DISEÑO DE UN PLAN DE CONTINGENCIA DEL SISTEMA DE INFORMACIÓN PARA LA ENTIDAD ITRC

HECTOR ALFONSO ACOSTA RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C.
2017

DISEÑO DE UN PLAN DE CONTINGENCIA DEL SISTEMA DE INFORMACIÓN PARA LA ENTIDAD ITRC

HECTOR ALFONSO ACOSTA RAMIREZ

PROYECTO DE GRADO PARA OPTAR EL TITULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA

ASESOR
ING. SALOMON GONZALEZ GARCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA, D.C.
2017

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Abierta y a Distancia UNAD, para optar al título de Especialista en Seguridad Informática

_____
JURADO

_____
JURADO

Bogotá, D.C., mayo de 2017

A mis hijos, a mi
Esposa Libia

AGRADECIMIENTOS

El autor expresa su agradecimiento a:

El ingeniero Guillermo Gomez, jefe de la Oficina Asesora de Tecnologías de la Información de la Agencia ITRC, por su apoyo para poder realizar este proyecto.

A los ingenieros del área de tecnología por sus aportes.

Al director de tesis el Ingeniero Salomón González García, por sus aportes.

Al ingeniero Miguel Ángel Mahecha, tutor de tesis por sus revisiones, comentarios y aportes.

Al ingeniero Edgar Alonso Bojaca Garavito, asesor asignado de la tesis por sus revisiones y aportes para lograr culminar esta tesis.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

En situaciones de desastre se requiere de una respuesta oportuna por parte de los departamentos de tecnología. Es por esto que en este proyecto se plantea un plan de contingencia que dé respuesta a los siniestros que puedan ocurrir, restableciendo los servicios informáticos en los tiempos máximos requeridos por la entidad.

Se presenta un capitulo completo del análisis de riegos de los activos de información para encontrar las amenazas a que están expuestos. Igualmente se plantean los procedimientos que se deben ejecutar en caso de siniestro para recuperar el acceso a la información de vital importancia para la Entidad.

Se plantea también el grupo de personas que atenderán después del siniestro con las actividades por tipo de activo

Por último, se encuentra la forma como se realizará la divulgación del plan de contingencia dentro de la Entidad.

1. INTRODUCCIÓN

En la actualidad se considera que la información de una empresa o entidad es el principal patrimonio, por lo que es de suma importancia aplicar medidas de seguridad que conlleven a proteger la información y estar preparados para hacerle frente a las contingencias y a los diferentes tipos de desastres.

Con un plan de contingencia se puede tener control sobre todo el sistema informático tanto físico como lógico y cuando se presenten desastres causados por hechos naturales o por el hombre. Así mismo, con los planes de contingencia se pueden establecer controles y tomar las medidas necesarias para proteger la información en caso de siniestro.

Para hacerle frente a la contingencia relacionada con la interrupción de actividades debida a la suspensión de los servicios informáticos se ve la necesidad de elaborar un plan de contingencias para la Agencia ITRC el cual comprende en realizar un análisis de los riesgos a los cuales están expuestos los sistemas informáticos y aplicar medidas de seguridad para afrontar las diferentes contingencias.

Para que la entidad logre sus objetivos es de vital importancia que los sistemas de información estén disponibles, por lo tanto, se necesita garantizar que el tiempo de recuperación en momentos de contingencia sea el menor posible a fin de no paralizar el normal funcionamiento.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

La Unidad Administrativa Especial Agencia del Inspector de Tributos, Rentas y Contribuciones (ITRC) es una entidad del gobierno ubicada en la ciudad de Bogotá y creada para realizar detección del fraude en la DIAN, COLJUEGOS y UGPP. Para cumplir con sus objetivos realiza investigaciones, auditorías y recomendaciones que conllevan a evitar el fraude. Es por esto que la ITRC debe actuar de manera oportuna con acciones preventivas y correctivas frente al riesgo de fugas de dinero.

Dando continuidad con esa misión, en el área de tecnología se realizó la implementación de la infraestructura tecnológica la cual da soporte a los sistemas de información conformando la Plataforma de Servicios Tecnológicos. También se realizó la implementación del sistema Integrado de Información misional de la ITRC conformando la Plataforma de gestión de procesos. Adicionalmente, se realizó el estudio previo para implantar un Sistema de Seguridad de la Información - SGSI de la ITRC el cual conforma la Plataforma de Seguridad.

Los procesos implantados dependen totalmente de la plataforma tecnológica, los cuales hacen que la ITRC dependa 100% de los sistemas de información. Actualmente se tienen aplicaciones críticas, las cuales tienen que estar disponibles, junto con todo el sistema informático.

Una aplicación crítica es el expediente digital para atender las investigaciones disciplinarias en la cual se lleva el control totalmente digital con plazos legales y con fechas que se deben cumplir. Lo cual hace que se tenga que prever que los servicios informáticos en la ITRC no dejen de funcionar y garantizar la continuidad del negocio.

Por lo anterior, se propone diseñar un Plan de Contingencia de tal forma que ayude a la Entidad en caso de siniestros al sistema informático, a recobrar rápidamente el control y poder continuar la marcha normal de la entidad.

2.2 FORMULACION DEL PROBLEMA

¿Cómo el diseño de un plan de contingencia del sistema de información para la entidad ITRC ubicada en la ciudad de Bogotá, permitirá, por un lado, mitigar los riesgos potenciales a los cuales está expuesta y, por el otro, a recuperarse garantizando la continuidad en las actividades de dicha entidad?

3. JUSTIFICACIÓN

El presente proyecto tiene como finalidad proponer el diseño de un plan de contingencia de Informática que le permita a la única sede de la Agencia ITRC y ubicada en la ciudad de Bogotá, por un lado, mitigar los riesgos potenciales a los cuales está expuesta y por el otro recuperarse.

Actualmente, la inexistencia de un plan de contingencia, hace que la entidad este expuesta a dejar de funcionar y no pueda responder por las investigaciones disciplinarias, las cuales tienen plazos legales, en fechas, y que pueden llegar a vencer.

Con el plan de contingencia propuesto en este proyecto, la oficina tecnología de Agencia ITRC contara con un instrumento más que abarca el buen manejo de las tecnologías en el campo de soporte y el desempeño. Además, se puede garantizar la continuidad del negocio y se minimizan los riesgos por estar preparado para hacerle frente a las contingencias.

Con este proyecto se evitará la interrupción prolongada de los servicios informáticos en las operaciones de la entidad en caso de contingencia, garantizando que no sea por más de un día, lo que puede llevar a:

- Perdida de información de expedientes como ya se verá en este proyecto.
- Se puedan presentar demandas por perdida de expedientes.
- Darle continuidad a las fechas de los procesados que hacen parte de los expedientes.
- Altos costos monetarios para darle continuidad a la entidad, además que no es fácil en el sector gobierno tener la disponibilidad de dinero porque es con base en presupuesto.

Todo esto conlleva a que este proyecto es necesario para prever qué procedimientos y qué recursos se necesitan ante imprevistos que afecten el sistema informático y que el impacto en las actividades del negocio sea el menor posible. A medida que la entidad se vuelve más dependiente de la tecnología digital para sus procesos diarios, es necesario que los sistemas informáticos estén disponibles ciento por ciento y que tenga un nivel continuo de disponibilidad ya que por el tipo de entidad le pueden acarrear sanciones y demandas.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un plan de contingencia para el sistema de información de la entidad Agencia ITRC ubicada en la ciudad de Bogotá, basado en las normas ISO/IEC 27001 e ISO/IEC 27002.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar los riesgos a que están expuestos los sistemas y recursos informáticos de la entidad, los cuales se tendrán en cuenta en el diseño del plan de contingencia.

- Establecer los procedimientos con los cuales se protegerá la información y garanticen el acceso a la información luego de siniestros de energía eléctrica, inundación, terremotos u otro tipo de fenómenos ambientales.

- Definir la estructura organizacional para formar una administración paralela de contingencia y acción que se encargará de llevar a cabo las acciones en la emergencia con comunicaciones ya definidas.

- Plantear la divulgación y el entrenamiento en los procedimientos del plan de contingencia para fomentar el conocimiento del plan. (buen manejo y aplicación del plan).

5. MARCO REFERENCIAL

5.1 MARCO TEORICO

Hoy en día las empresas manejan grandes cantidades de datos, por lo que es una necesidad incorporar sistemas de información que faciliten la administración de dichos datos y que ayuden en los procesos de gestión de la empresa. Estos sistemas ofrecen una gran cantidad de posibilidades entre las que se encuentran el acceder a los datos relevantes de manera rápida y oportuna y mantener bodegas de datos.

Según un estudio de investigación realizado por PandaLabs[1] en 2007, en la actualidad más del 70% de la seguridad de la información de las compañías están expuestas a situaciones tales como la pérdida de datos importantes, lo cual suele provocar la parálisis de los negocios o hasta el cierre de una empresa. La Seguridad de la información tiene como objetivos básicos garantizar la confidencialidad, integridad y disponibilidad de los datos, los cuales deben garantizarse, en caso de siniestro o contingencia[2]. Es por esto, que la seguridad de la información adquiere una mayor importancia, puesto que, a través de esta, se quiere preservar la confidencialidad, integridad y disponibilidad de la información.

La gestión de la seguridad de la información es un proceso realizado en las empresas para garantizar el nivel más alto de protección de la información. Este se logra desarrollando un proceso sistemático y documentado, cuyo propósito es garantizar que los riesgos de la seguridad de la información queden documentados y sean conocidos por toda la organización a la vez que esos riesgos sean asumidos

---

[1] PANDASECURITY.(2014).*Panda Mediacenter*. Obtenido de http://www.pandasecurity.com/mediacenter/panda-security/

[2] *ISO 27000.ES. "El portal ISO 27001 En Español", Obtenido de http://www.iso27000.es/herramientas.html*

ósea que se decida hasta donde son tolerados, también que se gestionen y por último que sean minimizados.

En el proceso de gestión de la seguridad de los sistemas de información existen una serie de elementos involucrados como: activos informáticos, amenazas, vulnerabilidades, impactos, riesgos, aplicación de salvaguardas y riesgos residuales, los cuales se definirán en el marco conceptual.

Es importante tener en cuenta que sobre los activos informáticos se pueden generar impactos, los cuales pueden ser minimizados a través de la gestión del riesgo, la cual contempla el análisis, la valoración y la clasificación del riesgo, para que luego pueda controlarse[3].

Dentro de los estándares de la gestión de la seguridad de la información podemos encontrar las siguientes: ISO, IEC, ISO/IEC 27000, ISO/IEC 27001 e ISO/27002. La ISO es la organización internacional de estándares y se especializa en el desarrollo y difusión de normas internacionales. La IEC es la comisión electrónica internacional y también es una organización que lidera en todo el mundo la elaboración y difusión de normas internacionales para todas las tecnologías electrónicas, estas dos organizaciones en conjunto crean normas y específicamente para la gestión de seguridad de la información se crearon las normas ISO/IEC 27000, que habla sobre generalidades y vocabularios necesarios para facilitar la implementación de la gestión de seguridad de la información en las empresas. Esta norma en resumen contiene todos los temas y las definiciones para dar una introducción a la gestión de seguridad de la información. Así mismo la ISO/IEC 27001 es la más importante de estas normas porque permite la certificación y además aplica a cualquier tamaño de empresa, también incluye las obligaciones para que en una empresa se establezca los procesos del sistema de seguridad de la información desde

[3] ISO 27001 SECURITY. “Consejos de implantación y métrica de ISO/IEC 27001 Y 27002” http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

implantarlo hasta mejorarlo, pasando por los procesos de operar, supervisar y revisar. Por último, la ISO/IEC 27002 es un compendio de buenas prácticas con recomendaciones referentes a las medidas a tomar para asegurar la gestión de seguridad de la información.

El análisis de riesgos a los sistemas de información, se puede realizar aplicando cualquier tipo de metodología entre ellas la MAGERIT. Esta metodología de análisis y gestión de riesgos de sistemas de información es la que nos permite saber cuánto valor y pérdida de tiempo están en juego, quienes la elaboraron piensan que la gestión de riesgos es el tema principal en las guías del sistema de gestión de seguridad porque antes de realizar la implantación del sistema de seguridad de la información se debe tener conocimientos de los riesgos, permitiendo conocer cuales riesgos deben minimizarse aplicando las medidas de seguridad.

Ahora para prevenir un riesgo, se debe realizar un “plan de contingencia” el cual minimiza considerablemente los riesgos de que los servicios se vean afectados debido a la ocurrencia de un incidente que comprometa la integridad, confidencialidad y disponibilidad de la información o de alguno de sus sistemas informáticos. Para así, restablecer las operaciones del Centro de Cómputo en el menor tiempo posible, después de un siniestro. Y Garantizar la continuidad de los procesos que componen los Sistemas de Información[4].

Para implementar un plan de contingencia según ISO 27000[5] la organización requiere: un análisis de riesgos, la Identificación de procesos críticos y procedimientos que permitan la recuperación de los sistemas de información.

---

[4] POYATO BORGHELLO, C. (2000 - 2009). Segu.info Seguridad de la información. Obtenido de http://www.segu-info.com.ar/politicas/contingencia.htm

[5] Ibid, ISO 27001

5.2 MARCO CONTEXTUAL

5.2.1 ¿Quién es la entidad? La Unidad Administrativa Especial Agencia ITRC, es una entidad del gobierno colombiano con una única sede en la ciudad de Bogotá y cuya principal función es la de vigilar y detectar el fraude en la DIAN, COLJUEGOS y UGPP. Para lograr este objetivo tiene la competencia para auditar a estas tres entidades y a la vez conocer de los procesos disciplinarios que se adelanten contra los funcionarios de dichas entidades. La Agencia ITRC realiza investigaciones de las conductas de dichos funcionarios, que tengan que ver con las faltas disciplinarias relacionadas con el fraude. Por otro lado también adelanta auditorías a estas entidades para realizar recomendaciones sobre los procesos y operaciones. Por todo lo anterior la Agencia necesita trabajar de manera oportuna sobre acciones preventivas o correctivas, ante la posibilidad de riesgo de fuga de dineros en la administración de tributos, aduanas, control del régimen cambiario de importaciones y exportaciones a cargo de la DIAN, UGPP y COLJUEGOS.

La agencia ITRC fue creada por el gobierno nacional, con el Decreto No. 4173 del 3 de Noviembre de 2011 y con el siguiente objeto “Por el cual se crea la Unidad Administrativa Especial Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales-ITRC, se fija su estructura y se señalan sus funciones.

El referido Decreto 4173, estableció que el régimen de personal de los servidores de la AGENCIA, en materia de administración de personal y de carrera administrativa, se regirán por lo establecido en la Ley 909 de 2004, el Decreto 2400 de 1968 y demás normas que lo modifiquen.

