaldo	Bajo	Alto	Bajo
		V05	Acceso inadecuado de medios de almacenamiento removibles	Bajo	Medio	Bajo
		V17	Activos de TI desprotegidos	Alto	Alto	Alto
		V24	Copias de respaldo desprotegidas	Bajo	Alto	Bajo
		V62	Ausencia de políticas, procesos y procedimientos para la administración de copias de respaldo (v.gr. Generación, rotulación, rotación, retención, custodia, recuperación y destrucción)	Bajo	Alto	Bajo
		V110	Desecho o reusó de medios de almacenamiento sin hacer borrado seguro de la información existente	Bajo	Alto	Bajo
		V121	Personal de seguridad física no capacitado	Bajo	Bajo	Bajo
		V147	Falta de concientización en seguridad	Bajo	Alto	Bajo
		V152	Falta de entrenamiento en seguridad	Medio	Alto	Alto
		V166	Falta de políticas para la seguridad de los dispositivos de computación móvil	Medio	Alto	Alto

		V185	Inexistencia de bitácoras de acceso a las instalaciones y áreas restringidas de la compañía.	Bajo	Alto	Bajo
		V192	Información de valor para el negocio desprotegida en los puestos de trabajo (v.gr. documentos desprotegidos, sesiones de trabajo no atendidas, etc.).	Bajo	Alto	Bajo
		V219	Protección inadecuada de los activos de información físicos clasificados como confidenciales (v.gr. Organización, archivo, etc.)	Bajo	Alto	Bajo
		V223	No se cuenta con un inventario de actualizado de las llaves y criptogramas generados	Bajo	Alto	Bajo
		V226	Recurso humano insuficiente para el desarrollo de la función de seguridad de la información de la compañía	Medio	Alto	Alto
		V228	No se cuenta con personal responsable por la administración de la seguridad de los diferentes sistemas de información	Bajo	Alto	Bajo
		V229	No se establecen responsabilidades de seguridad de la información para los funcionarios de la compañía	Medio	Alto	Alto
		V230	No se hace una inducción sobre el modelo de seguridad de la información a nuevos funcionarios	Bajo	Alto	Bajo

		V231	No se informa al nivel jerárquico adecuado los incidentes de seguridad.	Bajo	Medio	Bajo
		V239	Pérdida de los equipos de trabajo y/o sus dispositivos (v.gr. equipos portátiles, USB, Discos Portátiles, etc.)	Bajo	Alto	Bajo
		V244	Procedimientos de control de acceso físico deficientes	Medio	Alto	Alto
		V251	Puertas traseras (Backdoors)	Bajo	Medio	Bajo
		V258	Sesiones de trabajo desatendidas (v. gr. Estaciones de trabajo y servidores)	Bajo	Alto	Bajo
		V270	Ubicación susceptible a disturbios, robos o vandalismo.	Alto	Medio	Alto
		V277	Uso no restringido de dispositivos de almacenamiento extraíbles	Bajo	Alto	Bajo
		V84	Construcción deficiente de edificios (v.gr. protección inadecuada de puertas, ventanas, etc.)	Bajo	Medio	Alto
		V14	Acceso no supervisado a las oficinas/edificios/instalaciones de la compañía.	Bajo	Alto	Bajo
		V22	Administración indebida de mecanismos de acceso físico a las instalaciones de la compañía (v.gr. copias de tarjetas de acceso, uso compartido de tarjetas de acceso, etc.)	Medio	Medio	Medio
		V48	Ausencia de mecanismos de control de acceso físico a áreas restringidas de la compañía(v.gr. centros de cómputos, cuartos de cableado, operaciones, etc.).	Alto	Alto	Alto

		V50	Ausencia de mecanismos de identificación de equipos y autenticación de conexiones	Bajo	Alto	Bajo
		V49	Ausencia de mecanismos de control de acceso físico a las instalaciones de la compañía (v.gr. edificio, instalaciones, oficinas, etc.)	Alto	Medio	Alto
		V56	Ausencia de personal de seguridad física (vigilancia)	Bajo	Bajo	Bajo
		V63	Falta de mecanismos de protección física de las instalaciones(v. gr. edificio, puertas y ventanas)	Alto	Medio	Alto
		V121	Personal de seguridad física no capacitado	Bajo	Bajo	Bajo
		V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)	Alto	Alto	Alto
		V159	Falta de supervisión de mecanismos de monitoreo	Bajo	Medio	Bajo
		V244	Procedimientos de control de acceso físico deficientes	Bajo	Alto	Bajo
		V185	Inexistencia de bitácoras de acceso a las instalaciones y áreas restringidas de la compañía.	Bajo	Alto	Bajo
		V178	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información	Medio	Alto	Alto

A15	Defectos en el código del software aplicativo	V71	Ausencia de lineamientos de seguridad que deben ser considerados durante el desarrollo de aplicaciones (v.gr. in house y adquiridas)	Medio	Alto	Alto
		V79	Código Malicioso	Bajo	Alto	Bajo
		V90	Debilidades conocidas en el software	Bajo	Bajo	Bajo
		V128	Errores en diseño y construcción de la aplicación	Bajo	Medio	Bajo
		V129	Errores en la configuración funcional de la aplicación	Bajo	Bajo	Bajo
		V130	Errores en la configuración funcional de la base de datos	Bajo	Alto	Bajo
		V131	Especificaciones erradas o incompletas para analistas de desarrollo	Bajo	Medio	Bajo
		V142	Falla del software	Bajo	Alto	Bajo
		V99	Desbordamiento de memoria (búfer overflow)	Bajo	Bajo	Bajo
		V34	Atención inoportuna de un incidente de seguridad de la información	Bajo	Medio	Bajo
		V273	Uso de código no autorizado o no probado	Medio	Alto	Alto
		V285	Ausencia de un eficiente control de cambios	Medio	Bajo	Bajo
A16	Errores de procesamiento	V79	Código Malicioso	Alto	Medio	Alto
		V128	Errores en diseño y construcción de la aplicación	Bajo	Bajo	Bajo
		V129	Errores en la configuración funcional de la aplicación	Medio	Bajo	Bajo
		V130	Errores en la configuración funcional de la base de datos	Bajo	Bajo	Bajo
		V99	Desbordamiento de memoria (búfer overflow)	Bajo	Alto	Bajo

		V142	Falla del software	Bajo	Alto	Bajo
		V246	Procesamiento errado de información	Bajo	Alto	Bajo
		V41	Ausencia de documentación del proceso	Medio	Bajo	Bajo
		V284	Uso incorrecto de software y hardware	Bajo	Bajo	Bajo
A17	Instalación o implantación de Malware (v.gr. Virus, troyanos, HOAX / SPAM, dataminer, etc.).	V18	Administración inadecuada de la red	Bajo	Medio	Bajo
		V39	Ausencia de control en la descarga y uso de software	Bajo	Alto	Bajo
		V79	Código Malicioso	Bajo	Alto	Bajo
		V90	Debilidades conocidas en el software	Bajo	Medio	Bajo
		V142	Falla del software	Medio	Bajo	Bajo
		V250	Protocolos de red sin cifrar	Bajo	Bajo	Bajo
		V98	Software antivirus desactualizado	Medio	Bajo	Bajo
		V212	No aplicación de parches de seguridad liberados por los proveedores de soluciones de TI	Bajo	Medio	Bajo
		V51	Ausencia de mecanismos de identificación de incidentes o problemas de TI	Medio	Medio	Medio
		V34	Atención inoportuna de un incidente de seguridad de la información	Bajo	Medio	Bajo
		V273	Uso de código no autorizado o no probado	Bajo	Bajo	Bajo
A18	Degradación de los medios en lo que se almacena información	V160	Falta de personal de limpieza	Bajo	Bajo	Bajo
		V263	Susceptibilidad de equipos a humedad, polvo	Bajo	Medio	Bajo
		V167	Fluctuaciones Eléctricas	Alto	Alto	Alto
		V86	Copias de respaldo con información insuficiente / no integra	Bajo	Bajo	Bajo

		V87	Copias de respaldo en mal estado	Bajo	Bajo	Bajo
		V112	Deterioro de los medios magnéticos	Bajo	Medio	Bajo
		V256	Ausencia de estándares / patrones de seguridad para la información	Bajo	Medio	Bajo
		V291	Falta de custodia de copias de respaldo	Bajo	Alto	Bajo

Tabla 1: Valoración de riesgos.

PROBABILIDAD		BAJO	MEDIO	ALTO
	ALTO		V158,V159,V187,V270,,V43,V63,V79	V17,V48,V63,V157,V158,V167,V178,V187,V188,V255,V263,V264,V265,V268,V269,V270
	MEDIO	V41,V98,V129,V142,V157,V285	V84,V22,V51	V66,V71,V141,V152,V153,V158,V159,V161,V166,V187,V188,V197,V226,V229,V244,V259,V268,V273,V285
	BAJO	V56,V84,V86,V87,V90,V99,V121,V129,V130,V138,V139,V144,V159,V160,V185,V187,V197,V202,V203,V204,V207,V250,V254,V268,V271,V273,V282,V283,V284,V290	V01,V05,V14,V18,V19,V34,V84,V90,V112,V128,V131,V140,V159,V178,V187,V188,V202,V203,V204,V206,V212,V231,V251,V255,V,256,V260,V262,V263,V264,V269,V292	V01,V14,V22,V24,V49,V62,V99,V110,V117,V123,V141,V144,V147,V158,V159,V185,V192,V205,V219,V223,V228,V230,V239,V258,V261,V265,V277
			IMPACTO	

Tabla 2: Matriz de Riesgo.