Así mismo expidió el Decreto 0986 del 14 de mayo de 2012, por el cual se establece la planta de personal de la Unidad Administrativa Especial AGENCIA del Inspector General de Tributos, Rentas y Contribuciones Parafiscales la cual consta de 122 funcionarios de planta.

5.2.2 ¿Cómo está conformada? La Agencia ITRC cuenta actualmente con ciento veintidós servidores públicos, altamente calificados, y fueron seleccionados con pruebas de alto nivel. La planta de personal cuenta con expertos auditores financieros, jurídicos, de proceso y sistemas, así como con expertos analistas de inteligencia de negocios. También cuenta con abogados, investigadores expertos en derecho disciplinario y un equipo de policía judicial para adelantar investigaciones de manera conjunta con la Fiscalía General de la Nación, funcionarios judiciales, la Contraloría General de la República y demás servidores públicos que cumplan funciones de policía judicial.

La Agencia también cuenta con un grupo de profesionales y técnicos que aportan su experticia para desarrollar eficientemente las actividades administrativas, financieras y tecnológicas necesarias para dar soporte a los procesos misionales de la entidad.

Con este grupo de trabajo se busca la desarticulación de las posibles organizaciones criminales que se pueden infiltrar en las tres entidades auditadas, para lo cual se trabaja conjunta y coordinadamente con la Fiscalía General de la Nación, la Procuraduría General de la Nación y Contraloría General de la República.

5.2.3 ¿Cómo lo Hace? Dentro del marco del Proceso Disciplinario se investiga integralmente, generando fallos en primera y segunda instancia dentro de los procesos que se adelanten contra los empleados públicos encargados de la administración de tributos, aduanas, control del régimen cambiario de importaciones y exportaciones a cargo de la DIAN, contribuciones parafiscales a cargo de la UGPP y rentas de la nación a cargo de Coljuegos, por conductas que se relacionen con las faltas disciplinarias gravísimas.

La Agencia ITRC además promueve las buenas prácticas y detecta las fallas en los procesos y procedimientos, en la seguridad informática y en los recaudos e ingresos que administran las entidades auditadas.

5.2.4 Componente Tecnológico. La Agencia ITRC inicio actividades en el año 2012 y desde momento se iniciaron los proyectos de Tecnología de la Información y las Comunicaciones para dar soporte a los procesos misionales y de apoyo. La primera actividad consistió en implementar la infraestructura tecnológica que diera el soporte a los sistemas de información con lo cual se conformó la plataforma de operación. Como segunda actividad se realizó la Implementación del sistema Integrado de Información misional con lo cual se conformó la plataforma de gestión.

En el área misional de la auditoria se realiza el manejo de grandes volúmenes de información para lo cual se cuenta con bodega de datos, con las cuales se procesan paquetes estadísticos y econométricos; que permiten realizar análisis de caracterización de las entidades y de los contribuyentes que son las fuentes de las rentas de la Nación.

Por otro lado, en el área misional de investigación disciplinaria se implementó una herramienta de gestión de procesos con tecnología BPM en la cual se incorporan todos los expedientes disciplinarios desde su apertura jurídica de la queja/expediente hasta la resolución de sanción y también permitiendo el análisis y el procesamiento de “información” útil y oportuna para la investigación, y la presentación esquemática de casos.

Se cuenta también con herramientas tecnológicas especiales para realizar la labor de investigación con los cuales se busca nuevas formas delictuales y las organizaciones criminales, que se infiltran en entidades vigiladas.

Precisamente, esta área misional llamada la Subdirección de Investigaciones Disciplinarias de la Agencia ITRC, constituye el principal escenario de producción, análisis y consulta de información, de ahí que, se le dedique gran parte del estudio de este proyecto por ser una dependencia especializada en la generación de datos la importancia de su proceso sistematizado, el resguardo de su archivo digital y la dependencia de la tecnología informática.

5.3 MARCO LEGAL

El desarrollo del proyecto se sustenta en estándares normativos, metodologías y buenas prácticas de la información, tales como:

- ISO/IEC 27001:2013 Norma internacional que describe cómo gestionar la seguridad de la información en una organización[6].Específicamente en la sección 4.2.1 donde habla de cómo Establecer el SGSI y en la sección 4.2.2 sobre cómo Implementar y operar el SGSI

- ISO/IEC 27002: 2013 Es una guía de buenas prácticas para un SGSI que describe los objetivos de control y controles recomendados en cuanto a seguridad de la información.

5.4 MARCO CONCEPTUAL

5.4.1 Activos Informáticos. Elementos relacionados con el entorno, con los sistemas de Tecnología de Información de la Comunicación, con la información, con las funcionalidades de la organización. Ejemplo de estos son: personal, instalaciones, los equipos hardware y software, los componentes de

[6] *ICONTEC. NTC-ISO-IEC 27001:2013 ,Tecnología de la información- Técnicas de Seguridad- Sistemas de Gestión de Seguridad de la información- Requisitos.*

comunicaciones de datos[7].

Son los recursos conocidos como hardware y software con los que cuenta un sistema de información dentro de una empresa y sobre estos la mayor amenaza en caso de siniestro es que se destruyan y ocasionen que el sistema de información no funcione correctamente y como consecuencia de esto las operaciones de la empresa se vean afectadas o paralizadas.

5.4.2 Amenazas de los activos. Probabilidad de que ocurra un incidente porque se aprovecha una vulnerabilidad del activo del sistema Estas pueden provocar daños o pérdidas de todo tipo en la organización y se puede materializar desde el interior de la organización o del exterior[8].

Las amenazas se originan a partir de la presencia de una vulnerabilidad, que por un lado puede ser aprovechada por personas externas para hacer daño o por otro lado sin intención de daño pero que pueden poner en riesgo los activos de información.

5.4.3 Disponibilidad. Propiedad de la seguridad de la información que garantiza que la información esté disponible y pueda ser accedida por las personas autorizadas en el momento que ellas lo requieran[9].

---

[7] UNAD. (s.f.). *UNAD 3.2.1 Paso 1: Inventario de Activos*. Obtenido de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321_paso_1_inventario_de_activos.html

[8] Ibid, UNAD

[9] MALAGON,Chelo. MONSERRAT,Francisco. Recomendaciones de Seguridad. Definición de una Política de Seguridad. Obtenido: http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones.html

También se puede decir que es la capacidad que tiene el sistema de información que por un lado dichos sistemas están disponibles para todos los usuarios y por otro que los datos o información pueden ser consultados en todo momento.

5.4.4 Impactos. Consecuencias de la materialización de una amenaza sobre un activo, como pueden ser: la destrucción de ciertos activos, el peligro de integridad del sistema de información, la pérdida de autenticidad, de confidencialidad o de disponibilidad de la información[10].

5.4.5 Integridad. Propiedad que garantiza que la información no ha sido alterada, modificada por personas no autorizadas para hacerlo.

Es uno de objetivos que debe tener la seguridad de la información, la cual indica que es la garantía que la información no ha sido modificada desde que fue creada sin la debida autorización, lo cual nos da la garantía de que la información que se tiene en ese momento es por un lado valida y también que es consistente.

5.4.6 Planes de Contingencia. Planes realizados para minimizar considerablemente los riesgos de que los servicios informáticos se vean afectados debido a la ocurrencia de un incidente que comprometa la integridad, confidencialidad y disponibilidad de la información[11].

Es un plan con procedimientos específicos para cuando se presenta un siniestro y con los cuales se pretende restaurar el sistema informático en el menor tiempo posible.

---

[10] ISO 27001 SECURITY. “Consejos de implantación y métrica de ISO/IEC 27001 Y 27002” http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

[11] GASPAR, J, G. Planes de Contingencia la continuidad del Negocio en las organizaciones. Madrid: Díaz de Santos: D.L., 2004

5.4.7 Riesgos informáticos. Exposiciones dadas por atentados y/o amenazas donde hay posibilidad de pérdidas de información[12].

5.4.8 Riesgos residuales. Reducción de riesgo hasta un nivel aceptable[13].

Es el producto correspondiente a la necesidad de calificar los controles que se han implementado a las vulnerabilidades en el método de la valoración de riesgos, identificados en el sistema de información y con el cual se busca evaluar la efectividad de gestión de dichos controles.

5.4.9 Salvaguardas. Hace referencia a aquellos procedimientos o mecanismos que se realizan para reducir el riesgo[14].

5.4.10 Seguridad informática. Característica informática, de un sistema informativo, que indica que un sistema está libre de amenazas, peligro y/o riesgo[15].

Es una disciplina que busca proteger los recursos informáticos más valiosos, para esto se apoya en normas, procedimientos y la aplicación de estándares de buenas prácticas.

5.4.11 Vulnerabilidades. Debilidad que puede ser explotada por una amenaza[16].

---

[12] *AUDISISTEMAS, "Riesgos informáticos". Obtenido de http://audisistemas2009.galeon.com/productos2229079.html*

[13] Op, ISO 27001

[14] MAGERIT, Metodología de análisis y gestión de riesgos de los sistemas de información VI. Madrid, Ministerio de Administraciones Publicas, Manual 1997

[15] VILLALON HUERTA, A. Seguridad en Unix y redes, Versión 2.1, Free Software Foundation, Inc, 59 Temple Place, Suite 330, Boston, MA , 2002.

[16] MALAGON,Chelo. MONSERRAT,Francisco. Recomendaciones de Seguridad. Definición de una Política de Seguridad. Obtenido: http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones.html

En otras palabras, son los puntos débiles que se encuentran en un sistema informático y que pueden ser, por un lado aprovechados por Hackers o por otro lado ocurrir un daño en el sistema de información a causa de las debilidades.

6. DISEÑO METODOLÓGICO PRELIMINAR

6.1 METODOLOGÍA DE INVESTIGACIÓN

6.1.1 Población y Muestra. La población involucrada en este proyecto son 10 funcionarios de la entidad Agencia ITRC que se encuentran específicamente en el área de la oficina de Tecnologías de la Información. Se tomará también como muestra el cien por ciento de los activos de la plataforma tecnológica y los sistemas de información de dicha entidad.

6.1.2 Recolección y fuentes de información. Como fuentes de información se tendrán en cuenta los documentos del área de tecnología, los inventarios de activos y manuales.

6.1.3 Técnicas e instrumentos para recolección. Como técnicas de recolección se utilizará la revisión documental, para ello se consultarán documentos existentes que son soporte para la gestión de seguridad de la información como son: ISO/IEC 27001[17], ISO/IEC 27002[18], ISO/IEC 27005[19] Metodología MAGERIT y documentos de la organización que soportan el Sistema de Seguridad de la Información.

6.1.4 Procesamiento de la información. El procesamiento de la información para el diseño del plan de contingencia se hará organizando todo lo recolectado para analizarla y realizar el análisis de la información.

---

[17] ISO 27001 SECURITY. "Consejos de implantación y métrica de ISO/IEC 27001 Y 27002" http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

[18] IBID

[19] *ICONTEC. NTC-ISO-IEC 27001:2013 ,Tecnología de la información- Técnicas de Seguridad- Sistemas de Gestión de Seguridad de la información- Requisitos. 2013*

6.1.5 Análisis de datos. El análisis de datos de la información procesada se llevará a cabo con hojas de cálculo (Excel) agregando fórmulas y columnas calificadoras.

6.2 DISEÑO METODOLÓGICO

El diseño metodológico para el desarrollo del proyecto es de tipo analítico-descriptivo porque los resultados se basarán en la observación y análisis descriptivo de lo encontrado. Además, se basa en lo propuesto en la norma internacional ISO/IEC 27001 versión 2013, para el diseño de un Sistema de Gestión de Seguridad de la Información.

El proyecto se desarrollará de acuerdo con las siguientes fases:

6.2.1 Primera fase: planificación. Revisión de estado actual del sistema informático. En esta etapa se enmarcan todas las actividades que permitirán identificar los procesos críticos de la organización, para ello se realizará lo siguiente:

- revisión de estado actual del sistema informático.
- Inventario de los activos informáticos.
- Inventario de las aplicaciones.

6.2.2 Segunda fase: revisión de riesgos y costos. En esta etapa se busca realizar un estudio de los riesgos de todos los recursos informáticos, igualmente se realiza una valoración por interrupción del servicio.

Para realizar ese análisis de riesgos se utilizará la metodología “MAGERIT”, con la cual se podrá establecer, cuáles son los activos de mayor riesgo y de gran impacto. Está es una parte del análisis de riesgos en la cual se cuantifican las pérdidas que se podrían ocasionar en caso de un siniestro.

- Identificar procesos críticos de la organización.
- Listar y valorar los activos informáticos involucrados en cada proceso.

6.2.3 Tercera fase: diseño del plan. En esta etapa se diseñan los procedimientos y se genera el plan a ejecutar en caso del siniestro.

6.2.4 Cuarta fase: Divulgación procedimientos. En esta etapa se define como se van a divulgar los procedimientos en la entidad para que sean conocidos por todos los funcionarios.

7. RECURSOS DISPONIBLES

7.1 RECURSO HUMANO

- ING. HECTOR ACOSTA RAMIREZ, Gestor del proyecto.
- ING. RAFAEL BARRIOS, Encargado de Infraestructura de la Entidad ITRC.
- ING. GUILLERMO GÓMEZ, Jefe oficina de Tecnología de la Entidad ITRC.

7.2 RECURSOS TÉCNICOS, TECNOLÓGICOS, OTROS

Tabla 1. Recursos Técnicos y tecnológicos.

RECURSO	CANTID	NOMBRE	VALOR UNITARIO	VALOR TOTAL
TECNOLÓGICO	1	Computador Portátil	$ 1.500.000	$ 1.500.000
	1	Computador de Escritorio	$ 1.500.000	$ 1.500.000
	1	Impresora	$ 300.000	$ 300.000
TECNICO	1	Fotocopias de documentación	$ 50.000	$ 50.000
	5	Internet	$ 60.000	$ 300.000
	5	Luz	$ 30.000	$ 150.000
	5	Teléfono	$ 50.000	$ 250.000
	5	Transporte	$ 100.000	$ 500.000
			TOTAL	**$ 4.550.000**

Fuente: El Autor.

7.3 FINANCIAMIENTO

El financiamiento del proyecto será asumido totalmente por el ejecutor del proyecto.

8. CRONOGRAMA

A continuación, se presenta un cronograma de actividades para el desarrollo y elaboración del documento final, con un periodo de trabajo aproximando de 3 meses.

Tabla 2. Cronograma del proyecto

ACTIVIDAD	MESES/SEMANAS												
	AGO		SEP				OCT				NOV		
	3	4	1	2	3	4	1	2	3	4	1	2	3
FASE 1: REVISIÓN DE ESTADO ACTUAL DEL SISTEMA INFORMATICO													
FASE 2: REVISION DE RIESGOS Y COSTOS													
FASE 3: DISEÑO DEL PLAN													
FASE 4: DIVULGACION PROCEDIMIENTOS													

Fuente: El Autor

9. DISEÑO DEL PLAN DE CONTINGENCIA PARA LA AGENCIA ITRC

En este capítulo se desarrolla el diseño del plan de contingencia para esta entidad, buscando tener en cuenta todos los servicios que en este momento se encuentran activos.

Los objetivos de este proyecto se van a desarrollar siguiendo estas cuatro fases:

- Revisión del estado actual.
- Revisión de riesgos y costos.
- Diseño del plan.
- Divulgación Procedimientos.

Para el logro del primer objetivo, involucra que se desarrollen las fases 1 y 2 del cronograma propuesto.

Así mismo se realizará el análisis de riesgos y costos, el cual busca establecer cuáles son los activos de información de la Agencia ITRC que están expuestos a un mayor riesgo y cuáles son los activos de información que producirían un gran impacto en caso dado que se materialicen las amenazas que lo puedan afectar.

Es por esto que para realizar ese análisis de riesgos se utilizará la metodología “MAGERIT”, con la cual se podrá establecer cuáles son los activos de mayor riesgo y de gran impacto.

9.1 PRIMERA FASE: REVISION DEL ESTADO ACTUAL.

La Agencia ITRC empezó a funcionar a finales del año 2012, pero en tan corto tiempo se ha realizado la implementación de la infraestructura tecnológica la cual

da soporte a los sistemas de información conformando la Plataforma de Servicios Tecnológicos. También se realizó la implementación del sistema Integrado de Información misional de la ITRC conformando la Plataforma de gestión de procesos. Adicionalmente, se realizó el estudio previo para implantar un Sistema de Seguridad de la Información - SGSI de la ITRC el cual conforma la Plataforma de Seguridad. Pero este desarrollo en tan corto tiempo no ha permitido crear un plan de contingencia informático.

Por lo anterior, el diseño del Plan de Contingencia le va ayudar a la Entidad estar preparada en los casos de siniestros al sistema informático, y a recobrar rápidamente el control y poder continuar la marcha normal de la entidad.

Para revisar el estado actual del sistema de información se tendrá como base la siguiente información:

- Organigrama de la entidad presentado en el Anexo A.
- Inventario del centro de cómputo presentado en la Tabla 3.
- Inventario equipos de red presentado en la tabla 4.
- Inventario equipos de escritorio presentado en la tabla 5.
- Arquitectura actual de la red presentada en el anexo B.
- Inventario de servicios y aplicaciones presentado en la tabla 6.
- Descripción de todos los aplicativos y servicios presentados en las tablas 7 a la 15.

Tabla 3. Inventario del centro de cómputo.

CANT	TIPO DE EQUIPO	MARCA	MODELO
1	SWITCH BORDE 6	HP	MSM720
6	ACCES POINT	HP	MSM430
1	Aire Acondicionado APC	APC	In Row ACSC100 APC
4	BLADE	HP	ProLiant BL460c Gen8
5	BLADE	HP	ProLiant BL460c Gen8
3	BLADE	HP	ProLiant BL460c Gen8
2	BLADE	HP	ProLiant BL460c Gen8
1	CONTROLADORA	HP	MSM720
1	DVR - CCTV	SAMSUNG	Samsung DVR SRD-1670DC
1	ENCLOUSER	HP	C7000
2	FORTINET	FORTINET	D100
1	HP MSL4048 Library	HP	HP Storages Works MSL 4048 Tape Library
1	MONITOR	SAMSUNG	Samsung Sync Master T24B350
1	ROUTER ETB	HUAWEI	N/A
1	SERVIDOR	HP	Proliant DL360p Gen8
1	SERVIDOR	HP	ProLiant DL380e Gen8
1	SERVIDOR	HP	ProLiant DL380e Gen8
3	SWITCH BORDE	HP	A5120
2	SWITCH BORDE	HP	MSM720
1	SWITCH CORE	HP	HP 7506
1	SWITCH DE 8 PUERTOS	HP	N/A

CANT	TIPO DE EQUIPO	MARCA	MODELO
2	UPS Titan	TITAN	Titan EA9920 Cabinet

Fuente: Entidad Agencia ITRC

Tabla 4. Inventario equipos de red.

EQUIPO	TIPO DE DISPOSITIVO	MARCA
SWITCH DE 8 PUERTOS	SWITCH	HP
FORTINET 1	FIREWALL	FORTIGATE
FORTINET 2	FIREWALL	FORTIGATE
SWITCH CORE	SWITCH	HP
ROUTER ETB	ROUTER	HUAWEI
SWITCH BORDE 1	SWITCH	HP
SWITCH BORDE 2	SWITCH	HP
SWITCH BORDE 3	SWITCH	HP
ACCES POINT	ACCESS POINT	HP
ACCES POINT	ACCESS POINT	HP
ACCES POINT	ACCESS POINT	HP
ACCES POINT	ACCESS POINT	HP
ACCES POINT	ACCESS POINT	HP
ACCES POINT	ACCESS POINT	HP
CONTROLADORA	CONTROLADORA INALAMBRICA	HP

Fuente: Entidad Agencia ITRC

Tabla 5. Inventario equipos de escritorio

CANT	AREA	TIPO DE EQUIPO
5	DIR. GENERAL	Escritorio
9	TECNOLOGIAS DE INFORMACION	Escritorio
3	CONTROL INTERNO	Escritorio
4	PLANEACION	Escritorio
3	JURIDICA	Escritorio
20	SECRETARIA GENERAL	Escritorio
32	AUDITORIA I GESTION DEL RIESGO	Escritorio
8	AUDITORIA I GESTION DEL RIESGO	Portatil
37	INVESTIGACIONES DISCIPLINARIAS	Escritorio
8	AUDITORIA I GESTION DEL RIESGO	Portatil
8	INVESTIGACIONES DISCIPLINARIAS	Portatil
4	TECNOLOGIAS DE INFORMACION	Portatil
1	INVESTIGACIONES DISCIPLINARIAS	Impresora
1	SECRETARIA GENERAL	Impresora
1	AUDITORIA I GESTION DEL RIESGO	Impresora
1	TECNOLOGIAS DE INFORMACION	Video Beam
1	TECNOLOGIAS DE INFORMACION	Grabadora de Voz

Fuente: Entidad Agencia ITRC

Tabla 6. Inventario de servicios y aplicaciones

SISTEMA DE INFORMACION	AREA DUEÑA DE INFORMACION
Software automatización del proceso de gestión del expediente digital	Subdirección de Investigaciones Disciplinarias
Software control de inventarios, almacenes, contratos, compras	Secretaria General
NOMINA – GESTION DE PERSONAL - Software gestión del personal, y elaboración de la Nómina	Secretaria General - Talento Humano
CONTROL DE IMPRESIONES - Software de seguimiento y contabilidad de costos de impresión y control de los dispositivos de impresión	Oficina Tecnología de Información
Direccionamiento Estratégico - Software para la gestión del direccionamiento estratégico	Oficina Planeación
Software para auditoria forense	Subdirección de Auditoria
Software – Análisis Investigativo	Subdirección de Investigaciones Disciplinarias
Bases de datos – Oracle. Sybase, SQL, Postgres	Todas las áreas
Correo Electrónico	Todas las áreas
internet	Todas las áreas
Microsoft Office	Todas las áreas

Fuente: Entidad Agencia ITRC

Estos sistemas de información se presentan a continuación, en detalle con su arquitectura:

Tabla 7. Software gestión del expediente digital

CARACTERISTICA	DESCRIPCION
Tipo	Aplicación estratégica de ayuda a un área misional de la entidad
Área dueña información	Subdirección de Investigaciones disciplinarias
Unidades que usan la información	- 30 abogados de la subdirección de investigaciones disciplinarias - 5 notificadores - Funcionarios de la DIAN, COLJUEGOS, UGPPP investigados - Abogados apoderados de los investigados - Todos los funcionarios de la entidad, pues también se radica la correspondencia externa e interna
Equipamiento necesario para óptimo funcionamiento	Esta aplicación se encuentra implementada en cinco servidores físicos los cuales básicamente contienen: Servidor Webserver para la presentación de la aplicación vía web lo cual se realiza a través del presentador APACHE Servidor de Aplicación con JBOSS Servidor Web Services, contiene Servidor de mensajes y correo electrónico Servidor de Base de Datos Postgres Servidor de repositorio documental
Fecha necesitada la información con urgencia	Todos los días
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es el más alto que tiene dentro de la entidad. La entidad puede permanecer solo 4 horas sin disponer de la información. En el día y 12 horas en la noche

Fuente: Entidad Agencia ITRC

Tabla 8. Software control de inventarios- administrativo

CARACTERISTICA	DESCRIPCION
Tipo	Aplicación de apoyo a un área administrativa de la entidad
Área dueña información	Secretaría General
Unidades que usan la información	Personal de contratos Personal de compras Personal del área financiera
Equipamiento necesario para óptimo funcionamiento	Esta aplicación se encuentra implementada en tres servidores físicos los cuales básicamente contienen lo siguiente: Servidor Webserver para la presentación de la aplicación vía web lo cual se realiza a través del presentador APACHE Servidor de Aplicación con JBOSS Servidor de Base de Datos Oracle
Fecha necesitada la información con urgencia	Para inventario los fines de mes por cierre pero se requiere semanal para los contratos
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es medio. La entidad puede permanecer hasta 2 semanas sin disponer de la información de inventarios y hasta 1 semana para los contratos.

Fuente: Entidad Agencia ITRC

Tabla 9. Software gestión del personal -nomina

CARACTERISTICA	DESCRIPCION
Tipo	Aplicación de apoyo a un área administrativa de la entidad
Área dueña información	Secretaría General – Sección Talento Humano
Unidades que usan la información	Personal de talento humano Personal del área financiera

CARACTERISTICA	DESCRIPCION
Equipamiento necesario para óptimo funcionamiento	Esta aplicación se encuentra implementada en dos servidores físicos los cuales básicamente contienen lo siguiente: Servidor de Aplicación y presentación vía web se realiza a través del de la aplicación Meta4 Servidor de Base de Datos Oracle
Fecha necesitada la información con urgencia	Para la nómina los fines de mes
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es medio. La entidad puede permanecer hasta 3 semanas sin disponer de la información.

Fuente: Entidad Agencia ITRC

Tabla 10. Software control impresión

CARACTERISTICA	DESCRIPCION
Tipo	Aplicación de apoyo a toda la entidad
Área dueña información	Oficina de Tecnología de la información y toda la entidad.
Unidades que usan la información	Todo el personal de la entidad Personal del área de tecnología de la información.
Equipamiento necesario para óptimo funcionamiento	Esta aplicación se encuentra implementada en dos servidores físicos los cuales básicamente contienen lo siguiente: Servidor de Aplicación y presentación vía web se realiza a través de la aplicación Servidor de Base de Datos en SQL.
Fecha necesitada la información con urgencia	diariamente para el control de las impresiones
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es Alto. La entidad puede permanecer hasta 1 día sin disponer de la información.

Fuente: Entidad Agencia ITRC

Tabla 11. Software direccionamiento estratégico

CARACTERISTICA	DESCRIPCION
Tipo	Aplicación de apoyo a la oficina de Planeación
Área dueña información	Oficina de planeación y toda la entidad
Unidades que usan la información	Todo el personal de la entidad Personal del área de tecnología de la información.
Equipamiento necesario para óptimo funcionamiento	Esta aplicación se encuentra implementada en dos servidores físicos los cuales básicamente contienen lo siguiente: Servidor de Aplicación y presentación vía web se realiza a través del de la aplicación Tomcat Servidor de Base de Datos en Oracle
Fecha necesitada la información con urgencia	fin de mes para estadísticas
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es Bajo. La entidad puede permanecer hasta 3 semanas sin disponer de la información.

Fuente: Entidad Agencia ITRC

Tabla 12. Software auditoria forense

CARACTERISTICA	DESCRIPCION
Tipo	Aplicación de apoyo a la subdirección de Auditoria
Área dueña información	Subdirección de Auditoria
Unidades que usan la información	Personal del área de subdirección de Auditoria.
Equipamiento necesario para óptimo funcionamiento	Esta aplicación se encuentra implementada en un servidor físico, el cual básicamente contiene lo siguiente: Servidor con la Aplicación y el repositorio de datos

CARACTERISTICA	DESCRIPCION
Fecha necesitada la información con urgencia	Diario
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es Medio. La entidad puede permanecer hasta 1 día disponer de la información.

Fuente: Entidad Agencia ITRC

Tabla 13. Software Análisis investigativo

CARACTERISTICA	DESCRIPCION
Tipo	Aplicación de apoyo a la subdirección de Investigaciones disciplinarias
Área dueña información	Subdirección de Investigaciones disciplinarias
Unidades que usan la información	Personal del área de subdirección de Investigaciones disciplinarias
Equipamiento necesario para óptimo funcionamiento	Esta aplicación es de tipo cliente-servidor y se encuentra implementada en un servidor físico el cual básicamente contienen lo siguiente: Servidor con la aplicación Servidor de base de datos SQL.
Fecha necesitada la información con urgencia	Diario
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es Medio. La entidad puede permanecer hasta 1 día disponer de la información.

Fuente: Entidad Agencia ITRC

Tabla 14. Bases de datos, Oracle, Sybase, Postgres

CARACTERISTICA	DESCRIPCION
Tipo	Bases de datos – Oracle. Sybase, SQL, Postgres
Área dueña información	Todas las áreas.

CARACTERISTICA	DESCRIPCION
Unidades que usan la información	Todo el personal
Equipamiento necesario para óptimo funcionamiento	Los motores de base de datos se encuentran implementados en tres servidores físicos los cuales contienen lo siguiente: Servidor con motor Oracle conteniendo las instancias de: Control de Inventarios, Direccionamiento estratégico, Nomina , Servidor con motor Postgres con la instancia de: Expediente Digital Servidor con motor SQL conteniendo las instancias de: Control de Impresiones, análisis investigativo
Fecha necesitada la información con urgencia	Diario
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es Alto. La entidad puede permanecer de acuerdo a los sistemas de información que requieren de la base de datos desde 4 horas hasta 1 semana sin disponer de la información.

Fuente: Entidad Agencia ITRC

Tabla 15. Otros servicios informáticos

CARACTERISTICA	DESCRIPCION
Tipo	Servicio Correo electrónico, Internet
Área dueña información	Todas las áreas.
Unidades que usan la información	Todo el personal
Equipamiento necesario para óptimo funcionamiento	
Fecha necesitada la información con urgencia	Diario
Nivel de importancia y Tiempo máximo de interrupción	El nivel de importancia estratégico es Alto. La entidad puede permanecer de acuerdo a los sistemas de información que requieren de la

CARACTERISTICA	DESCRIPCION
	base de datos desde 4 horas hasta 1 semana sin disponer de la información.