Después de realizar las inspecciones respectivas para identificar de manera adecuada cada una de las amenazas a la cual la compañía se encuentra expuesta de acuerdo a su actividad se realizó un análisis para detectar las vulnerabilidades que pueden causar un gran impacto en el departamento de sistemas la cual puede poner en riesgo la operación normal de la compañía.

Las amenazas que se consideraron como prioritarias son las siguientes:

Acceso físicos no autorizados, interrupción parcial o total del fluido eléctrico, fenómenos climáticos, ladrones o robos por la ubicación de la empresa la cual se encuentra en barrios de alto riesgo en cuanto a la seguridad ya que la compañía se encuentra rodeada por los barrios el bosque, san Martin, San Luis, El Universal como se aprecia en la siguiente imagen.

Otra amenaza como lo son las inundaciones se ha presentado en más de una oportunidad en la compañía porque en la temporadas invernales un arroyo que rodea las instalaciones se desborda con se observa en una de las inundaciones del año 2006 la cual se repitió el año 2009 Y 2012.

La compañía no cuenta con mecanismos de monitoreo (Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, etc.) lo cual es una parte vulnerable de la compañía que en cualquier momento una vulnerabilidad puede materializarse.

8.3. ANÁLISIS DE IMPACTO

En este punto en particular se pretenderá identificar cada uno de los recursos críticos con que cuenta la compañía en la cual ella soporta toda su operación diaria.

Después de haber identificado las aéreas esenciales se enfocara en el trabajo de recuperación lo cual nos dará como resultado el tiempo que podrá demorar la contingencia sin afectar significativamente la operación de la compañía.

Para obtener información vital para el proyecto se realizaron entrevistas al personal del Departamento de Sistemas de compañía lo cual dieron a conocer cada una de las aplicaciones, recursos y actividades que realizan cada persona para mantener toda la plataforma en operación sin ningún contratiempo. (Véase el Anexo A)

En el Dpto. de Sistemas se evidencio documentación necesaria para aquellos casos de criticidad muy alta. Lo cual se observó que se maneja cada contingencia por separado para aplicaciones y recursos. Pero no cuentan con un plan de recuperación bien organizado y estructurado que le permita actuar de manera efectiva en caso de activar la contingencia.

El Dpto. de Sistemas cuenta con un servidor espejo que le permite restablecer de manera provisional los servicios para su normal funcionamiento se tienen manuales algunos de ellos sin actualizar.

El anterior análisis nos ayudara a plantear la siguiente matriz de recursos tecnológicos principales de la compañía.

Punto Objetivo de Recuperación (RPO, Recovery Point Objective) Básicamente, RPO significa lo que la organización está dispuesta a perder en cantidad de datos. Para reducir un RPO es necesario aumentar el sincronismo de réplica de datos.

Tiempo Objetivo de Recuperación (RTO, Recovery Time Objective) es el tiempo que pasará una infraestructura antes de estar disponible. Para reducir el RTO, se requiere que la Infraestructura (Tecnológica, Logística, Física) esté disponible en el menor tiempo posible pasado el evento de interrupción.

Recursos de TI	Descripción	Requerimientos	Responsable	RTO	RPO
Server Windows Correo Electrónico	Equipo informático que administra el servicio de correo electrónico de la compañía	PC, Electricidad, Conexión	Jefe de Plataforma tecnológica	6	20
Server Windows Terminal Server	Equipo informático que administra el servicio de terminal Server	PC, Electricidad, Conexión	Jefe de Plataforma tecnológica	2	4

Server Windows Dominio	Equipo informático que administra el servicio de Dominio	PC, Electricidad, Conexión	Jefe de Plataforma tecnológica	1	0
Server Windows Ejecutables ERP	Equipo informático que administra el servicio de ERP	PC, Electricidad, Conexión	Jefe de Plataforma tecnológica	1	0
Telecomunicaciones	Es la plataforma de comunicaciones con la cual todos los sistemas se interrelacionan automatizadamente	Dispositivos Activos, redes, servicios de proveedores, instalaciones físicas, electricidad	Jefe de Infraestructura	3	1
Bases de datos	Fuente de datos para todas las aplicaciones operacionales	Servidores, conexiones, clientes, plataforma, electricidad	DBA	4	0
Software - Aplicaciones	Programas de ofimática, y actividades de soporte	Computadores, electricidad, plataforma, conexiones	Jefe de soporte	2	0

RTO	19	HORAS
RPO	20	

Tabla 3: Análisis de recursos de TI críticos (RPO y RTO)

Con el anterior análisis se puede observar que el que el tiempo de recuperación es de 19 horas, de igual forma hay que tener presente que cada actividad de recuperación de los recursos tecnológicos no se hacen de manera simultánea teniendo en cuenta las condiciones de la compañía.

Los resultados del análisis se mostraran gráficamente a continuación:

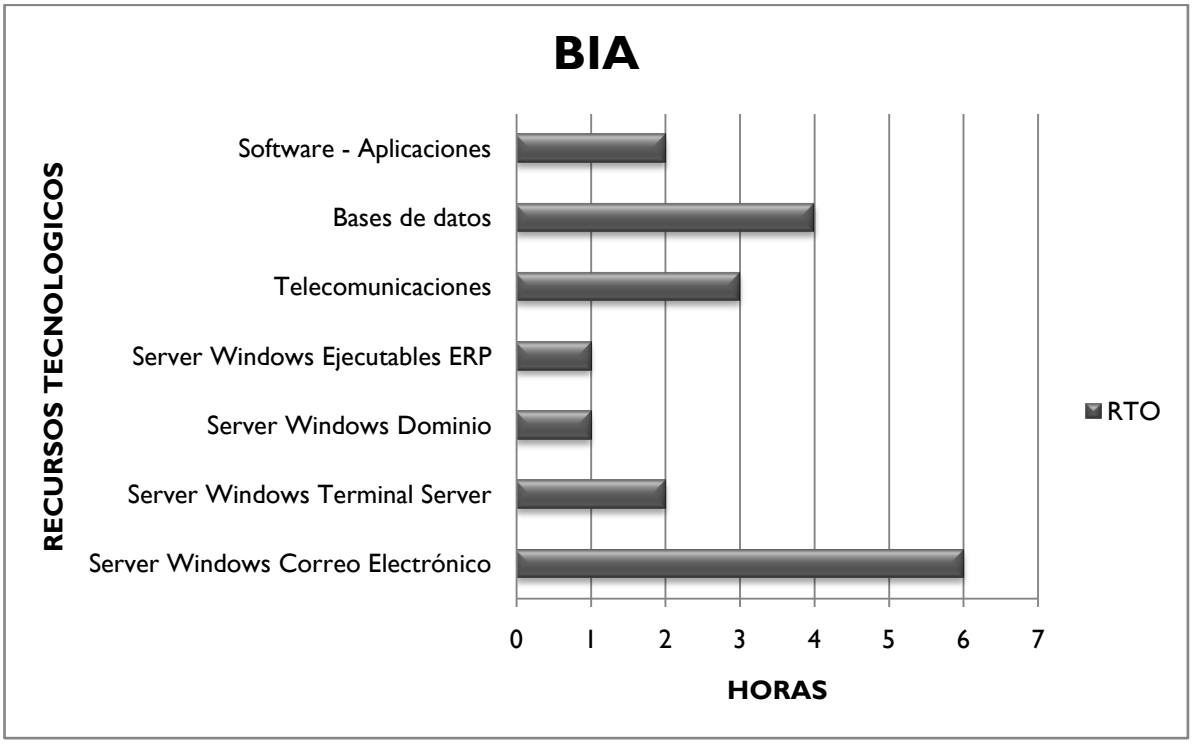

Figura 9: RTO con recursos tecnológicos

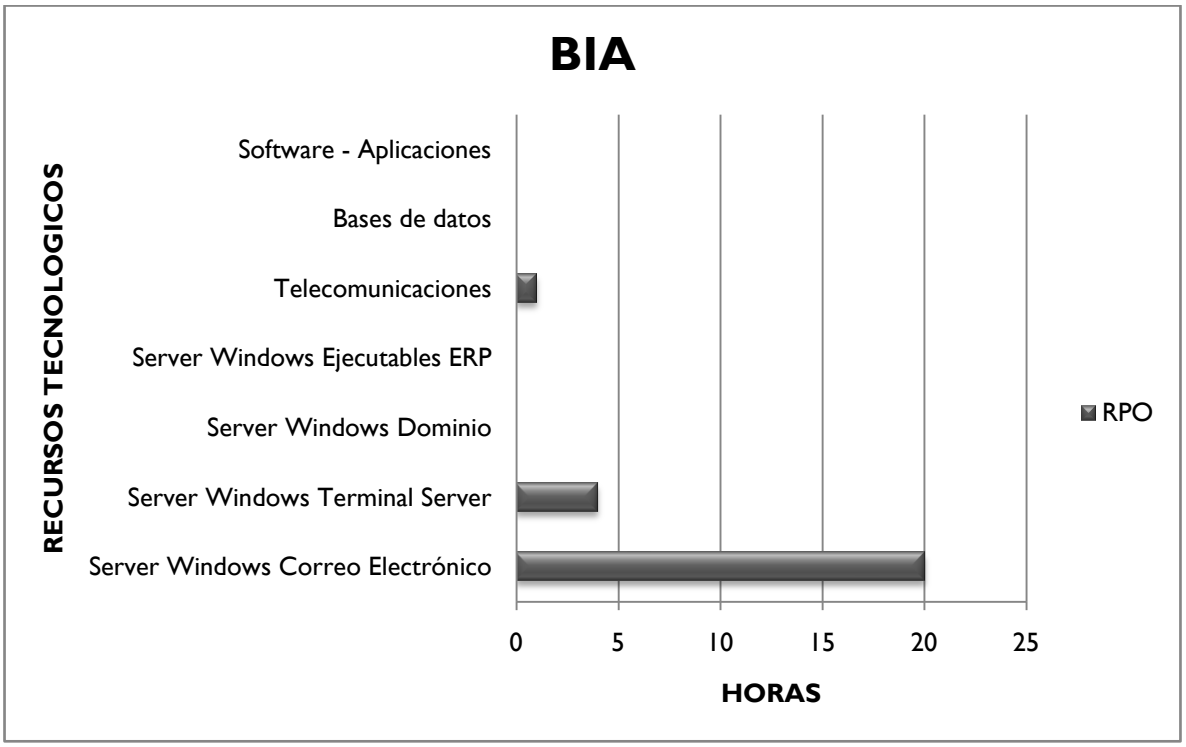

Figura 10: RPO con recursos tecnológicos

En la anterior figura se puede observar que el punto objetivo de recuperación que la compañía como máximo acepta es de 20 hrs ya que los procesos de restauración de los respaldos se llevan a cabo una vez al día cada 5 días de la semana.

En las vulnerabilidades detectadas en el análisis de riesgo se observó que muchas de ellas se pueden mitigar o disminuir su impacto de manera considerable como son las fuentes de energía apropiadas que en casos de emergencia se cuenta con el fluido para continuar las operaciones de manera normal.

De igual forma sistemas contraincendios detectores de humo, censores de humedad, sistemas de refrigeración apropiados para los equipos de cómputo y la seguridad perimetral entre otras.

8.4. ELECCIÓN DE ESTRATEGIAS PARA LA RECUPERACIÓN

Este punto es una de los más importantes ya que por medio de este la compañía volverá a su normal funcionamiento todos los recursos con que cuenta después de un posible desastre.

Hay muchos factores definitivos pero el más significativo para las compañías es el costo y otros de igual forma importantes como son los controles que se tengan ya implementados, los datos que se protegerán y requerimientos adicionales que puedan surgir.

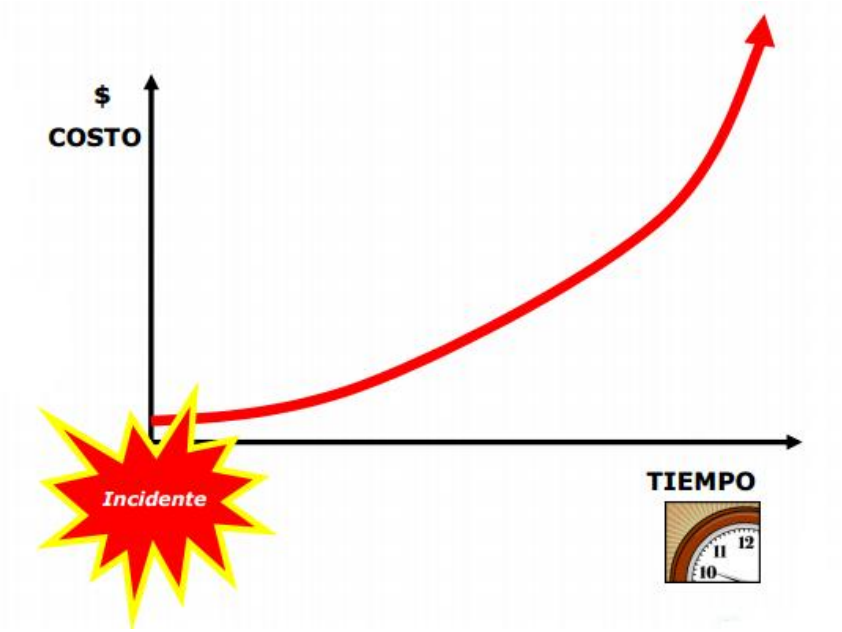

Figura 11: Curva de impacto al negocio.

“Se deberá trabajar con la alta gerencia ya que ellos son una parte fundamental en el proceso, y se determinara el punto óptimo para recuperar del sistema de información y equilibrar el costo del sistema inoperativo con el costo de los recursos necesarios para restaurar el sistema y su apoyo general que se fundamenta en los procesos del negocio. Esto se presenta mediante la siguiente figura"[8].

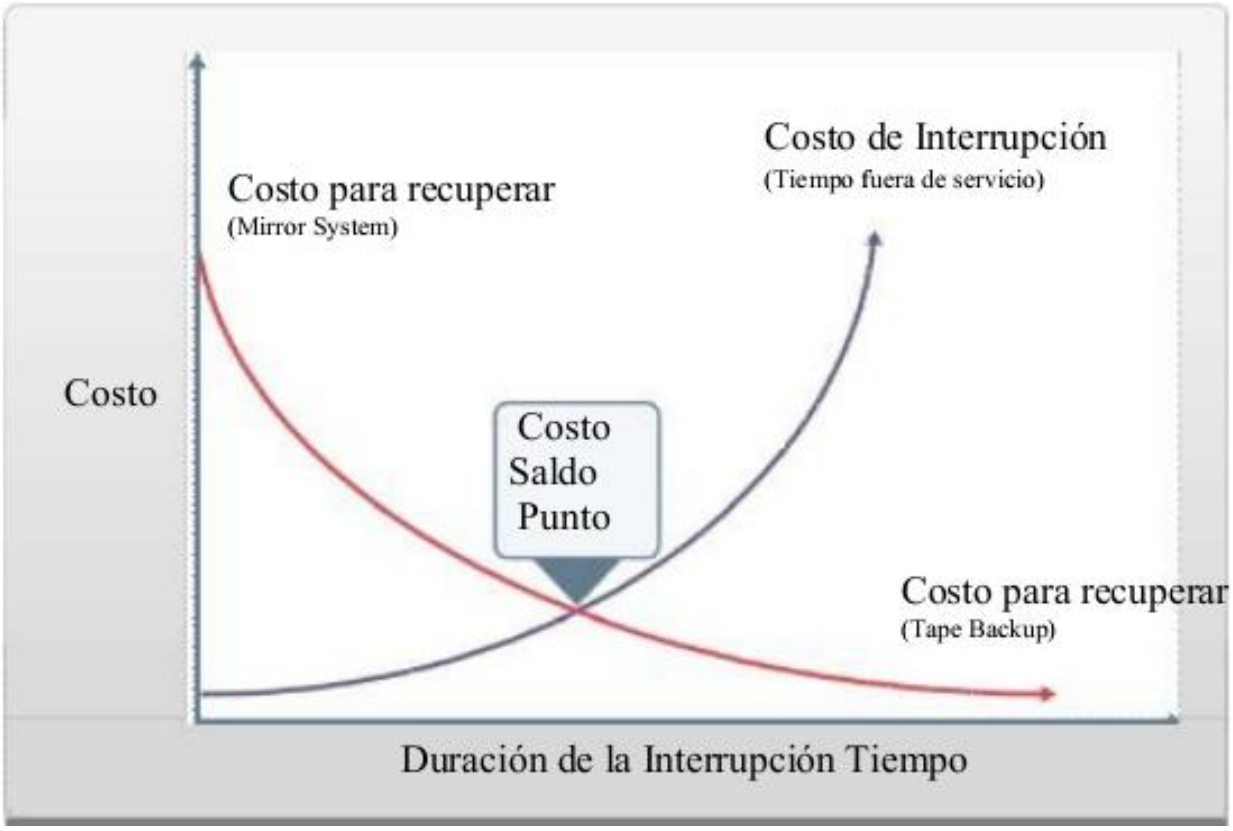

Figura 12: Punto de equilibrio del costo

[8]NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems, Charter 3, Pág. 32

Visto lo anteriormente existen varias alternativas como lo menciona Juan Gaspar Martínez “que dependiendo de los umbrales de recuperación que se hayan puesto como objetivos, habremos de definir el tipo de centro en función del tiempo de disponibilidad pues, si bien cada día es más frecuente la presencia de aplicaciones de una gran criticidad ”[9]

Existen varios tipos de centros los cuales definiremos a continuación los cuales dependiendo de la necesidad de la compañía podría adoptar cualquiera de ellos que se amolde a las necesidades de la misma.

Centro en frio: Es una sala preparada con las condiciones ambientales necesarias para albergar equipos informáticos con cierta estructura de comunicaciones.