Fuente: Entidad Agencia ITRC

9.2 SEGUNDA FASE: REVISION DE RIESGOS Y COSTOS

En esta etapa se busca realizar un estudio de las vulnerabilidades, enfocado solo para el caso de siniestros, de todos los recursos informáticos. Igualmente se realiza una valoración por interrupción del servicio. Esta es una parte del análisis de riesgos en la cual se cuantifican las pérdidas que se podrían ocasionar en caso de un siniestro.

Así mismo se realizará el análisis de riesgos y costos, el cual busca establecer cuáles son los activos de información de la Agencia ITRC ubicada en ciudad de Bogotá, que están expuestos a un mayor riesgo y cuáles son los activos de información que producirían un gran impacto en caso dado que se materialicen las amenazas que lo puedan afectar.

Como se indicó en el apartado anterior se utilizará la metodología “MAGERIT” para realizar este análisis de riesgos, por lo que se van a desarrollar los siguientes pasos:

- Identificación de activos de información
- Valoración de los activos de información
- Identificación de amenazas
- Valoración de las amenazas
- Determinar el impacto potencial y el riesgo potencial
- Determinar el riesgo residual

9.2.1 Identificación de activos de Información. Para realizar el análisis de riesgos involucra la identificación de activos de información que apoyan los procesos de la Agencia ITRC y con ello llegar a identificar aquellos activos de información de mayor criticidad para la entidad

Según la norma ISO/IEC 27001 un “activo de Información” es cualquier cosa que tenga valor para una organización y en consecuencia, deba ser protegido. El primer paso es la identificación de activos de información y se debe hacer teniendo en cuenta la importancia que cada “candidato” a ser activo posea dentro del proceso de la cadena de valor que lo utiliza y de la sensibilidad de la información que maneja. Una vez identificados preliminarmente los activos de información asociados a los procesos que se hayan definido como alcance, se debe validar con los propietarios de dichos activos su existencia y unicidad. Posteriormente, cada activo de información debe ser valorado de acuerdo con su impacto por la pérdida de la Confidencialidad, la Integridad y la Disponibilidad.

Los activos identificados se presentan a continuación:

Tabla 16. Activos de información

TIPO DE ACTIVO	PROCESO	ACTIVO	SIGLA ACTIVO
ACTIVO DE INFORMACION	Gestión Tecnologías de la Información	Bases de datos – Oracle. Sybase, SQL, Postgres	BD
SOFTWARE O APLICACIONES	Gestión investigaciones Disciplinarias	Software automatización del proceso de gestión del expediente digital	EXP-DIGITAL
SOFTWARE O APLICACIONES	Gestión Administrativa	Software control de inventarios, almacenes, contratos, compras	ADMINIST
SOFTWARE O APLICACIONES	Gestión de Talento Humano	NOMINA – GESTIÓN DE PERSONAL - Software gestión del personal, y elaboración de la Nómina	NOMINA

TIPO DE ACTIVO	PROCESO	ACTIVO	SIGLA ACTIVO
SOFTWARE O APLICACIONES	Gestión Tecnologías de la Información	CONTROL DE IMPRESIONES - Software de seguimiento y contabilidad de costos de impresión y control de los dispositivos de impresión	IMPRES
SOFTWARE O APLICACIONES	Gestión estratégica	Direccionamiento Estratégico - Software para la gestión del direccionamiento estratégico	DIR-ESTRAT
SOFTWARE O APLICACIONES	Gestión Auditoria y Riesgos	Software para auditoria forense	FORENSE
SOFTWARE O APLICACIONES	Gestión investigaciones Disciplinarias	Software – Análisis Investigativo	INVEST
SOFTWARE O APLICACIONES	Gestión Tecnologías de la Información	Microsoft Office	OFFICE
HARDWARE	Gestión Tecnologías de la Información	BLADE HP ProLiant BL460c Gen8	SERV
HARDWARE	Gestión Tecnologías de la Información	BLADE HP ProLiant BL460c Gen8	SERV
HARDWARE	Gestión Tecnologías de la Información	BLADE HP ProLiant BL460c Gen8	SERV
HARDWARE	Gestión Tecnologías de la Información	BLADE HP ProLiant BL460c Gen8	SERV
HARDWARE	Gestión Tecnologías de la Información	ENCLOUSER HP C7000	SERV
HARDWARE	Gestión Tecnologías de la Información	HP MSL4048 Library HP HP Storages Works MSL 4048 Tape Library	SERV
HARDWARE	Gestión Tecnologías de la Información	SERVIDOR HP Proliant DL360p Gen8	SERV
HARDWARE	Gestión Tecnologías de la Información	SERVIDOR HP ProLiant DL380e Gen8	SERV
HARDWARE	Gestión Tecnologías de la Información	SERVIDOR HP ProLiant DL380e Gen8	SERV

TIPO DE ACTIVO	PROCESO	ACTIVO	SIGLA ACTIVO
HARDWARE	Gestión Tecnologías de la Información	ALMACENAMIENTO SAN HP 6300 EVA FC/ 1GB GBE DFF DE 22 Y 12 DISCOS SFR	ALMAC
HARDWARE	Gestión Tecnologías de la Información	SOLUCION DE ALMACENAMIENTO SAN DELL	ALMAC
HARDWARE	Gestión Tecnologías de la Información	DISCOS 480GB,SAS, 6GB, 2.5" SSD	ALMAC
HARDWARE	Gestión Tecnologías de la Información	DISCOS 6TB SAS, 12GB, 3.5" 7K HHD	ALMAC
HARDWARE	Gestión Tecnologías de la Información	DISCOS 600GB, SAS, 6GB, 2.5", 10K HDD	ALMAC
HARDWARE	Toda la Agencia ITRC	PC DE ESCRITORIOS	PC
HARDWARE	Gestión Tecnologías de la Información	DVR - CCTV SAMSUNG Samsung DVR SRD-1670DC	CCTV
HARDWARE	Gestión Tecnologías de la Información	FORTINET FORTINET D100	FORTINET
RED	Gestión Tecnologías de la Información	CONTROLADORA HP MSM720	SWITCH
RED	Gestión Tecnologías de la Información	SWITCH BORDE 6 HP MSM720	SWITCH
RED	Gestión Tecnologías de la Información	SWITCH BORDE HP A5120	SWITCH
RED	Gestión Tecnologías de la Información	SWITCH BORDE HP MSM720	SWITCH
RED	Gestión Tecnologías de la Información	SWITCH CORE HP HP 7506	SWITCH
RED	Gestión Tecnologías de la Información	SWITCH DE 8 PUERTOS HP N/A	SWITCH
RED	Gestión Tecnologías de la Información	ACCES POINT HP MSM430	ACCES-P

TIPO DE ACTIVO	PROCESO	ACTIVO	SIGLA ACTIVO
RED	Gestión Tecnologías de la Información	ROUTER ETB HUAWEI N/A	ROUTER
SERVICIO	Gestión Tecnologías de la Información	Internet	INTERNET
SERVICIO	Gestión Tecnologías de la Información	Correo Electrónico	EMAIL
INFRAESTRUCTURA	Gestión Tecnologías de la Información	Aire Acondicionado APC APC In Row ACSC100 APC	AIRE-ACON
INFRAESTRUCTURA	Gestión Tecnologías de la Información	UPS Titan TITAN Titan EA9920 Cabinet	UPS
INFRAESTRUCTURA	Gestión Tecnologías de la Información	Detección de Incendios	DET INCEND
INFRAESTRUCTURA	Gestión Tecnologías de la Información	control acceso	CONT ACCESO
PERSONAL	Gestión Tecnologías de la Información	personal informático (9 personas)	PERS
PERSONAL	Toda la Agencia ITRC	usuarios finales (120 personas)	PERS

Fuente: Entidad Agencia ITRC

9.2.2 Valoración de los activos de información. Para el desarrollo del proyecto se tendrá en cuenta la siguiente tabla para la valoración cualitativa de los activos, la cual se utilizar en la valoración de activos y que se presenta en la tabla de valoración de activos.

Tabla 17. Valoración Cualitativa de los activos

VALORACION CUALITATIVA	COSTO DEL ACTIVO (millones de pesos)
MUY ALTO	1.000 a 3.000
ALTO	500 a 999

VALORACION CUALITATIVA	COSTO DEL ACTIVO (millones de pesos)
MEDIO	100 a 499
BAJO	50 a 49
MUY BAJO	1 a 49

Fuente: El Autor**.**

Tabla 18. Valoración de activos

TIPO DE ACTIVO	ACTIVO	VALORACION CUALITATIVA
ACTIVO DE INFORMACION	Bases de datos – Oracle. Sybase, SQL, Postgres	MUY ALTO
SOFTWARE O APLICACIONES	Software automatización del proceso de gestión del expediente digital	MUY ALTO
SOFTWARE O APLICACIONES	Software control de inventarios, almacenes, contratos, compras	MEDIO
SOFTWARE O APLICACIONES	NOMINA – GESTION DE PERSONAL - Software gestión del personal, y elaboración de la Nómina	BAJO
SOFTWARE O APLICACIONES	CONTROL DE IMPRESIONES - Software de seguimiento y contabilidad de costos de impresión y control de los dispositivos de impresión	MUY BAJO
SOFTWARE O APLICACIONES	Direccionamiento Estratégico - Software para la gestión del direccionamiento estratégico	MEDIO
SOFTWARE O APLICACIONES	Software para auditoria forense	MEDIO
SOFTWARE O APLICACIONES	Software – Análisis Investigativo	MEDIO
SOFTWARE O APLICACIONES	Microsoft Office	BAJO
HARDWARE	BLADE HP ProLiant BL460c Gen8	ALTO
HARDWARE	BLADE HP ProLiant BL460c Gen8	ALTO
HARDWARE	BLADE HP ProLiant BL460c Gen8	ALTO
HARDWARE	BLADE HP ProLiant BL460c Gen8	ALTO
HARDWARE	ENCLOUSER HP C7000	ALTO

TIPO DE ACTIVO	ACTIVO	VALORACION CUALITATIVA
HARDWARE	HP MSL4048 Library HP HP Storages Works MSL 4048 Tape Library	MEDIO
HARDWARE	SERVIDOR HP Proliant DL360p Gen8	ALTO
HARDWARE	SERVIDOR HP ProLiant DL380e Gen8	ALTO
HARDWARE	SERVIDOR HP ProLiant DL380e Gen8	ALTO
HARDWARE	ALMACENAMIENTO SAN HP 6300 EVA FC/ 1GB GBE DFF DE 22 Y 12 DISCOS SFR	MUY ALTO
HARDWARE	SOLUCION DE ALMACENAMIENTO SAN DELL	MUY ALTO
HARDWARE	DISCOS 480GB,SAS, 6GB, 2.5" SSD	ALTO
HARDWARE	DISCOS 6TB SAS, 12GB, 3.5" 7K HHD	ALTO
HARDWARE	DISCOS 600GB, SAS, 6GB, 2.5", 10K HDD	ALTO
HARDWARE	PC DE ESCRITORIOS	MUY BAJO
HARDWARE	DVR - CCTV SAMSUNG Samsung DVR SRD-1670DC	MUY BAJO
HARDWARE	FORTINET FORTINET D100	MEDIO
RED	CONTROLADORA HP MSM720	MEDIO
RED	SWITCH BORDE 6 HP MSM720	ALTO
RED	SWITCH BORDE HP A5120	ALTO
RED	SWITCH BORDE HP MSM720	ALTO
RED	SWITCH CORE HP HP 7506	MUY ALTO
RED	SWITCH DE 8 PUERTOS HP N/A	MEDIO
RED	ACCES POINT HP MSM430	MEDIO
RED	ROUTER ETB HUAWEI N/A	BAJO
SERVICIO	Internet	BAJO
SERVICIO	Correo Electrónico	BAJO
INFRAESTRUCTURA	Aire Acondicionado APC APC In Row ACSC100 APC	MEDIO
INFRAESTRUCTURA	UPS Titan TITAN Titan EA9920 Cabinet	MEDIO
INFRAESTRUCTURA	Detección de Incendios	MUY BAJO
INFRAESTRUCTURA	control acceso	MUY BAJO

Fuente: Entidad Agencia ITRC

9.2.3 Identificación de amenazas. La identificación de las amenazas se realiza de acuerdo a la siguiente clasificación y están clasificadas en cuatro grandes grupos:

[N] Desastres naturales
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

[I] De origen industrial
[I.1] Fuego
[I.2] Daños por agua
[I*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración

[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino

[E.9] Errores de [re-]encaminamiento

[E.10] Errores de secuencia

[E.14] Fugas de información

[E.15] Alteración de la información

[E.16] Introducción de falsa información

[E.17] Degradación de la información

[E.18] Destrucción de la información

[E.19] Divulgación de información

[E.20] Vulnerabilidades de los programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.24] Caída del sistema por agotamiento de recursos

[E.25] Pérdida de equipos

[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.4] Manipulación de la configuración

[A.5] Suplantación de la identidad del usuario

[A.6] Abuso de privilegios de acceso

[A.7] Uso no previsto

[A.8] Difusión de software dañino

[A.9] [Re-] encaminamiento de mensajes

[A.10] Alteración de secuencia

[A.11] Acceso no autorizado

[A.12] Análisis de tráfico

[A.13] Repudio

[A.14] Interceptación de información (escucha)

[A.15] Modificación de información

[A.16] Introducción de falsa información

[A.17] Corrupción de la información

[A.18] Destrucción de la información

[A.19] Divulgación de información

[A.22] Manipulación de programas

[A.24] Denegación de servicio

[A.25] Robo de equipos

[A.26] Ataque destructivo

[A.27] Ocupación enemiga

[A.28] Indisponibilidad del personal

Estas amenazas se aplicaran más adelante por tipo de activo según la siguiente tabla y que se presenta sobre la tabla 10 calificación del riesgo residual por tipo de activo.

Tabla 19. Activos agrupados por tipo de activo

TIPO ACTIVO	ACTIVO
INFORMACION	• Bases de datos – Oracle • Bases de datos – Sybase • Bases de datos – Postgres • Bases de datos – SQL
SOFTWARE O APLICACIONES	• Software automatización del proceso de gestión del expediente digital • Software control de inventarios, almacenes, contratos, compras • NOMINA – GESTION DE PERSONAL - Software gestión del personal, y elaboración de la Nómina

TIPO ACTIVO	ACTIVO
	• CONTROL DE IMPRESIONES - Software de seguimiento y contabilidad de costos de impresión y control de los dispositivos de impresión • Direccionamiento Estratégico - Software para la gestión del direccionamiento estratégico • Software para auditoria forense • Software – Análisis Investigativo • Microsoft Office
HARDWARE	• BLADE HP ProLiant BL460c Gen8 • BLADE HP ProLiant BL460c Gen8 • BLADE HP ProLiant BL460c Gen8 • BLADE HP ProLiant BL460c Gen8 • ENCLOUSER HP C7000 • HP MSL4048 Library HP HP Storages Works MSL 4048 Tape Library • SERVIDOR HP Proliant DL360p Gen8 • SERVIDOR HP ProLiant DL380e Gen8 • SERVIDOR HP ProLiant DL380e Gen8 • ALMACENAMIENTO SAN HP 6300 EVA FC/ 1GB GBE DFF DE 22 Y 12 DISCOS SFR • SOLUCION DE ALMACENAMIENTO SAN DELL • DISCOS 6TB SAS, 12GB, 3.5" 7K HHD • DISCOS 600GB, SAS, 6GB, 2.5", 10K HDD • PC DE ESCRITORIOS • DVR - CCTV SAMSUNG Samsung DVR SRD-1670DC • FORTINET FORTINET D100
RED	• CONTROLADORA HP MSM720 • SWITCH BORDE 6 HP MSM720

TIPO ACTIVO	ACTIVO
	• SWITCH BORDE HP A5120 • SWITCH BORDE HP MSM720 • SWITCH CORE HP HP 7506 • SWITCH DE 8 PUERTOS HP N/A • ACCES POINT HP MSM430 • ROUTER ETB HUAWEI N/A
SERVICIO	• Internet • Correo Electrónico
INFRAESTRUCTURA	• Aire Acondicionado APC APC In Row ACSC100 APC • UPS Titan TITAN Titan EA9920 Cabinet • Detección de Incendios • control acceso
PERSONAL	• personal informático (9 personas) • usuarios finales (120 personas)

Fuente: Entidad Agencia ITRC y el autor

9.2.4 Valoración de las amenazas. En este punto se procede a realizar a cada tipo de activo de información, la valoración de la amenaza que sobre el recaen. Se determinan con base en el cuadro de la frecuencia con que la amenaza se puede presentar y el valor del impacto de la amenaza que afecta a cada dimensión de la seguridad.

Para valorar la frecuencia con que ocurre una amenaza, se utiliza la siguiente escala de valores:

Tabla 20. Valoración frecuencia de la amenaza

FRECUENCIA	VALOR	DESCRIPCION La amenaza se materializa a lo sumo:
MUY BAJA	1	Una vez al año
BAJA	2	Una vez cada 6 meses
MEDIA	3	Una vez cada mes
ALTA	4	Una vez cada semana
MUY ALTA	5	Una vez al día

Fuente: El autor

Después de esto se valora el impacto que causara la amenaza en caso que esta se materialice o se haga realidad.

Para esto se utiliza la siguiente tabla de valoración

Tabla 21. Valoración impacto amenaza

IMPACTO	VALOR	DESCRIPCION Si la amenaza se materializa:
MINIMO	1	El daño no tiene consecuencias muy relevantes para la Entidad
BAJO	2	El daño no tiene consecuencias relevantes para la Entidad
MEDIO	3	El daño tiene consecuencias reseñables para la Entidad
ALTO	4	El daño tiene consecuencias graves reseñables para la Entidad
CRITICO	5	El daño tiene consecuencias muy graves reseñables para la Entidad

Fuente: El autor

Esta valoración se realiza sobre las cinco dimensiones de seguridad:

A – Autenticidad

C – Confiabilidad

I – Integridad

D – Disponibilidad

T – Trazabilidad

9.2.5 Determinar el impacto potencial y el riesgo potencial. A partir de las anteriores tablas en las cuales se obtuvo el impacto en los activos de informacion y de la valoracion de la probabilidad de que una amenaza explote una vulnerabilidad, se obtiene el riesgo potencial, para lo cual se utiliza la siguiente formula:

RIESGO POTENCIAL = IMPACTO AMENAZA x FRECUENCIA OCURRENCIA

Finalmente se calcula el nivel de aceptación del riesgo los cuales utilizamos la tabla del nivel de impacto y la tabla de probabilidad.

Con base en las tablas 20 y 21 al combinarlas queda de la siguente manera:

Tabla 22. Valoracion zonas de riesgo

		NIVEL DE IMPACTO				
		1. MINIMO	2. BAJO	3. MEDIO	4. ALTO	5. CRITICO
PROBABILIDAD	1. MUY BAJA	1	2	3	4	5
	2. BAJA	2	4	6	8	10
	3. MEDIA	3	6	9	12	15
	4. ALTA	4	8	12	16	20
	5. MUY ALTA	5	10	15	20	25

Estas zonas resumen el riesgo potencial asi:

MUY BAJO	Zona de riesgo sin problema (1 >= VR <=2)
BAJO	Zona de riesgo Aceptable (3 >= VR <= 7)
MEDIO	Zona de riesgo Tolerable (8 >= VR <= 15)
ALTO	Zona de riesgo Intolerable (16 >= VR <= 25)

Fuente: El autor.

9.2.6 Determinar el riesgo residual. El riesgo residual corresponde a la necesidad de evaluar los controles, teniendo en cuenta la valoración de los riesgos identificados aquí en el anterior capitulo y la evaluación de la efectividad de la gestión de los controles.

Para realizar la calificación de la gestión de los controles se valora la efectividad con la siguiente escala de cinco valores.

Tabla 23. Valoración efectividad controles

VALOR	ESTADO	CRITERIO
1	NO IMPLANTADO	No existen controles. Es posible que se haya identificado su carencia.
2	INICIAL	Los controles están implantados, pero no han sido estandarizados, no están documentados y no dejan evidencia
3	REPETIBLE	Los controles están implantados de manera estandarizada y dejan evidencia, pero no están documentados.

VALOR	ESTADO	CRITERIO
4	DEFINIDO	Los controles están implantados de manera estandarizada, se encuentran documentados, se han difundido y dejan evidencia. No se encuentran en un proceso de mejora continua.
5	ADMINISTRADO	Es posible monitorear y medir el cumplimiento de los controles y tomar medidas cuando no estén trabajando de forma efectiva. Los controles se encuentran en un proceso de mejora continua.

Fuente: El autor.

Seguidamente el riesgo residual se obtiene a partir del valor de riesgo potencial dividido por el valor obtenido de la calificación de la gestión del control

$$\text{RIESGO RESIDUAL} = \frac{\text{Valor del riesgo potencial}}{\text{Valor eficacia del control}}$$

Tabla 24. Valoración del riesgo residual.

NIVEL DEL RIESGO	CALIFICACION DEL RIESGO RESIDUAL
INACEPTABLE	(16 >= VR <= 25)
IMPORTANTE	(11 >= VR <= 15)
MODERADO	(6 >= VR <= 10)
TOLERABLE	(2 >= VR <= 5)
ACEPTABLE	(0 >= VR <= 1)

Fuente: El autor.

A continuación, se presenta la tabla con el riesgo residual en donde se muestra las amenazas por cada tipo de activo con la respectiva información de riesgo residual.

En esta tabla para mejor comprensión se utilizan las siguientes convenciones:

- Frec : es la frecuencia con que ocurre una amenaza
- A – Autenticidad
- C – Confiabilidad
- I – Integridad
- D – Disponibilidad
- T – Trazabilidad
- Efic contr : es la valoración de la eficacia de los controles.

Tabla 25. Calificación del Riesgo residual

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
INFORMACION																		
[N.*] Desastres naturales	4	5	5				20	20				A17.1.1 Planificación de la continuidad de la seguridad de la información	1	20	20			
[I.1] Fuego	3	5	5				15	15				A11.1.4 Protección contra amenazas externas y ambientales.	4	3,8	3,8			
[I.2] Daños por agua	1	3	3				3	3				A11.1.4 Protección contra amenazas externas y ambientales.	2	1,5	1,5			
[I*] Desastres industriales	1	3	3				3	3				A16.1.2 Reporte de eventos de seguridad de la información	3	1	1			
[I.4] Contaminación electromagnética	1	5	4				5	4				A11.1.4 Protección contra amenazas externas y ambientales.	2	2,5	2			
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	A12.6.1 Gestión de las vulnerabilidades técnicas	4	3,8	3			3
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	3	3	3		2,3
[E.2] Errores del administrador	3	4	4			3	12	12			9	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	2	6	6			4,5
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4	A9.4.1 Restricción de acceso a la información	3	1,7	1,7	1,7		1,3
[E.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6	A9.4.1 Restricción de acceso a la información	3	2,7	2,7	3,3	3,3	2

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[E.18] Destrucción de la información	1	4	5			5	4	5			5	A12.3.1 Respaldo de la información	2	2	2,5			2,5
[E.19] Divulgación de información	3		4	5		3		12	15		9	A13.2.4 Acuerdos de confidencialidad o de no divulgacion	3		4	5		3
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	A.14.2.5 Principio de Construcción de los Sistemas Seguros.	3	2,7	2,7			2
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4	4			3	8	8			6	A.14.2.2 Procedimientos de control de cambios en sistemas	3	2,7	2,7			2
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6	A9.3.1 Uso de información de autenticación secreta	2	3	5	5	5	3
[A.6] Abuso de privilegios de acceso	3	3	3	3	3	2	9	9	9	9	6	A9.2.5 Revisión de los derechos de acceso de usuarios	4	2,3	2,3	2,3	2,3	1,5
[A.8] Difusión de software dañino	2	4	5			4	8	10			8	A12.2.1 Controles contra códigos maliciosos	4	2	2,5			2
[A.11] Acceso no autorizado	2		5	5	5			10	10	10		A9.1.1 Política de control de acceso	3		3,3	3,3	3,3	
[A.15] Modificación de información	3	4	4	5	5	4	12	12	15	15	12	A9.4.1 Restricción de acceso a la información	4	3	3	3,8	3,8	3
[A.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6	A12.3.1 Respaldo de la información	4	2	2	2,5	2,5	1,5
[A.17] Corrupción de la información	2		5	5	3	3		10	10	6	6	A8.2.2 Etiquetado de la información	3		3,3	3,3	2	2
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4	A12.3.1 Respaldo de la información	4	1,3	1,3	1		1
[A.19] Divulgación de información	2		4	5		3		8	10		6	A13.2.4 Acuerdos de confidencialidad o de no divulgacion	3		2,7	3,3		2
[A.26] Ataque destructivo	1	5	5				5	5				A12.3.1 Respaldo de la información	3	1,7	1,7			

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
SOFTWARE O APLICACIONES																		
[N.*] Desastres naturales	4	5	5				20	20				A17.1.1 Planificación de la continuidad de la seguridad de la información	1	20	20			
[I.4] Contaminación electromagnética	1	3	4			4	3	4			4	A11.1.4 Protección contra amenazas externas y ambientales.	4	0,8	1			1
[I.6] Corte del suministro eléctrico	3	3	3			4	9	9			12	A12.6.1 Gestión de las vulnerabilidades técnicas	3	3	3			4
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	3	3	3		2,3
[E.2] Errores del administrador	3	4	4			3	12	12			9	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	3	3			2,3
[E.4] Errores de configuracion	3	5	5	5		4	15	15	15		12	A14.2.5 Principio de Construcción de los Sistemas Seguros.	3	5	5	5		4
[E.8] Difusion de software dañino	1	4	4				4	4				A12.2.1 Controles contra códigos maliciosos	3	1,3	1,3			
[E.20] Vulnerabilidades de los programas (software)	1	4	5	5		5	4	5	5		5	A14.2.9 Prueba de aceptación de sistemas	4	1	1,3	1,3		1,3
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	A.14.2.5 Principio de Construcción de los Sistemas Seguros.	3	2,7	2,7			2
[E.24] Caída del sistema por agotamiento de recursos	2	4	4			3	8	8			6	A.11.2.4 Mantenimiento de los equipos.	3	2,7	2,7			2
E.28] Indisponibilidad del personal	3	4				4	12				12	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	3	4				4

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[A.4] Manipulación de la configuración	2	3	3	3	3	2	6	6	6	6	4	A9.2.5 Revisión de los derechos de acceso de usuarios	4	1,5	1,5	1,5	1,5	1
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	4	6	10	10	10	8	A9.3.1 Uso de información de autenticación secreta	3	2	3,3	3,3	3,3	2,7
[A.6] Abuso de privilegios de acceso	1	3	4	3	4	2	3	4	3	4	2	A9.2.5 Revisión de los derechos de acceso de usuarios	4	0,8	1	0,8	1	0,5
[A.8] Difusión de software dañino	2	4	4			4	8	8			8	A12.2.1 Controles contra códigos maliciosos	4	2	2			2
[A.11] Acceso no autorizado	2		4	5	5	2		8	10	10	4	A9.1.1 Política de control de acceso	4		2	2,5	2,5	1
[A.13] Repudio	2	3				3	6				6	A9.1.2 Acceso a redes y a servicios en red	4	1,5				1,5
[A.22] Manipulación de programas	1	5	5	4	3	4	5	5	4	3	4	A9.4.4 Uso de programas utilitarios privilegiados	4	1,3	1,3	1	0,8	1
[A.24] Denegación de servicio	1	4	5			3	4	5			3	A13.1.2 Seguridad de los servicios de red	3	1,3	1,7			1
[A.28] Indisponibilidad del personal	3	4				4	12				12	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	3				3
HARDWARE																		
[N.*] Desastres naturales	4	5	5			3	20	20			12	A17.1.1 Planificación de la continuidad de la seguridad de la información	1	20	20			12
[I.1] Fuego	3	4	4			4	12	12			12	A11.1.4 Protección contra amenazas externas y ambientales.	3	4	4			4
[I.2] Daños por agua	1	3	3			3	3	3			3	A11.1.4 Protección contra amenazas externas y ambientales.	3	1	1			1

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[I*] Desastres industriales	1	3	3			4	3	3			4	A16.1.2 Reporte de eventos de seguridad de la información	3	1	1			1,3
[I.4] Contaminación electromagnética	1	5	4			3	5	4			3	A11.1.4 Protección contra amenazas externas y ambientales.	4	1,3	1			0,8
[I.5] Avería de origen físico o lógico	2	4	4			3	8	8			6	A.11.2.4 Mantenimiento de los equipos.	4	2	2			1,5
[I.6] Corte del suministro eléctrico	3	4	4			3	12	12			9	A12.6.1 Gestión de las vulnerabilidades técnicas	4	3	3			2,3
[I.7] Condiciones inadecuadas de temperatura o humedad	3	5	5			4	15	15			12	A11.1.4 Protección contra amenazas externas y ambientales.	3	5	5			4
[I.8] Fallo de servicios de comunicaciones	2	4	4			3	8	8			6	A12.6.1 Gestión de las vulnerabilidades técnicas	3	2,7	2,7			2
I.9] Interrupción de otros servicios o suministros esenciales	1	4	5			5	4	5			5	A12.6.1 Gestión de las vulnerabilidades técnicas	4	1	1,3			1,3
[E.24] Caída del sistema por agotamiento de recursos	3	5	5			3	15	15			9	A.11.2.4 Mantenimiento de los equipos.	3	5	5			3
E.25] Pérdida de equipos	1	4	4	5		3	4	4	5		3	A.8.1.1 Inventario de activos	3	1,3	1,3	1,7		1
[E.28] Indisponibilidad del personal	2	4	4			3	8	8			6	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	3	2,7	2,7			2
[A.4] Manipulación de la configuración	2	3	5	5	5	3	6	10	10	10	6	A9.2.5 Revisión de los derechos de acceso de usuarios	3	2	3,3	3,3	3,3	2
[A.5] Suplantación de la identidad del usuario	1	3	5	5	3	2	3	5	5	3	2	A9.3.1 Uso de información de autenticación secreta	4	0,8	1,3	1,3	0,8	0,5
[A.6] Abuso de privilegios de acceso	2	3	3	2	3	4	6	6	4	6	8	A9.2.5 Revisión de los derechos de acceso de usuarios	3	2	2	1,3	2	2,7
[A.7] Uso no previsto	2					4					8	A8.1.3 Uso aceptable de los activos	4					2