Esto está recomendado para empresas que por su estructura pueden estar un cierto tiempo sin servicios informáticos funcionando con procedimientos alternativos.

[9]Juan Gaspar Martínez, Planes de Contingencia la continuidad del negocio en las organizaciones, Unidad 4. Pág. 70.

Centro en caliente: es una instalación con un C.P.D. totalmente configurado a las especificaciones del cliente y disponible en pocas horas. Esta recomendado para organizaciones en las cuales su tiempo de ruptura no supera las 24/48 horas.

Centro espejo: En el caso de que las necesidades de respuesta sean inmediatas, la solución está en el llamado centro espejo, que consiste en dos instalaciones idénticas y actualizadas permanentemente con objeto de que una de ellas se haga cargo automáticamente del trabajo si la otra sufre interrupción.

Centros móvil: Existe otro tipo de servicio que consiste en trasladar las facilidades informáticas de respaldo al lugar determinado previamente en el Plan de Contingencia. Consiste en una sala acondicionada, equipada en un contenedor y configurable en pocas horas. Dependiendo del centro de suministro, los umbrales de recuperación cubiertos pueden ir desde 6-8 horas en adelante.

De igual forma debe existir una política de planificación de contingencia exitosa esto quiere decir que se debe construir un sistema flexible ya nivel de componentes que eviten fracasos o interrupciones del sistema.

Lo cual hay que determinar los métodos apropiados que deben estar basados en el riesgo. En función de los resultados del proceso de gestión del riesgo, estos métodos pueden o no ser aplicables a un sistema.

El sistema y sus datos pueden dañarse como resultado de un fallo de alimentación o sobre carga de energía. Hardware críticos, como servidores, se puede configurar con fuentes de alimentación duales para prevenir la corrupción.

Sin embargo, un sistema de UPS puede proteger el sistema si se pierde la alimentación. Una UPS normalmente proporciona 30 a 60 minutos de copia de seguridad temporal poder para permitir un apagado ordenado

8.5. DOCUMENTACIÓN DE PROCESOS

En esta etapa del plan de recuperación de desastres todos los documentos de información del personal que se encargara de la emergencia deberán estar constantemente actualizados en el caso de que se amerite activar la contingencia.

Para ello recomendamos la siguiente documentación:

Figura 13: Ficha de contacto

Esta ficha de igual forma se utilizara para los contactos secundarios y de apoyo.

PROCEDIMIENTOS QUE SE DEBERAN TENER ENCUENTA EN UNA CONTINGENCIA

Cada uno de estos procedimientos estará documentado y actualizado:

- Descripción de los procesos
- Requerimientos mínimos
- Determinar cada uno de los registros vitales y la ubicación de cada uno de ellos.
- Formatos críticos
- Descripción de los equipos y del software
- Software que se usara en la recuperación
- Software usado en producción
- Estructura y diseño de las redes
- Necesidades de las redes durante el proceso de recuperación
- Necesidades de comunicación tanto en producción como en el sitio de recuperación.
- Inactivar procesos y funciones
- Uso de instalaciones alternativas para el procesamiento de datos.
- Transferir funciones a diferentes organizaciones (Sistemas).

PLAN DE LOS RECURSOS QUE SE UTILIZARAN PARA EL FUNCIONAMIENTO DEL PLAN DE CONTINGENCIA.

A continuación estableceremos los criterios mínimos para retornar a las operaciones normales las cuales detallaremos a continuación de la siguiente manera:

- ❖ Proceso para la adquisición o compra de equipos o partes.
- ❖ Proceso para reiniciar o restaurar los sistemas según sea la necesidad.
- ❖ Procesos de verificación de los sistemas y de las funciones y análisis de resultados.
- ❖ Procesos de notificación al personal para el retorno al modo normal de las operaciones.
- ❖ Procesos de recuperación y de corrección de datos perdidos o dañados o en el caso de que se presenten datos corruptos.

8.6. PLAN DE PRUEBA

En este proceso se pretende plantear un prototipo de plan de pruebas con las actividades de recuperación con que se cuentan para dar una garantía más confiable para operar sin ningún tipo de fallas. Para ello diseñamos el siguiente plan de pruebas.

PAVIMENTO UNIVERSAL S.A. **PROTOTIPO PLAN DE PRUEBAS**				
No	**Nombre del recurso**	**Responsable de la Prueba**	**Duración**	**Procedimiento**
1	UPS	Jefe de Tecnología Y soporte	2 Horas y 30 Min.	**1.** Realice una prueba de capacidad cuando la batería sea nueva como parte de la prueba de aceptación. **2.** Realice una prueba de impedancia al mismo tiempo para establecer los valores de referencia de la batería. **3.** Repita los pasos anteriores en 1 años por motivos de garantía. **4.** Realice una prueba de impedancia cada año en celdas inundadas y cada cuatro meses en celdas VRLA. **5.** Realice una prueba de capacidad por lo menos a cada 25% de la vida de servicio esperada. **6.** Realice una prueba de capacidad anualmente cuando la batería haya llegado al 85% de su vida de servicio esperada o si la capacidad ha bajado más del 10% desde la prueba anterior o está por debajo del 90% de lo establecido por el fabricante. **7.** Realice una prueba de capacidad si los valores de impedancia han cambiado significativamente. **8.** Siga las prácticas establecidas (preferiblemente por los estándares IEEE450 Y IEEE1188) para mediciones de temperatura, voltaje, gravedad, etc. y realizar un informe. Esto ayudará a establecer tendencias y rastrear fallos.

2	Sistemas de seguridad	Jefe de Tecnología Y soporte	1 Hora y 30 Min.	**1.** Verificar el sistema de acceso al centro de computo **2.** Inspeccionar que los sistemas de alarmas se encuentren funcionando de manera adecuada. **3.** Revisar los planes de seguridad de la compañía.
3	Base de Datos	DBA	5 horas	**1.** Realizar copias de seguridad de cada una de las bases de datos. **2.** Restablecer respaldos anteriores para verificar el estado de las copias. **3.** verificar si se tiene una manual de operaciones de las bases de datos. **4.** Inspeccionar los equipos de almacenamiento si funcionan adecuadamente.
4	Server Windows ERP	Jefe de Tecnología Y soporte	3 horas	**1.** Realizar previamente informes antes de hacer cualquier actividad. **2.** Verificar que se cuentan en el centro de respaldo con los backup actualizados del servidor ERP. **3.** Desactivar temporalmente todos los servicios y posteriormente restaurar las copias más recientes en el centro de respaldo. **4.** Verificar que cada uno de los servicios desactivados estén funcionando de manera normal y generar informes. **5.** Comparar los informes antes y después del procedimiento.
5	Servidor de correos electrónicos	Jefe de Tecnología Y soporte	3 horas	**1.** Desactivar el servicio de manera temporal y restaurar las copias de respaldo más reciente de la BD. **2.** Verificar las configuraciones para los grupos de usuarios que se encuentren activos. **3.** Generar informes para cotejar información. **4.** Determinar los tiempos de respuesta que se obtengan para esta prueba.

6	Server Windows Terminal Server	Jefe de Tecnología Y soporte	3 horas	**1.** Realizar previamente informes antes de hacer cualquier actividad. **2.** Verificar que se cuentan en el centro de respaldo con los backup actualizados del servidor. **3.** Apagar temporalmente todos los servicios y posteriormente restaurar las copias más recientes en el centro de respaldo. **4.** Verificar que cada uno de los servicios apagados estén funcionando de manera normal y generar informes. **5.** Comparar los informes antes y después del procedimiento.
7	Server Windows Dominio	Jefe de Tecnología Y soporte		**1.** Generar informes previos antes de realizar cualquier tipo de cambio. **2.** Desactivar el servicio y realizar una reconfiguración del servidor alterno. **3.** Realizar un re-direccionamiento de las políticas de autenticación de algunos usuarios escogidos al azar para realizar pruebas con ellos. **4.** Realizar informes de los datos obtenidos de las pruebas para tener un historial de referencia futura.

Tabla 4: Prototipo del plan de pruebas

8.7. SOCIALIZACIÓN

Para la parte de sensibilización o socialización de la propuesta se planteó enviar copias a las partes interesadas o responsables con la intensión de revisar y aprobar y de igual forma se utilizaran medios físicos y/o electrónicos para su posterior divulgación y cumplimiento en la compañía.

El plan de recuperación de desastres estará en una etapa donde cada una de las partes expondrá sus sugerencias las cuales el departamento de sistemas las analizara detalladamente para que luego se envíen las copias a los responsables de cada departamento.

DEPARTAMENTO	**No. COPIAS**
SISTEMAS	3
GERENCIA	2
OTRAS AREAS	4

Tabla 5: Socialización

8.8. MANTENIMIENTO

En cada política empresarial se debe definir los procesos de mantenimiento para las actualizaciones del plan de recuperación de desastres cuando exista un cambio o cuando se requiera una actualización más compleja esto con el fin de alinearlo con las necesidades de la compañía.

Por tal motivo en cada adquisición se involucrara la estrategia de contingencia, por ende cuando exista algún cambio se deberá planificar de una manera adecuada según las necesidades de la compañía.