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[A.25] Robo de equipos	1	4	4	5		4	4	4	5		4	A11.1.3 Seguridad de oficinas, recintos e instalaciones.	4	1	1	1,3		1
A.26] Ataque destructivo	2	4	4			3	8	8			6	A12.3.1 Respaldo de la información	4	2	2			1,5
[A.27] Ocupación enemiga	1	5	4			3	5	4			3	A11.1.2Controles de acceso físicos	4	1,3	1			0,8
[A.28] Indisponibilidad del personal	2	3				4	6				8	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	1,5				2
RED																		
[N.*] Desastres naturales	4	5	5			4	20	20			16	A17.1.1 Planificación de la continuidad de la seguridad de la información	1	20	20			16
[I.1] Fuego	3	4	4			4	12	12			12	A11.1.4 Protección contra amenazas externas y ambientales.	3	4	4			4
[I.2] Daños por agua	1	4	4			4	4	4			4	A11.1.4 Protección contra amenazas externas y ambientales.	3	1,3	1,3			1,3
[I*] Desastres industriales	1	3	3			3	3	3			3	A11.1.4 Protección contra amenazas externas y ambientales.	3	1	1			1
[I.4] Contaminación electromagnética	1	5	4			4	5	4			4	A11.1.4 Protección contra amenazas externas y ambientales.	4	1,3	1			1
[I.5] Avería de origen físico o lógico	2	4	4			3	8	8			6	A.11.2.4 Mantenimiento de los equipos.	4	2	2			1,5
[I.6] Corte del suministro eléctrico	3	4	4			3	12	12			9	A12.6.1 Gestión de las vulnerabilidades técnicas	4	3	3			2,3
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	5			4	5	5			4	A11.1.4 Protección contra amenazas externas y ambientales.	3	1,7	1,7			1,3
[I.8] Fallo de servicios de comunicaciones	3	4	4			3	12	12			9	A12.6.1 Gestión de las vulnerabilidades técnicas	3	4	4			3

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[E.4] Errores de configuración	2	4	4			3	8	8			6	A14.2.5 Principio de Construcción de los Sistemas Seguros.	3	2,7	2,7			2
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	4	4			3	4	4			3	A.14.2.2 Procedimientos de control de cambios en sistemas	3	1,3	1,3			1
E.25] Pérdida de equipos	1	3	5	5		3	3	5	5		3	A.8.1.1 Inventario de activos	3	1	1,7	1,7		1
[A.4] Manipulación de la configuración	1	3	3	3	3	2	3	3	3	3	2	A9.2.5 Revisión de los derechos de acceso de usuarios	4	0,8	0,8	0,8	0,8	0,5
[A.6] Abuso de privilegios de acceso	1	4	5	3	3	4	4	5	3	3	4	A9.2.5 Revisión de los derechos de acceso de usuarios	3	1,3	1,7	1	1	1,3
[A.11] Acceso no autorizado	1	3	3	5	5		3	3	5	5		A9.1.1 Política de control de acceso	4	0,8	0,8	1,3	1,3	
[A.25] Robo de equipos	3	2	4	5		4	6	12	15		12	A11.1.3 Seguridad de oficinas, recintos e instalaciones.	4	1,5	3	3,8		3
A.26] Ataque destructivo	1	4	4			3	4	4			3	A12.3.1 Respaldo de la información	4	1	1			0,8
[A.28] Indisponibilidad del personal	1	3				4	3				4	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	0,8				1
SERVICIOS																		
[N.*] Desastres naturales	4	5	5			3	20	20			12	A17.1.1 Planificación de la continuidad de la seguridad de la información	1	20	20			12
[I.1] Fuego	3	4	4			4	12	12			12	A11.1.4 Protección contra amenazas externas y ambientales.	3	4	4			4
[I.2] Daños por agua	1	3	3			3	3	3			3	A11.1.4 Protección contra amenazas externas y ambientales.	3	1	1			1
[I*] Desastres industriales	1	3	3			3	3	3			3	A16.1.2 Reporte de eventos de seguridad de la información	3	1	1			1

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[I.4] Contaminación electromagnética	1	5	4			3	5	4			3	A11.1.4 Protección contra amenazas externas y ambientales.	4	1,3	1			0,8
[I.5] Avería de origen físico o lógico	2	4	4	4		3	8	8	8		6	A.11.2.4 Mantenimiento de los equipos.	4	2	2	2		1,5
[I.6] Corte del suministro eléctrico	3	4	4			3	12	12			9	A12.6.1 Gestión de las vulnerabilidades técnicas	4	3	3			2,3
[I.8] Fallo de servicios de comunicaciones	2	4	4			3	8	8			6	A12.6.1 Gestión de las vulnerabilidades técnicas	3	2,7	2,7			2
[E.1] Errores de los usuarios	2	4	4	3		3	8	8	6		6	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	3	2,7	2,7	2		2
[E.2] Errores del administrador	2	4	4			3	8	8			6	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	3	2,7	2,7			2
[E.4] Errores de configuración	2	4	4			3	8	8			6	A.14.2.5 Principio de Construcción de los Sistemas Seguros.	3	2,7	2,7			2
[E.8] Difusión de software dañino	1	4	4			3	4	4			3	A12.2.1 Controles contra códigos maliciosos	3	1,3	1,3			1
E.24] Caída del sistema por agotamiento de recursos	2	3	5			3	6	10			6	A.11.2.4 Mantenimiento de los equipos.	3	2	3,3			2
A.16] Introducción de falsa información	1	4	5	4	4	4	4	5	4	4	4	A9.4.1 Restricción de acceso a la información	4	1	1,3	1	1	1
[A.24] Denegación de servicio	1	4	4			3	4	4			3	A13.1.2 Seguridad de los servicios de red	4	1	1			0,8

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[A.25] Robo de equipos	1	4	5	5		3	4	5	5		3	A11.1.3 Seguridad de oficinas, recintos e instalaciones.	4	1	1,3	1,3		0,8
A.26] Ataque destructivo	1	5	5			4	5	5			4	A12.3.1 Respaldo de la información	4	1,3	1,3			1
INFRAESTRUCTURA																		
[N.*] Desastres naturales	4	5	5			3	20	20			12	A17.1.1 Planificación de la continuidad de la seguridad de la información	1	20	20			12
[I.1] Fuego	3	5	5			4	15	15			12	A11.1.4 Protección contra amenazas externas y ambientales.	3	5	5			4
[I.2] Daños por agua	1	3	3			4	3	3			4	A11.1.4 Protección contra amenazas externas y ambientales.	3	1	1			1,3
[I*] Desastres industriales	1	3	3			3	3	3			3	A11.1.4 Protección contra amenazas externas y ambientales.	3	1	1			1
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	A12.6.1 Gestión de las vulnerabilidades técnicas	4	3,8	3			3
[I.7] Condiciones inadecuadas de temperatura o humedad	3	5	4			4	15	12			12	A12.6.1 Gestión de las vulnerabilidades técnicas	4	3,8	3			3
[E.1] Errores de los usuarios	2	4	4	4		3	8	8	8		6	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	2	2	2		1,5
[A.26] Ataque destructivo	1	4	4			3	4	4			3	A12.3.1 Respaldo de la información	3	1,3	1,3			1
[A.28] Indisponibilidad del personal	1	5					5					A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	1,3				
PERSONAL																		

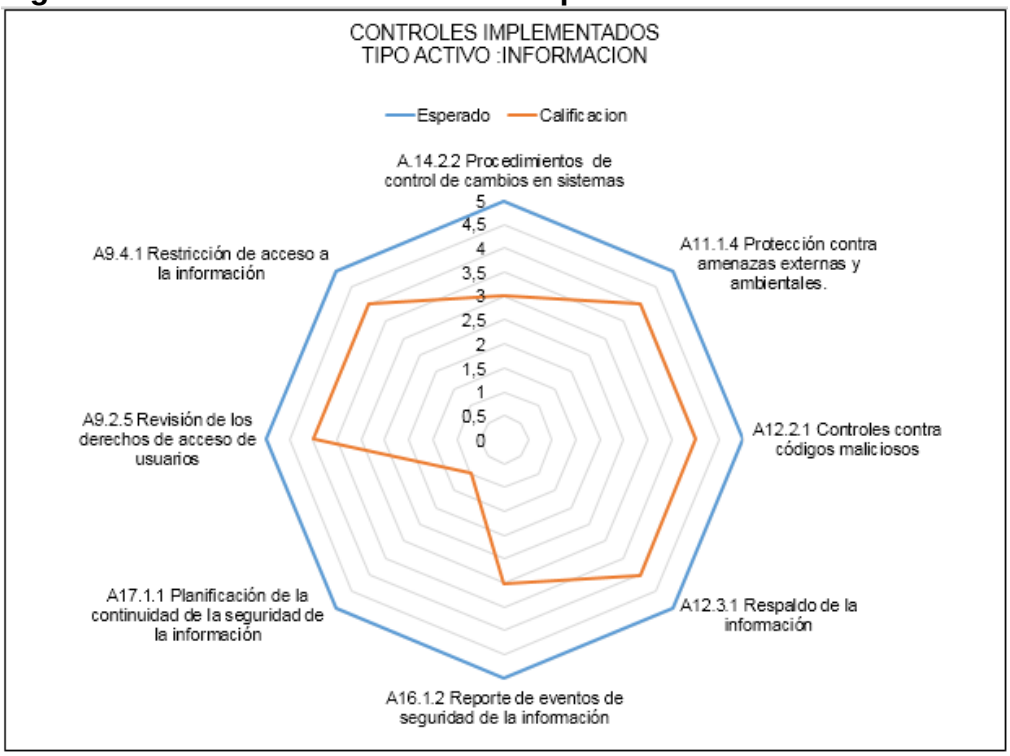
TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[N.*] Desastres naturales	4	5	5			3	20	20			12	A17.1.1 Planificación de la continuidad de la seguridad de la información	1	20	20			12
[I.1] Fuego	3	4	4			4	12	12			12	A11.1.4 Protección contra amenazas externas y ambientales.	3	4	4			4
[I.2] Daños por agua	1	4	4			4	4	4			4	A11.1.4 Protección contra amenazas externas y ambientales.	3	1,3	1,3			1,3
[I*] Desastres industriales	1	3	3			3	3	3			3	A11.1.4 Protección contra amenazas externas y ambientales.	3	1	1			1
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	3	3	3		2,3
[E.2] Errores del administrador	3	4	4			3	12	12			9	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	4	3	3			2,3
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4	A9.4.1 Restricción de acceso a la información	3	1,7	1,7	1,7		1,3
[E.16] Introducción de falsa información	2	4	4	5		3	8	8	10		6	A9.4.1 Restricción de acceso a la información	3	2,7	2,7	3,3		2
[E.18] Destrucción de la información	1	4	5			5	4	5			5	A12.3.1 Respaldo de la información	4	1	1,3			1,3
[E.19] Divulgación de información	3		4	5		3		12	15		9	A13.2.4 Acuerdos de confidencialidad o de no divulgación	3		4	5		3
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	4	4			3	12	12			9	A.14.2.2 Procedimientos de control de cambios en sistemas	3	4	4			3
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6	A9.3.1 Uso de información de autenticación secreta	3	2	3,3	3,3	3,3	2

TIPO DE ACTIVO/AMENAZA	Frec	Valoración Impacto Potencial					Valoración riesgo Potencial					Controles	Efic contr	Valoración riesgo Residual				
		D	I	C	A	T	D	I	C	A	T			D	I	C	A	T
[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4	A9.2.5 Revisión de los derechos de acceso de usuarios	4	1,5	1,5	1,5	1,5	1
[A.8] Difusión de software dañino	2	4	5			4	8	10			8	A12.2.1 Controles contra códigos maliciosos	3	2,7	3,3			2,7
[A.11] Acceso no autorizado	3		5	5	5			15	15	15		A9.1.1 Política de control de acceso	4		3,8	3,8	3,8	
[A.15] Modificación de información	3	4	4	5	5	4	12	12	15	15	12	A9.4.1 Restricción de acceso a la información	4	3	3	3,8	3,8	3
[A.17] Corrupción de la información	1		5	5	3	3		5	5	3	3	A8.2.2 Etiquetado de la información	4		1,3	1,3	0,8	0,8
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4	A12.3.1 Respaldo de la información	4	1,3	1,3	1		1
[A.19] Divulgación de información	3		4	5		3		12	15		9	A13.2.4 Acuerdos de confidencialidad o de no divulgación	3		4	5		3
[A.28] Indisponibilidad del personal	1	5				4	5				4	A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.	3	1,7				1,3

Fuente: Entidad Agencia ITRC y el Autor

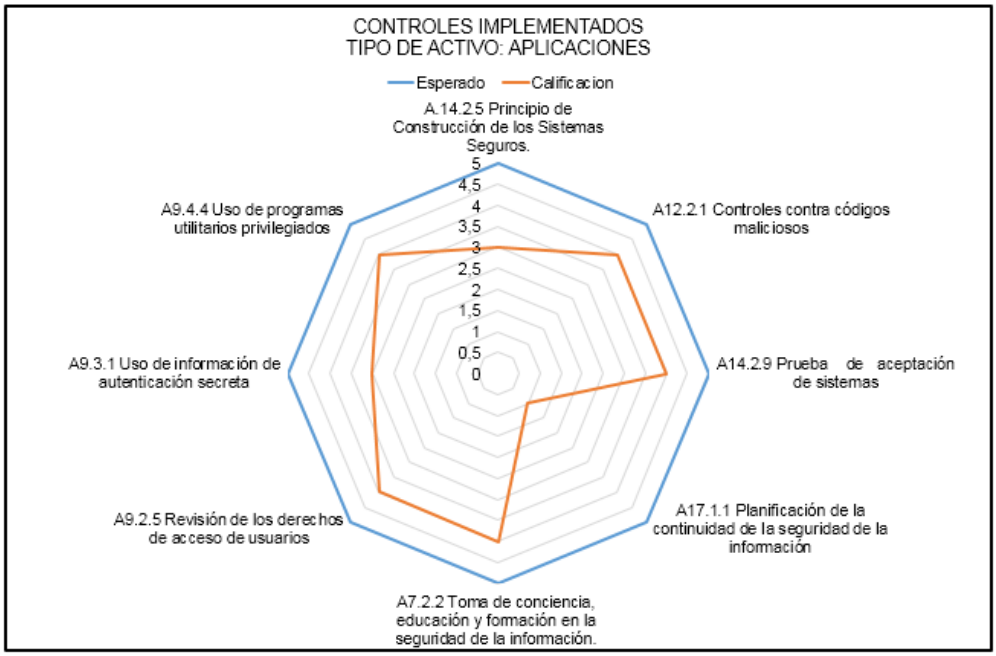
En las siguientes figuras, se puede observar la calificación de todos los controles implementados por tipo de activo. En las cuales se observa claramente que en todos los tipos de activo hay deficiencia en el control A17.1.1-Planificación de la continuidad de la seguridad de la información. El cual obtuvo la calificación más baja y esta sobre 1.

Figura 1. Grafica Radial de activos aplicación



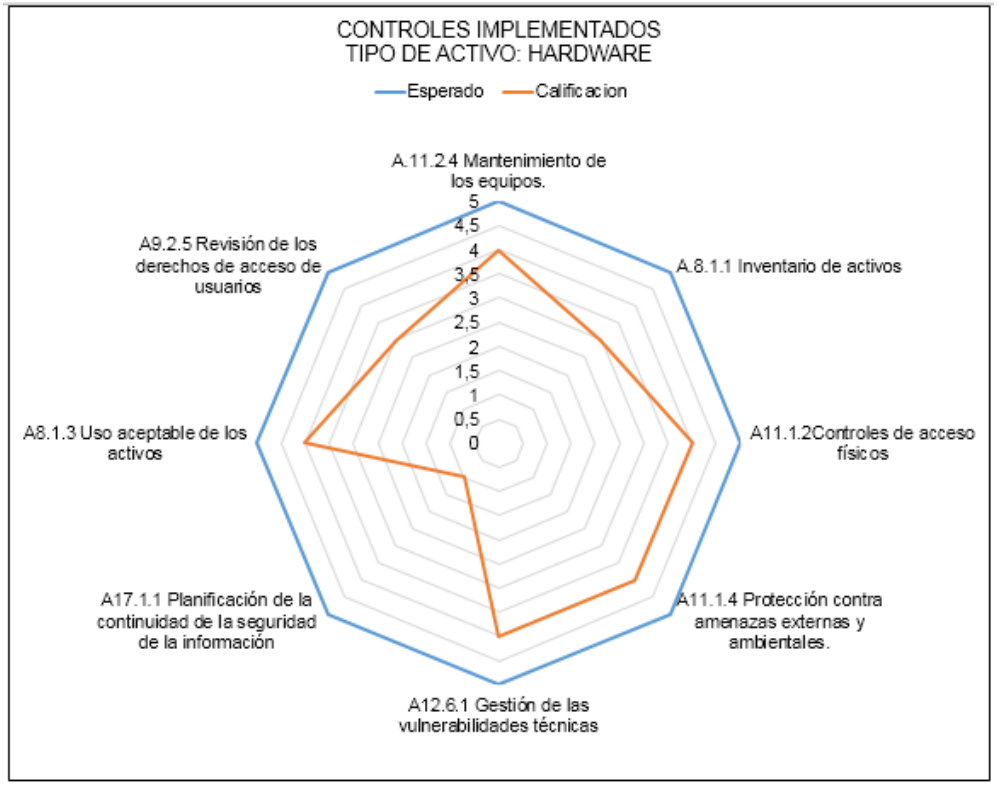
Fuente: El Autor

Figura 2. Grafica Radial activos Software Aplicaciones



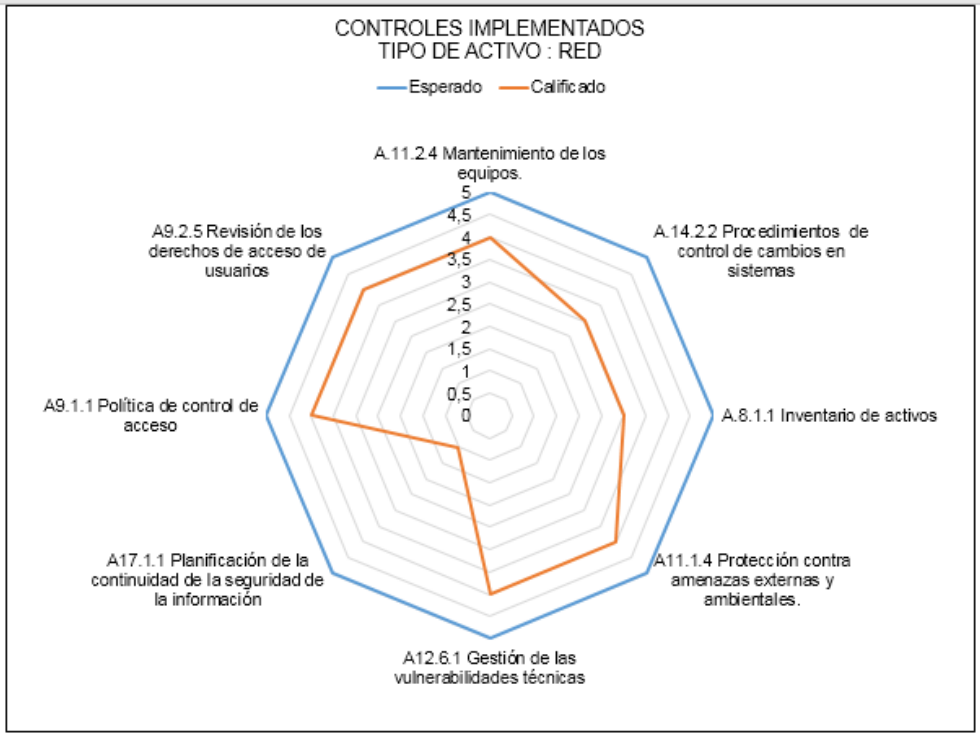
Fuente: El Autor

Figura 3. Grafica Radial de activo Hardware



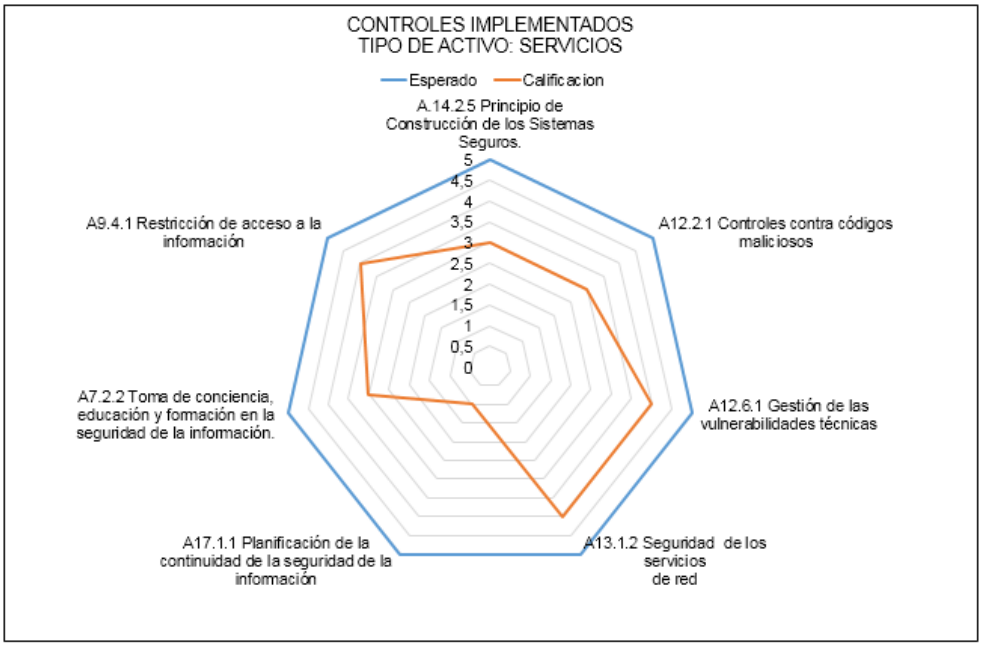
Fuente: El Autor

Figura 4. Grafica Radial activo Red



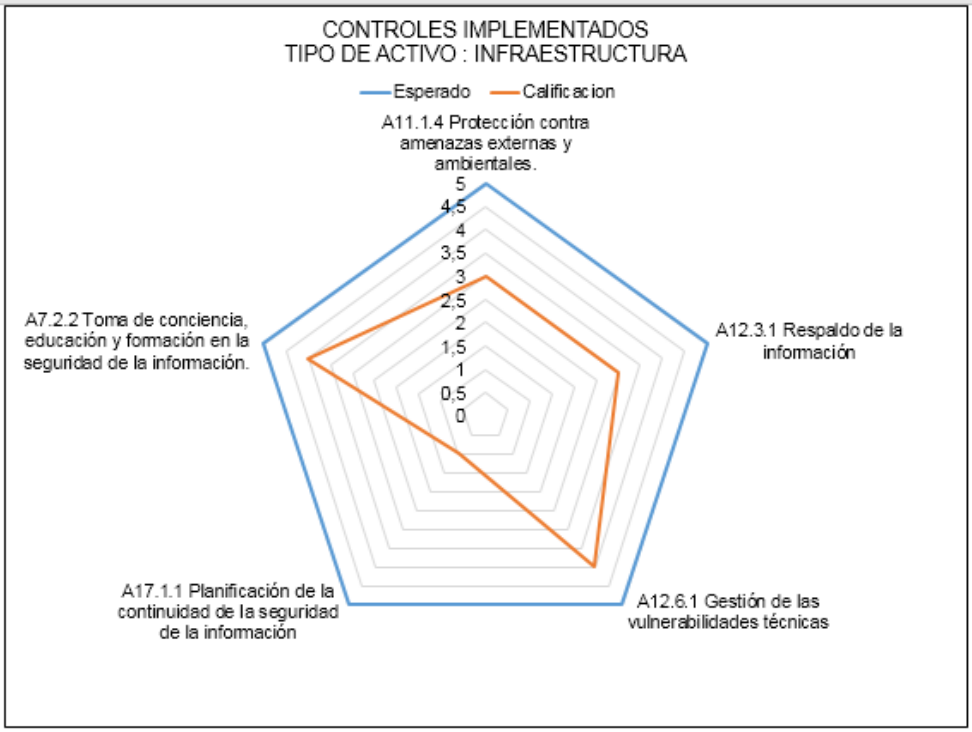
Fuente: El Autor

Figura 5. Grafica Radial activo Servicios



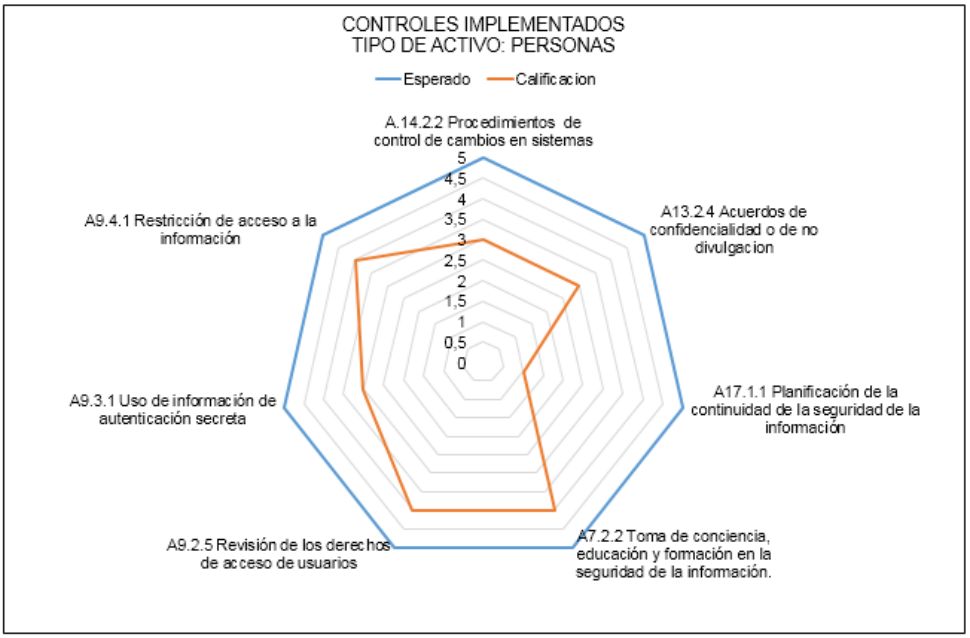
Fuente: El Autor

Figura 6. Grafica Radial activo Infraestructura



Fuente: El Autor

Figura 7. Grafica Radial activo Personas



Fuente: El Autor

9.2.7 Costos de los activos. Para presentar los costos se tendrán en cuenta el costo total para proveer los servicios que ofrece la Oficina de Tecnología incluyendo los costos de mantenerla.

En este capítulo se presentan los costos incurridos, para poder proveer los servicios y utilizar un componente de la infraestructura informática a lo largo de su ciclo de vida, se trata de considerar todos los costos relevantes como:

Costos presupuestados

- Hardware y Software- se toma lo invertido en activos fijos y cuotas de leasing, se incluye además estaciones de trabajo, redes e infraestructura.
- Administración- gastos por personal para la administración de la infraestructura de TI.
- Soporte- gastos para soportar a los usuarios.
- Desarrollo – gastos de mano de obra para el diseño, pruebas, documentación y mantenimiento de aplicaciones.
- Comunicaciones- gastos anuales por servicios de web y acceso remoto.
- Costos no presupuestados.
- Costos en usuario final – Costos por soporte a usuarios no presupuestados, también la capacitación informal.

Tabla 26. Costos tecnología

CATEGORIA	SIGLA	COSTO TOTAL	SUBTOTAL
APLICACIONES	EXP-DIGITAL	1,321,926,453	
	ADMINIST	164,604,000	
	NOMINA	0	
	IMPRES	30,502,456	
	DIR-ESTRAT	86,071,980	
	FORENSE	165,811,330	
	INVEST	249,262,090	
			2,018,178,309

CATEGORIA	SIGLA	COSTO TOTAL	SUBTOTAL
INFORMACION	BD	1,352,042,613	
	EMAIL		
			1,352,042,613
SOFTWARE	INTERNET	85,342,500	
	OFFICE	125,062,621	
			210,405,121
HARDWARE	SERV	712,670,300	
	ALMAC	510,254,423	
	CCTV	47,016,852	
	SEGURID	453,256,100	
			1,723,197,675
RED	SWITCH	303,612,838	
	ACCES-P	35,075,210	
	ROUTER	36,046,372	
			374,734,420
INFRAESTRUCTURA	AIRE-ACON	25,125,256	
	UPS	89,451,011	
	DET INCEND	8,799,628	
	CONT ACCESO	6,308,544	
			129,684,439
SOPORTE Y CAPACITACION		358,323,256	
			358,323,256
		TOTAL	6,166,565,833

Fuente: Entidad Agencia ITRC

9.3 TERCERA FASE: DISEÑO DEL PLAN

En esta etapa se diseñan los procedimientos y se genera el plan a ejecutar en caso del siniestro.