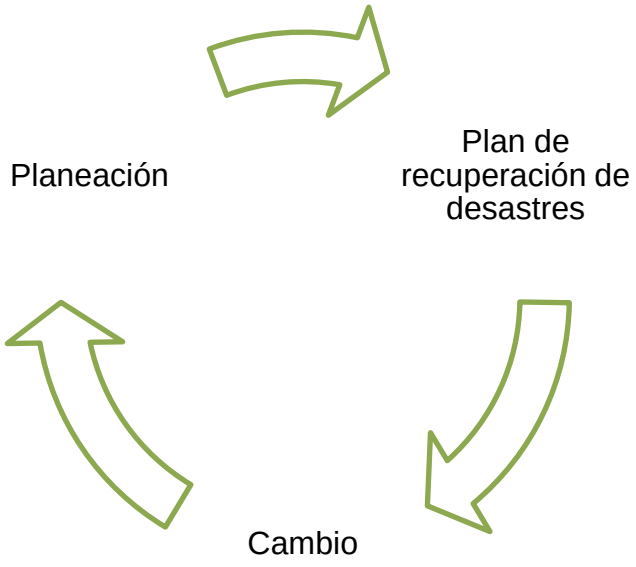

Figura 14: Interrelación de los componentes del mantenimiento

9. CONCLUSION

Concluimos que existen en la actualidad muchas empresas que tienen diversos tipos de procesos que pueden o no estar automatizados. Lo que conlleva a que las empresas adopten un estándar o norma que les sirva de apoyo para crear su propio plan de recuperación. Sabemos muy bien de que existen diferentes estándares como NIST SP 800-34, DRII, ISO 24762 y guías de buenas prácticas como Cobit entre otras.

Con la combinación o fusión de estos estándares de acuerdo con la estructura y necesidad de la empresa se busca tener un plan de recuperación de desastres completo y ordenado.

En la entrevista que se sostuvo con el personal de TI se logró identificar cada uno de los recursos críticos y plataformas en la cual la empresa soporta sus operaciones diarias y con sus respectivas vulnerabilidades.

Con toda la información obtenida se realiza un plan de pruebas teniendo en cuenta la infraestructura tecnológica de la compañía, el cual llene las expectativas del personal de TI de PAVIMENTO UNIVERSAL S.A.

Hecho todo lo anterior obtendremos un plan de recuperación de desastres bien estructurado para la compañía.

10. RECOMENDACIONES

Como recomendación se deja sentado los siguientes puntos:

- El departamento de sistemas debe actualizar la documentación de los procesos y aplicativos que se estén utilizando actualmente en la compañía y de igual manera cada uno de los recursos de TI..

- Se les recomienda mantener permanentemente actualizado el plan de recuperación.

- En cuanto a la adquisición o compra de equipos se deberá incluir en el plan de recuperación para evitar impactos que lleguen a causar el normal funcionamiento de la infraestructura tecnológica del negocio.

- Para probar la eficiencia del plan de recuperación de desastres llevar a cabo un cronograma de pruebas el cual nos permita identificar fallas para así poder las corregir oportunamente sin que afecte la estabilidad de los procesos.

- Continuar con el proyecto hasta llegar a concretar un plan de continuidad del negocio bien estructurado que a la compañía le sirva para fortalecer sus estrategias en cada nivel.

PRESUPUESTO

PAPELERIA	Und	Costo	C. Total
Hojas Cartas	2.00	$ 8,600.00	$ 17,200
Hojas Oficio	1.00	$ 9,600.00	$ 9,600
Bolígrafos	2.00	$ 600.00	$ 1,200
Lápiz negro	3.00	$ 500.00	$ 1,500
Otros		$ 6,000.00	$ 6,000
Total			**$ 35,500.00**

TRANSPORTE	Und	Costo	C. Total
Gastos de autobús	20.00	$ 1,500.00	$ 30,000.00
Gastos de taxi	6.00	$ 8,000.00	$ 48,000.00
Gastos de autobús intermunicipal	30.00	$ 8,000.00	$ 240,000.00
Total			**$ 318,000.00**

ALIMENTACIÓN	Und	Costo	C. Total
Comestibles	13.00	$ 2,800.00	$ 36,400.00
Restaurantes	20.00	$ 6,000.00	$ 120,000.00
Otros		$ 20,000.00	$ 20,000.00
Total			**176,400.00**

TOTAL PROYECTO			**$ 529,900.00**

Tabla 6: Presupuesto

BIBLIOGRAFIA

NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. U.S. Department of Commerce, Mayo de 2010.

IT Governance Institute, COBIT 4.1

http://www.sisteseg.com/sindustrial.html

Ing Ferrer V. Rodrigo. Plan de continuidad para el negocio. Sisteseg

[Online],http://www.sisteseg.com/files/Microsoft_PowerPoint_-_PLANES_DE_CONTINUIDAD_NEGOCIO_V_3.0.pdf. Marzo 2009.

Britannic Standard 25999:2008

NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs.2007 Edition.

International standardorganization, ISO 27000:2002

Juan Gaspar Martínez, Planes de Contingencia la continuidad del negocio en las organizaciones, Editorial Díaz de Santos 2004.

http://www.iteam.com.co/comercial/ITEAM_SOLUCIONES-BCM_PRE_20100803.pdf

DissasterRecoveryJournal. Glosario de continuidad de negocio, Desarrollada en conjunto con DRII,

Megger, Guía para Prueba de baterías,http://www.artec-ingenieria.com/pdf/guias_megger/GuiaTecnica_pruebadebaterias.pdf

http://itil.osiatis.es/Curso_ITIL

International standard organization, ISO/IEC 27001:2005

Ing. Ferrer V. Rodrigo y Ing. Donoso Yezid,Planes de recuperación ante desastres(DRP)[Online]www.acis.org.co/fileadmin/Conferencias/DRP_BCP.pdf

Ing. MBA Guillermo Martín Palacios Rubio,Consideraciones clave para el cálculo de los RTO [Online]http://ebookbrowse.com/consideraciones-para-calcular-los-rto-pdf-d174903589 Octubre de 2011

International standard ISO/IEC 24762, Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services.FirstEdition 2008

ANEXOS

ANEXO A

ENCUESTA PARA EL ANALISIS DE IMPACTO EN PLAN DE RECUPERACION DE DESASTRES

Referente a Jefe de sistemas, Jefe de soporte y personal a fin.

Objetivos: 1) Identificar cada proceso crítico de la compañía para determinar los tiempos de recuperación y el punto objetivo de recuperación

2) Priorizar los procesos críticos de la compañía de acuerdo a su criticidad.

3) Identificar el posible impacto de una interrupción.

Nombre del encuestado:	
Cargo en la compañía:	

PREGUNTAS

1. Que procesos o recursos de TI lidera usted en la compañía
2. Tienen algún formato donde se puede encontrar los datos de los contactos del personal responsable de cada uno de los procesos de TI
3. Cueles son los procesos críticos de la compañía que lidera usted de mayor a menor criticidad.
4. De los procesos que usted lidera cuales los puede hacer de forma manual y por cuento tiempo.
5. Describa los recursos tecnológicos de cada uno de los procesos y el lugar o sitio donde se ejecutan.

6. Cueles son las funciones que cumplen de acuerdo al cargo.

7. De los procesos que usted lidera cuales están debidamente documentados y estandarizados.

8. De acuerdo al volumen de trabajo que se presenta en cada uno de los procesos que clasificación le daría a cada uno de ellos en sus momentos críticos.

9. Dentro de los procesos de la compañía cuales están con terceros y de qué forma lo están.

10. Que otros recursos de TI necesitaría para restablecer su proceso.

11. Cuáles de los procesos que usted tiene a cargo interactúan con otros y de qué forma lo hacen.

12. Que necesitaría para restablecer el proceso que usted lidera en la compañía.

13. Si se interrumpe un proceso crítico para restablecerlo que equipos necesitaría en cuanto a cantidad y especificaciones para restablecer el servicio.

14. En cada proceso cual es el tiempo objetivo de recuperación para cada uno de los procesos críticos de la compañía.

15. Describa cada uno de los registros que considera usted que son vitales para la continuidad del proceso y especifique el lugar donde se encuentran.

16. En caso de que haya algún incidente en la compañía cuales son las personas o proveedores que deben ser contactados.

17. Para restablecer cualquier proceso de la compañía que datos necesitaría. Y en qué lugar se encuentran.

ANEXO B

LISTADO DE VULNERABILIDADES

Código	Vulnerabilidades
V01	Acceso de personal no autorizado a la información almacenada en copias de respaldo
V02	Acceso inadecuado a procesos almacenados en los recursos de TI (v.gr. storeprocedures)
V03	Acceso inadecuado de aplicaciones y herramientas a las bases de datos
V04	Acceso inadecuado de leguajes de programación instalados por defecto en los recursos de TI
V05	Acceso inadecuado de medios de almacenamiento removibles
V06	Acceso irrestricto a los utilitarios de los recursos de TI (v.gr. herramientas de gestión, consulta, etc.)
V07	Acceso no autorizado a los archivos de configuración de seguridad, técnica y funcional de la aplicación
V08	Acceso no autorizado a los archivos de configuración de seguridad, técnica y funcional de la Base de Datos
V09	Acceso no autorizado a los archivos de configuración de seguridad, técnica y funcional del sistema operativo
V10	Acceso no restringido a las herramientas de auditoría
V11	Acceso no restringido a los mensajes electrónicos (correo)
V12	Acceso no restringido a los recursos de información del Banco (v.gr. Aplicaciones, bases de datos, servidores, estaciones de trabajo, equipos de comunicaciones y de seguridad, etc.)
V13	Acceso no restringido a los registros de auditoría
V14	Acceso no supervisado a las oficinas/edificios/instalaciones de la compañía.
V15	Acceso no restringido de los desarrolladores a los ambientes de producción (v.gr. Aplicaciones, bases de datos, etc.).
V16	Acceso no restringido de los usuarios a los ambientes de desarrollo y pruebas (v.gr. Aplicaciones, bases de datos, etc.)
V17	Activos de TI desprotegidos
V18	Administración inadecuada de la red
V19	Administración inadecuada de los componentes de la infraestructura de TI
V20	Administración inadecuada de parches de seguridad y actualizaciones de software

V21	Administración indebida de cuentas y contraseñas de acceso (v.gr. cuentas de acceso sin contraseña, uso compartido de cuentas, cuentas de acceso genéricas, cuentas por defecto, contraseñas triviales, etc.)
V22	Administración indebida de mecanismos de acceso físico a las instalaciones
V23	Almacenamiento de contraseñas de acceso en texto claro (sin inscripción)
V24	Copias de respaldo desprotegidas
V25	Almacenamiento inadecuado de llaves y criptogramas (v. gr. Único responsable)
V26	Aplicación errada / inconsistente de los procedimientos de monitoreo y seguimiento al cumplimiento del Sistema de Gestión de Seguridad de la Información
V27	Selección e implementación de componentes de seguridad que no cumplan con los requerimientos exigidos por los entes de control (v.gr. estándares de industria, etc.).
V28	Aplicación errada / inconsistente del proceso de administración de vulnerabilidades (v.gr. identificación, investigación, solución, etc.)
V29	Ausencia y/o aplicación no consistente del proceso de evaluación y clasificación de riesgos de seguridad de la información (v.gr. Frecuencia, alcance, etc.)
V30	La arquitectura de seguridad de TI no tiene alcance o es aplicada a los activos de información que requieren protección
V31	Asignación de múltiples cuentas y perfiles de acceso sobre una aplicación para un mismo usuario
V32	Asignación errada de privilegios de acceso a los usuarios, terceros y clientes (v.gr. excesivos, no autorizados, etc.)
V33	Asignación indebida de privilegios de administración sobre los recursos de TI (v.gr. administración de cuentas y contraseñas de acceso, conexión remota, etc.)
V34	Atención inoportuna de un incidente de seguridad de la información
V35	Atención no oportuna de las novedades de usuarios relacionadas con bloqueos, inactivación, creación y eliminación de privilegios de acceso de usuarios
V36	Ausencia / definición errada de un esquema de gobierno de seguridad de la información (v.gr. roles, responsabilidades, esquema de reporte, etc.)
V37	Ausencia / insuficiencias de las herramientas de identificación y análisis de vulnerabilidades sobre los recursos de información
V38	Ausencia de actividades de monitoreo y seguimiento al cumplimiento del Sistema de Gestión de Seguridad de la Información
V39	Ausencia de control en la descarga y uso de software

V40	Ausencia de copias de respaldo de la información almacenada y administrada en los recursos de TI del Banco
V41	Ausencia de documentación del proceso
V42	Ausencia de mecanismos de control para regular la seguridad de la información que se intercambia entre procesos (v.gr. acuerdos de confidencialidad, integridad, etc.)
V43	Recursos de tecnología de información que no cuentan con esquemas de autenticación de usuarios (v.gr. cuentas y contraseñas de acceso)
V44	Selección e implementación de componentes de seguridad que no cumplan con los estándares de seguridad de la información definidos por el Banco (v.gr. evaluable, escalable, integrable, etc.).
V45	Ausencia de lineamientos y procedimientos para el acceso desde y hacia la red del Banco
V46	Ausencia de mantenimiento, monitoreo y análisis de logs de seguridad de la infraestructura de TI
V47	Ausencia de mecanismos adecuados para la protección de las transacciones electrónicas
V48	Ausencia de mecanismos de control de acceso físico a áreas restringidas de la compañía (v.gr. centros de cómputos, cuartos de cableado, operaciones, etc.).
V49	Ausencia de mecanismos de control de acceso físico a las instalaciones(v.gr. edificio, instalaciones, oficinas, etc.)
V50	Ausencia de mecanismos de identificación de equipos y autenticación de conexiones
V51	Ausencia de mecanismos de identificación de incidentes o problemas de TI
V52	Ausencia de mecanismos de control de acceso lógico desde internet a los recursos de información del Banco (v.gr. firewalls, etc.).
V53	Ausencia de mecanismos de revisión periódica a las configuraciones seguras que deben tener los recursos de TI (v.gr. equipos portátiles, estaciones de trabajo, etc.)
V54	Ausencia de perfiles de acceso de los usuarios
V55	Realización no autorizada de copias de respaldo y/o restauración de la mismas
V56	Ausencia de personal de seguridad física (vigilancia)
V57	Ausencia de políticas y procedimientos de seguridad de la información vigentes, formales y aplicados
V58	El personal encargado de la administración de recursos de TI no cuenta con los conocimientos técnicos y competencias adecuadas
V59	Ausencia de políticas y procedimientos implementados de clasificación de información basados en contenido, valor y riesgos asociados a la misma

V60	Ausencia de políticas y procedimientos sobre el licenciamiento del software
V61	Ausencia de políticas, procesos y procedimientos para el cumplimiento de los requerimientos legales y entes de control, relacionados con la seguridad de la información (v.gr. CE 052, Ley habeas data, etc.)
V62	Ausencia de políticas, procesos y procedimientos para la administración de copias de respaldo (v.gr. Generación, rotulación, rotación, retención, custodia, recuperación y destrucción)
V63	Falta de mecanismos de protección física de las instalaciones físicas (v. gr. edificio, puertas y ventanas)
V64	Ausencia de registros de auditoría de las actividades realizadas por los usuarios sobre la información que soporta las operaciones del Banco
V65	Ausencia de restricciones de acceso remoto a los recursos de TI
V66	Ausencia de señalización adecuada al interior de las instalaciones.
V67	Ausencia de un esquema de análisis, comunicación, tratamiento y aceptación de riesgos de seguridad de la información
V68	Ausencia de un plan estratégico y táctico de seguridad de la información
V69	Ausencia de un programa de concienciación de seguridad de la información
V70	Ausencia de una estructura organizacional responsable por ejecutar la función de seguridad de la información
V71	Ausencia de lineamientos de seguridad que deben ser considerados durante el desarrollo de aplicaciones (v.gr. in house y adquiridas)
V72	Ausencia o inadecuada definición de métricas e indicadores de desempeño de la función de seguridad de la información (v.gr. KPIs, KGIs, etc.)
V73	Ausencia o inadecuada definición de roles y responsabilidades del recurso humano asignado a la función de seguridad de la información
V74	Ausencia y/o aplicación inconsistente del proceso y procedimientos para la gestión de incidentes de seguridad de la información (v.gr. registro, análisis, clasificación, investigación, escalamiento, etc.)
V75	Ausencia y/o no asignación de responsabilidades sobre los activos de información (v.gr. custodio, etc.)
V76	Brechas en las obligaciones definidas en los contratos
V77	Brechas existentes en la legislación o regulación
V78	Circulación de correo spam en la red del Banco
V79	Código Malicioso
V80	Conexiones con redes públicas no protegidas

V81	Configuración errada o deficiente de los parámetros de control y seguridad de cuentas y contraseñas de acceso (v.gr. bloqueo por tiempo de inactividad, control histórico de contraseñas, bloqueo por intentos de acceso fallidos, longitud mínima de la contraseña de acceso, cambio periódico de la contraseña de acceso, etc.)
V82	Configuración errada de servicios y puertos de comunicación
V83	Configuración inadecuada de los dispositivos de comunicaciones y seguridad del Banco
V84	Construcción deficiente de edificios (v.gr. protección inadecuada de puertas, ventanas, etc.)
V85	Control inadecuado de cambios de la TI que impactan la seguridad de los recursos de información
V86	Copias de respaldo con información insuficiente / no integra
V87	Copias de respaldo en mal estado
V88	Cuentas de acceso con capacidad establecer más de una sesión de acceso a los recursos de TI
V89	Configuración errada de pistas de auditoría
V90	Debilidades conocidas en el software
V91	Asignación deficiente de responsabilidades para la generación y custodia de llaves y criptogramas a terceros (v.gr. Proveedores, contratistas, temporales, etc.)
V92	Definición de contraseñas de acceso triviales (v.gr. Nulas, fáciles de descifrar, etc.)
V93	No aplicación de los estándares de seguridad de la información sobre los recursos de TI del Banco
V94	Definición errada de políticas de seguridad de la información (v.gr. alcance, definiciones, etc.)
V95	Definición y configuración de relaciones de confianza y vínculos no necesarios
V96	Definición de llaves y criptogramas con longitud mínima
V97	Denegación de servicio
V98	Software antivirus desactualizado
V99	Desbordamiento de memoria (búfer overflow)
V100	Desconocimiento de dispositivos de computación móvil y los funcionarios responsables asignados
V101	Desconocimiento de incidentes de seguridad de la información
V102	Desconocimiento de las obligaciones de cumplimiento de los requisitos legales del Banco (v.gr. derechos de autor, privacidad y comercio electrónico).
V103	Desconocimiento de los accesos y privilegios asignados de los usuarios, proveedores y contratistas, etc.

V104	Desconocimiento de prácticas de seguridad de la información por parte de los usuarios del Banco
V105	Desconocimiento del ambiente de TI que soporta las operaciones del Banco (v.gr. aplicaciones, software, hardware, etc.)
V106	Desconocimiento del estado de los activos de información que se usan fuera de las instalaciones
V107	Desconocimiento o conocimiento desactualizado de los activos de información que soportan las operaciones del Banco
V108	Desconocimiento de las técnicas de hacking y tendencias, por parte de los administradores de sistema.
V109	Inadecuada definición y/o ausencia de cláusulas de seguridad de la información en los contratos con empleados, clientes y terceras partes (v.gr. Confidencialidad, etc.)
V110	Desecho o reusó de medios de almacenamiento sin hacer borrado seguro de la información existente
V111	Destrucción no autorizado de información
V112	Deterioro de los medios magnéticos
V113	Diseño deficiente de la arquitectura de seguridad de la información
V114	Divulgación de información confidencial
V115	Documentación desactualizada del SGSI
V116	Documentación insuficiente/obsoleta de los procesos y procedimientos de operación de recursos de TI
V117	Estrategias de recuperación desactualizadas
V118	El recurso humano asignado a la función de seguridad de la información no cuenta con las competencias y habilidades técnicas para el desarrollo de sus funciones
V119	Eliminación de pistas de auditoría en forma no autorizada
V120	Personal no capacitado en el desarrollo del proceso del Banco
V121	Personal de seguridad física no capacitado
V122	Envío de información a destinos no autorizados
V123	Error de controles medio ambientales
V124	Error en el cargue de las llaves y criptogramas
V125	Errores de usuario
V126	Errores del personal encargado de la administración de los recursos de TI
V127	Errores del personal encargado de brindar soporte sobre el funcionamiento de los recursos de TI del Banco
V128	Errores en diseño y construcción de la aplicación
V129	Errores en la configuración funcional de la aplicación
V130	Errores en la configuración funcional de la base de datos

V131	Especificaciones erradas o incompletas para analistas de desarrollo
V132	Cuentas de acceso de usuarios finales con privilegios de administración sobre una aplicación
V133	Iniciativas de gestión de la seguridad de la información que no cumplen con las definiciones de seguridad emitidas por el nivel jerárquico adecuado
V134	Existencia de cuentas y contraseñas de acceso genéricas
V135	Existencia de cuentas de acceso por defecto en los recursos de TI
V136	Existencia de cuentas de acceso activas asignadas a personal retirado del Banco.
V137	Existencia de protocolos innecesarios
V138	Falla de elementos de soporte (UPS)
V139	Falla de la copia de respaldo (backup)
V140	Falla del aire acondicionado
V141	Falla del hardware
V142	Falla del software
V143	Fallas causadas por pruebas de intrusión
V144	Fallas de mantenimiento
V145	Fallas en la integración de componentes de seguridad en la arquitectura tecnológica.
V146	Falta de compromiso de los empleados del Banco con las prácticas de Seguridad de la Información del Banco.
V147	Falta de concientización en seguridad
V148	Falta de control de acceso de usuarios remotos
V149	Falta de depuración de usuarios de los sistemas de información
V150	Falta de documentación de manejo de incidentes de seguridad
V151	Falta de documentación o documentación insuficiente del software
V152	Falta de entrenamiento en seguridad
V153	Falta de esquemas de crecimiento y escalabilidad de la plataforma
V154	Falta de independencia de la función de seguridad de la información
V155	Falta de lineamientos para el manejo, administración y uso de mensajería electrónica
V156	Falta de lineamientos y procedimientos para el uso de utilitarios del sistema.
V157	Falta de mecanismos de control de fluctuaciones de energía
V158	Falta de mecanismos de monitoreo (v.gr. Cámaras de vigilancia, detectores de humedad, detectores de humo, sensores de temperatura, sensores sísmicos, etc.)
V159	Falta de supervisión de mecanismos de monitoreo
V160	Falta de personal de limpieza
V161	Falta de políticas de escritorio y pantalla limpia

V162	Falta de políticas para el uso correcto de software
V163	Falta de políticas para el uso de medios de comunicación
V164	Falta documentación sobre uso de las llaves y criptogramas
V165	Falta de políticas para la conservación y retención de eventos de seguridad
V166	Falta de políticas para la seguridad de los dispositivos de computación móvil
V167	Fluctuaciones Eléctricas
V168	Funcionamiento inadecuado de los dispositivos de seguridad (v.gr. Firewall, etc.)
V169	Generar llaves y criptogramas genéricas o de fácil deducción
V170	Gestión inadecuada de las vulnerabilidades técnicas de seguridad
V171	Habilitación de utilitarios innecesarios en la plataforma tecnológica (Sistemas Operativos)
V172	Ausencia de políticas de sanciones disciplinarias para los casos de violación del modelo de seguridad de la información
V173	Inadecuada administración de acceso remoto (v.gr. falta de procedimientos, reglas del firewall)
V174	Inadecuada asignación de responsabilidad sobre los archivos de información críticos almacenados en los recursos de TI
V175	Inadecuada configuración de seguridad de los ambientes de producción, pruebas y desarrollo
V176	Inadecuada definición de planes de tratamiento de riesgos
V177	Inadecuada definición e implementación de privilegios de acceso sobre los directorios y archivos críticos de los recursos de TI (v.gr. grupos de acceso, perfiles, etc.)
V178	Inadecuada infraestructura física para proteger las áreas que contienen información y servicios de procesamientos de información
V179	Inadecuada segregación de funciones en los perfiles de acceso sobre los sistemas de información
V180	Inadecuada segregación de redes
V181	Inadecuado enrutamiento entre redes
V182	Inadecuado uso de cuentas de administración de los recursos de información (v.gr. Registro de operaciones, etc.)
V183	Inadecuados mecanismos para proteger la información en dispositivos de computación móvil
V184	Incumplimiento con las disposiciones con los derechos de autor y propiedad intelectual
V185	Inexistencia de bitácoras de acceso a las instalaciones y áreas restringidas de la compañía.
V186	Inexistencia de mecanismos de control para el filtrado de tráfico entre

	segmentos de red
V187	Inexistencia de planes de continuidad de negocio y/o los procesos y procedimientos que los soportan
V188	Inexistencia de planes de recuperación de desastres y/o los procesos y procedimientos que los soportan
V189	Inexistencia de procesos y procedimientos para el control de acceso lógico de los usuarios, clientes y terceros a los recursos de información del Banco (v.gr. creación de cuentas de acceso, modificación de cuentas de acceso, etc.)
V190	Inexistencia de un proceso y procedimientos para la gestión de vulnerabilidades
V191	Inexistencia y/o ejecución errada o inconsistente de los procesos y procedimientos de monitoreo de pistas de auditoría de los recursos de TI del Banco
V192	Información de valor para el negocio desprotegida en los puestos de trabajo (v.gr. documentos desprotegidos, sesiones de trabajo no atendidas, etc.).
V193	La consola del servidor se encuentra habilitada cuando se encuentra desatendida
V194	Implantación de recursos informáticos que no contemplan módulo de seguridad (v.gr. gestión de cuentas de acceso, contraseñas, etc.)
V195	Las novedades de cambios organizacionales no se reportan oportunamente a los administradores de recursos informáticos (v.gr. Ingreso de empleados, traslados de empleados, retiros, etc.)
V196	Utilización de datos de producción en ambientes de desarrollo o pruebas
V197	Los equipos de control ambiental no reciben mantenimiento preventivo adecuado y suficiente (v.gr. componentes de TI, sistemas contra incendios, de suministro de energía, etc.).
V198	Cuentas y contraseñas de acceso que se comparten entre varios funcionarios
V199	Uso indebido de los recursos de procesamiento de información o activos de información
V200	Uso herrado o deficiente de las herramientas de auditoría
V201	Mal uso de los sistemas (v.gr. Accidental, deliberado)
V202	Mantenimiento insuficiente a la red de energía y tableros de control
V203	Mantenimiento insuficiente de controles medioambientales
V204	Mantenimiento insuficiente de las instalaciones
V205	Mantenimiento insuficiente de los recursos de TI y/o seguridad
V206	Materiales inflamables empleados en la construcción y acabado de las instalaciones

V207	Materiales inflamables en inmediaciones
V208	Mecanismos deficientes para el reporte de eventos y debilidades relacionadas con la seguridad de la información.
V209	Modificación o eliminación de los mensajes en forma no autoriza
V210	Modificación no autorizado de información
V211	Definición errada de los estándares / patrones de seguridad de la información
V212	No aplicación de parches de seguridad liberados por los proveedores de soluciones de TI
V213	No se cuenta con procedimientos para la generación, custodia y entrega de llaves y criptogramas
V214	Inexistencia de inventario de las redes y servicios a los que pueden acceder los usuarios.
V215	Desincronización de relojes en la plataforma tecnológica del banco.
V216	No existe procedimientos de monitoreo de uso de llaves y criptogramas.
V217	No existen lineamientos para la gestión centralizada de la seguridad
V218	No existen procedimientos que garanticen la devolución de los activos o bienes de información al finalizar la relación laboral o contractual
V219	Protección inadecuada de los activos de información físicos clasificados como confidenciales (v.gr. Organización, archivo, etc.)
V220	No se comunica al personal del Banco los canales por los cuales puede reportar un incidente de seguridad.
V221	No se cuenta con canales para reporte de incidentes
V222	No se cuenta con indicadores de efectividad sobre el programa de concientización
V223	No se cuenta con un inventario de actualizado de las llaves y criptogramas generados
V224	No se cuentan con herramientas para filtrar mensajes electrónicos proveniente de listas negras
V225	No se cuenta con mecanismos seguros para la custodia de las llaves y criptogramas
V226	Recurso humano insuficiente para el desarrollo de la función de seguridad de la información del Banco
V227	Los responsables de los activos de información no se involucran en la autorización de acceso para el uso de los activos de información
V228	No se cuenta con personal responsable por la administración de la seguridad de los diferentes sistemas de información
V229	No se establecen responsabilidades de seguridad de la información para los funcionarios del Banco
V230	No se hace una inducción sobre el modelo de seguridad de la información a nuevos funcionarios
V231	No se informa al nivel jerárquico adecuado los incidentes de seguridad.

V232	Ausencia de acuerdos de confidencialidad firmados
V233	No se pueda establecer si el mensaje en el tiempo ha sido cambiado, alterado-
V234	No se registran los incidentes de seguridad reportados
V235	No se tiene un programa de concientización periódico para todo el personal que permita sensibilizar sobre temas de seguridad
V236	No se verifican de manera periódica las cuentas de acceso y los privilegios asignados
V237	No se verifican los registros de auditoría
V238	Pérdida de integridad de los registros de auditoría
V239	Pérdida de los equipos de trabajo y/o sus dispositivos (v.gr. equipos portátiles, USB, Discos Portátiles, etc.)
V240	Personal no capacitado en el uso de una aplicación
V241	Personal no capacitado en el uso de la Base de Datos
V242	Personal no capacitado en el uso del sistema operativo
V243	Conexión no autorizada de dispositivos de acceso inalámbricos a la red de datos del Banco
V244	Procedimientos de control de acceso físico deficientes
V245	Procedimientos inadecuados para gestión de contratos con terceros (v.gr. Evaluación, selección, terminación, etc.).
V246	Procesamiento errado de información
V247	Procesamiento no autorizado de información
V248	Programas espía (v.gr. aplicaciones de captura de teclado "Keylogger", etc.).
V249	Protección inadecuada de tráfico de datos
V250	Protocolos de red sin cifrar
V251	Puertas traseras (Backdoors)
V252	Puertos o servicios inseguros habilitados (v.gr. ftp, telnet, etc.)
V253	Puertos y servicios no requeridos sobre los recursos de TI
V254	Punto única de falla
V255	Red energética inestable
V256	Ausencia de estándares / patrones de seguridad para la información
V257	Aplicación errada / inconsistente de los estándares de seguridad de la información
V258	Sesiones de trabajo desatendidas (v. gr. Estaciones de trabajo y servidores)
V259	Sistemas insuficientes contra incendios
V260	Situación social inestable (v.gr. manifestaciones políticas, sindicales, ideológicas, etc.).
V261	Subvaloración de un incidente de seguridad de la información
V262	Suplantación de funcionarios del Banco (v.gr. Mediante el uso de

	cuentas y contraseñas de acceso a los recursos informáticos, etc.)
V263	Susceptibilidad de equipos a humedad, polvo
V264	Susceptibilidad de los recursos de TI a variaciones de temperatura
V265	Susceptibilidad de los equipos a variaciones de voltaje
V266	Todas las partes de un llave o criptograma asignadas y/o conocidas a un mismo custodio
V267	Ausencia de supervisión sobre los trabajos realizados por personal externo (v.gr. Limpieza, etc.)
V268	Ubicación de las instalaciones en sector de alto riesgo (v.gr. inundación, terremoto, etc.)
V269	Ubicación inadecuada de equipos
V270	Ubicación susceptible a disturbios, robos o vandalismo.
V271	Uniones deficientes de cables de energía
V272	Uso de canales de comunicación no seguros
V273	Uso de código no autorizado o no probado
V274	Uso del software por usuarios no autorizados
V275	Uso no controlado del correo electrónico.
V276	Uso no restringido de comandos sensitivos sobre los recursos de información
V277	Uso no restringido de dispositivos de almacenamiento extraíbles
V278	Usuarios finales con acceso directo sobre la plataforma de TI que soporta el funcionamiento de las aplicaciones (v.gr. base de datos, sistemas operativos, etc.).
V279	Utilización de algoritmos para cifrado no seguros
V280	Utilización de derechos ilimitados o de administrador de forma predeterminada
V281	Valoración errónea de la criticidad de los activos de información (en relación con su confidencialidad, integridad y disponibilidad)
V282	Uso inadecuado o descuidado del control de acceso físico al edificio y oficinas.
V283	Conexión deficiente de los cables de red
V284	Uso incorrecto de software y hardware
V285	Ausencia de un eficiente control de cambios
V286	Ausencia de acuerdos de niveles de servicio, o insuficiencia de los mismos
V287	Procedimiento inadecuado de contratación
V288	Ausencia de pruebas de envío o recepción de mensajes
V289	Ausencia de identificación y autenticación de emisor y receptor
V290	Ausencia de protección física de la edificación, puertas y ventanas
V291	Falta de custodia de copias de respaldo
V292	Falta de mantenimiento de instalaciones hidráulicas y sanitarias

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Barranquilla, 28 de Julio de 2014

Marque con una X

Tesis [ ] **Trabajo de Grado** [X]

Yo **PABLO ANTONIO GALLEGO MERCADO**, identificado con C.C. No. 8.647.994, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado **DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA PAVIMENTO UNIVERSAL S.A.** presentado y aprobado en el año 2014 como requisito para optar al título de **ESPECIALISTA EN AUDITORIA DE SISTEMAS DE INFORMACIÓN**; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en

defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 28 días del mes de Julio de Dos Mil Catorce 2014

_____

FIRMA

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Barranquilla, 28 de Julio de 2014

Marque con una X

Tesis [ ] **Trabajo de Grado** [X]

Yo **KORINA ISABEL CERVANTES BLANCO**, identificado con C.C. No. 22.491.979, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado **DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA PAVIMENTO UNIVERSAL S.A.** presentado y aprobado en el año 2014 como requisito para optar al título de **ESPECIALISTA EN AUDITORIA DE SISTEMAS DE INFORMACIÓN**; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en

defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 28 días del mes de Julio de Dos Mil Catorce 2014

_____

FIRMA

FORMULARIO DE LA DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS O TRABAJO DE GRADO:

DISEÑO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA PAVIMENTO UNIVERSAL S.A.

SUBTÍTULO, SI LO TIENE:

_____

_____

AUTOR AUTORES

Apellidos Completos	Nombres Completos
GALLEGO MERCADO CERVANTES BLANCO	PABLO ANTONIO KORINA ISABEL

DIRECTOR (ES)

Apellidos Completos	Nombres Completos

JURADO (S)

Apellidos Completos	Nombres Completos

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos

TRABAJO PARA OPTAR AL TÍTULO DE:**ESPECIALISTA EN AUDITORIA DE SISTEMAS DE INFORMACIÓN**

FACULTAD: CIENCIAS ECONIMICAS

PROGRAMA: Pregrado ____ Especialización X

NOMBRE DEL PROGRAMA: ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN

CIUDAD: Barranquilla **AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO:2014**

NÚMERO DE PÁGINAS 118

TIPO DE ILUSTRACIONES:

- ☒ Ilustraciones
- ☐ Láminas
- ☐ Retratos
- ☐ Tablas, gráficos y diagramas
- ☐ Planos
- ☐ Mapas
- ☐ Fotografías

MATERIAL ANEXO (Vídeo, audio, multimedia o producción electrónica):

Duración del audiovisual: _____ minutos.

Número de casetes de vídeo: _____ Formato: VHS ___ Beta Max ___ ¾ ___ Beta Cam ____ Mini DV ____ DVCam ____ DVC Pro ____ Vídeo 8 ____ Hi 8 ____

Otro. Cuál? _____

Sistema: Americano NTSC _____ Europeo PAL _____ SECAM _____

Número de casetes de audio: _____

Número de archivos dentro del DVD (En caso de incluirse un DVD diferente al trabajo de grado):

_____

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial)*:

_____

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS: Son los términos que definen los temas que identifican el contenido. (*En caso de duda para designar estos descriptores, se recomienda consultar con la Unidad de Procesos Técnicos de la Unidad de información en el correo biblioteca@cuc.edu.co, donde se les orientará).*

ESPAÑOL **INGLÉS**

_____ _____

_____ _____

_____ _____

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS:(Máximo 250 palabras-1530 caracteres):

_____

_____

_____

_____

_____