9.3.1 Procedimientos de reanudación. Después de la contingencia, son los primeros procedimientos a ejecutar para recuperar los procesos más críticos, estos

pueden ser en el sitio principal del centro de cómputo o en el sitio alterno, para esto se cuenta con:

- Procesos críticos dados en el anexo C
- Inventario de activos (cuadro de evaluación) según anexo D
- La entidad en este momento cuenta con sitio alterno

9.3.1.1 Procedimiento para recuperación en el sitio principal

Tabla 27. Procedimiento recuperación en sitio principal

PASO	¿QUE HACER?	¿COMO HACERLO?	¿QUIEN?
1	Evaluar el estado de los activos	Se toma el inventario de activos afectados y se llena el cuadro evaluación de activos	Comité de emergencia tecnológica
2	Evaluar los diferentes escenarios	Se llena el cuadro de escenario del desastre: . Fallas de energía eléctrica . Estado de los servidores críticos . Estado de la red local . Estado de las telecomunicaciones . Estado de las Bases de Datos . Estado de las aplicaciones criticas	Comité de emergencia tecnológica
3	Por falta de energía eléctrica	Gestionar para que se reestablezca la corriente eléctrica, Si el daño va a durar más de 2 días, debe informar al Jefe de Tecnologías de la Información, quien tomara la decisión de pasar al sitio alterno Gestiona y verifica el estado de la planta eléctrica del edificio.	Auxiliar de la Mesa de Ayuda
4	Verificar el estado de los servidores críticos	Ya con la energía funcionando, se procede a verificar el estado	Ingeniero de Infraestructura

PASO	¿QUE HACER?	¿COMO HACERLO?	¿QUIEN?
		de los servidores en el cuadro de evaluación de activos. Si los servidores críticos están bien se procede a encenderlos.	
5	Verificar el estado de la red local	Revisar los switch de Borde y el switch core Verificar si hay red en las estaciones Si hay puertos dañados se procede a reconfigurar los swiches o cargar el archivo de backup de la configuración . el diseño de la red cuenta con un switch de alta disponibilidad	Ingeniero de Redes
6	Verificar el estado de las telecomunicaciones	Si no hay salida a internet se debe: . verificar el estado de la fibra óptica y del canal redundante . gestionar y reportar el incidente ante el proveedor los cuales deben restablecer el servicio en un tiempo máximo de 4 horas	Ingeniero de Redes

Fuente: El Autor**.**

9.3.1.2 Procedimiento recuperación base de datos. Para óptimo funcionamiento de esta aplicación se requieren que los motores de base de datos estén implementados en tres servidores físicos, los cuales contienen lo siguiente:

- Servidor con motor Oracle conteniendo las instancias de: Control de Inventarios, Direccionamiento estratégico, Nomina.
- Servidor con motor Postgres con la instancia de: Expediente Digital.
- Servidor con motor SQL conteniendo las instancias de: Control de Impresiones, análisis investigativo.

Con el siguiente procedimiento se restaurarán todas las bases de datos:

Tabla 28. Procedimiento recuperación Bases de Datos

P	¿QUE HACER?	¿COMO HACERLO?	¿QUIEN?
1	Restaurar la bd Oracle . prerrequisitos	. utilizar la misma versión de cliente usado en el export, como para el import .realizar la configuración de la variable Oracle Home .	Ingeniero DBA
2	Ejecutar el import	Conectarse a la instancia de Oracle Conectarse a la base de datos por sqlplus C:>sqlplus as sysdba SQL >CREATE TABLESPACE TS_AITRC_1_DAT DATAFILE 'C:\app\Administrator\oradata\AITRC2\TS_AITRC_1.DAT' SIZE 100M REUSE AUTOEXTEND ON; SQL>create USER AITRC identified by AITRC default tablespace TS_AITRC_1_DAT temporary tablespace TEMP quota unlimited on TS_AITRC_1_DAT; SQL>GRANT CONNECT TO AITRC with ADMIN OPTION; SQL>grant dba to AITRC; SQL>grant create user to AITRC; SQL>grant alter user to AITRC; SQL>alter USER AITRC identified by AITRC; SQL>exit C:>Impdp AITRC/AITRC@AITRC schemas=AITRC	Ingeniero DBA

P	¿QUE HACER?	¿COMO HACERLO?	¿QUIEN?
3	Revisar que no haya errores	Después del import se debe revisar el log que no haya errores. Si hay errores se deben resolver y volver a ejecutar el paso anterior hasta que la operación sea ejecutada con éxito sin errores.	Ingeniero DBA
4	Restaurar BD Sybase Reinicio del servidor	. Para reiniciar el servidor de base de datos SYBASE se debe entrar como usuario root para mapear los raw device. . Se verifican los permisos sobre la ruta dev/null con el siguiente comando: ls -ltr /dev/null . Si únicamente aparece el raw decive “rawctl” quiere decir que no están mapeados. .Si no están mapeados se deben ejecutar los siguientes comandos: con el usuario root :raw /dev/raw/raw1 /dev/vg01/temp_iq :raw /dev/raw/raw2 /dev/vg02/data_iq :raw /dev/raw/raw3 /dev/vg03/data_system_iq .Validar que ya están mapeados, estando en la ruta '/dev/raw': ls .Deben aparecer los siguientes raw devices: raw1 raw2 raw3 rawctl Entrar con el usuario sybaseiq y subir el motor: Ir a la ruta '/sybaseiq/itrcdb' y ejecutar la siguiente instrucción: :start_iq @itrc_iq.cfg itrc_iq.db Para backup de IQ Backup database to ‘ruta_backup/nombrebackup’ size 2048000 (equivalente a 2 gb)	Ingeniero DBA

P	¿QUE HACER?	¿COMO HACERLO?	¿QUIEN?
		Para backup de ASE Dump database staging_db to ‘ruta_backuo/nombrebackup.bck’	
5	Ejecutar la importación de los datos	En el isql conéctese como sa y verifique las bases de datos que existen actualmente en el dispositivo master y ejecute el cargue de la base de datos > select name from sysdatabases > go > load database Itrc_iq from "Itrc_iq_db_dump" > go	Ingeniero DBA

Fuente: El Autor.

9.3.1.3 Procedimientos recuperación aplicación Expediente Digital. Para óptimo funcionamiento de esta aplicación se requiere que esté implementada en cinco servidores físicos los cuales básicamente contienen:

- Servidor Webserver para la presentación de la aplicación vía web lo cual se realiza a través del presentador APACHE.
- Servidor de Aplicación con JBOSS.
- Servidor Web Services, contiene Servidor de mensajes y correo electrónico.
- Servidor de Base de Datos Postgres.
- Servidor de repositorio documental.

Para restablecer el servidor WEB APACHE se debe realizar los siguientes pasos:

- Utilizar el instalador ubicado en los backups.
- Instalar el Apache con la opción personalizada.
- Dar la información del Network Domain y Server Name utilizar : localhost.

- Dar el nombre de la carpeta del programa: \server\apache.
- Ejecutar el apache como administrador desde la siguiente ubicación C:\server\apache\bin.
- Dar la instrucción httpd.exe -k install.
- Entrar el monitor del apache server, con el cual se puede parar, arrancar, o restablecer el servicio.
- Verificar el funcionamiento del servidor web en el navegador con la siguiente URLhttp:\\localhost.
- Copiar el archivo de backup httpd.conf a la dirección \server\apache\conf, el cual contiene toda la configuración del apache para la aplicación de expediente digital.

Para restablecer el servidor de aplicaciones JBOSS se debe realizar los siguiente:

- Previo instalar el JDK.
- Instalar el Jboss dejando sobre la ruta c:\expdig\jboss.
- Subsistema Domain Web.
- Interfaces – modo de escucha de Jboss.
- Grupos separar las instancias (.war).
- Ejecutar script para la creación de usuarios.
- Configurar la etiqueta de Server.
- Hacer los ajustes a los parámetros de seguridad – configuración archivos ejb’s.
- Configurar las instancias de la aplicación.

En resumen, esta es la información de instalación:

Tabla 29. Resumen instalación expediente digital

RESUMEN INSTALACION APLICACIÓN EXPEDIENTE DIGITAL				
SERVIDOR DE BASE DE DATOS				
Sistema Operativo:	Windows Server 2008	**Versión:**	R2	
Nombre Servidor:	SERVER-BD	**IP:**	IP-BASE-DATOS	
Base de Datos:	POSTGRES	**Versión:**	9.3	
Instancia:	EXPED_DIG EXPED_QUA	**Table Space:**	Default	
Usuario:	ITRCDIG ITRCQUA	**Clave:**		
SERVIDOR DE APLICACIONES				
Sistema Operativo:	WINDOWS SERVER 2012	**Versión:**	R2	
Nombre Servidor:	EXP_DIG	**IP:**	IP-EXPDIG	
Servidor:		**Java:**		
Puerto de servicio:	18080	**Puerto administrador:**	9990	
ITEM				**INSTALADO (S/N)**
Instalación Jboss				
Ruta del Jboss:	**C:\EXPDIG\jobss7**			
Configuración Origen de Datos				
URL:	IP-BASE-DATOS:5432:EXPD_DIG			
Usuario:	ITRCDIG	**Clave:**		
No. Conexiones Activas:		**Nro. de Conexione Abiertas:**		
Configuración de instancias en jobss				
Instancia : Itrc-plant		Puerto:18080		
Instancia : Itrc-msg		Puerto:19080		
URL:	IP-APLICACIÓN:8080/ITRC/			
Configurar cuenta de correo				

RESUMEN INSTALACION APLICACIÓN EXPEDIENTE DIGITAL				
E-Mail:	ITRC-APLIC@ITRC.GOV.CO			
Servidor:	Smpt.office365.com	**Protocolo:**	Smpt	

Fuente: Agencia ITRC

9.3.1.4 Procedimiento recuperación Control de inventarios – administrativo.

Para óptimo funcionamiento de esta aplicación se requieren que esté implementada en tres servidores físicos los cuales básicamente contienen lo siguiente:

- Servidor de Base de Datos ORACLE.
- Servidor Webserver para la presentación de la aplicación vía web lo cual se realiza a través del presentador APACHE.
- Servidor de Aplicación con JBOSS.

Para realizar la instalación desde cero del software ADMIN en el ambiente de producción, se utiliza un CD de backup con la instalación de este aplicativo, el cual contiene los programas de instalación junto con la documentación técnica.

Para restablecer el Servidor DB se debe realizar lo siguiente:

Proceso de creación de la base de datos ADMIN. Se incluyen los siguientes scripts:

- Scripts de creación de tablespaces y usuario.
- Scripts de creación de objetos de bases de datos (tablas, triggers, procedures, datos básicos).
- Scripts e instrucciones para migración de base de datos a producción.

Para restablecer el Servidor Web

Se tienen los diferentes directorios de instalación de productos necesarios para la aplicación ADMIN como son: Java y JBoss.

En el caso de la aplicación se encuentran los archivos war de las diferentes aplicaciones para instalación en el servidor Web como son:

- Archivo WAR de erpRecursos.
- Archivo WAR de erpDocumentos.
- Archivo WAR de la aplicación ADMIN.

Tabla 30. Resumen instalación control inventarios

RESUMEN INSTALACION APLICACIÓN CONTROL DE INVENTARIOS			
SERVIDOR DE BASE DE DATOS			
Sistema Operativo:	Windows Server 2008	**Versión:**	R2
Nombre Servidor:	SERVER-BD	**IP:**	IP-BASE-DATOS
Base de Datos:	Oracle	**Versión:**	11G
Instancia:	AITRC	**Table Space:**	Default
Usuario:	ITRC	**Clave:**	
LISTA DE CHEQUEO			
ITEM			**INSTALADO (S/N)**
Creación usuario DML			
Instalación Tablas			
Instalación Procedimientos almacenados			
Instalación Paquetes			
Instalación datos de carga			
SERVIDOR DE APLICACIONES			

RESUMEN INSTALACION APLICACIÓN CONTROL DE INVENTARIOS				
Sistema Operativo:	WINDOWS SERVER 2012		**Versión:**	R2
Nombre Servidor:	APLICACIÓN		**IP:**	IP-APLICACION
Servidor:			**Java:**	
Puerto de servicio:	8080		**Puerto administrador:**	8080
ITEM				**INSTALADO (S/N)**
Instalación Java Development Kit				
Ruta del JDK:	**C:\Java\JDK1.7.0-09**			
Configuración Origen de Datos				
URL:	IP-BASE-DATOS:1521:AITRC			
Usuario:	ITRC	**Clave:**		
No. Conexiones Activas:		**Nro. de Conexione Abiertas:**		
Instalación de la aplicación erpRecursos.war				
Instalación de la aplicación erpDocumentos.war				
Instalación de la aplicación Formatos.war				
Instalación de la aplicación ADMIN.war				
URL:	IP-APLICACIÓN:8080/ITRC/			
Configurar cuenta de correo				
E-Mail:	ITRC-APLIC@ITRC.GOV.CO			
Servidor:	Smpt.office365.com	**Protocolo:**	Smpt	
Usuario:		**Clave:**		
Pruebas de instalación del sistema				
Ingreso con usuario ADMIN.				
Ingreso opciones usu, grp, sis, mew, con, pct, ADMIN.				
Ejecución de un reporte				
Pruebas de envío de correo				

RESUMEN INSTALACION APLICACIÓN CONTROL DE INVENTARIOS		
Instalación de Alertas (Inspector)		
Ruta:	C:\inspector	
Variable [sis]:	Configurar la variable de sistema **Inspector.path** con la ruta de la carpeta del inspector.	
Configuración de la ejecución automática del inspector		

Fuente: Agencia ITRC

9.3.1.5 Procedimiento recuperación Gestión de personal – nomina. Para óptimo funcionamiento de esta aplicación se requieren que esté implementada en dos servidores físicos los cuales básicamente contienen lo siguiente:

- Servidor de Aplicación y presentación vía web se realiza a través de la aplicación Meta4.
- Servidor de Base de Datos Oracle.

Para la Instalación del servidor de aplicaciones se realiza lo siguiente:

Modificar la variable del sistema ORACLE_HOME y path para la ruta del cliente de Oracle 32 bits.
Realizar la instalación del appserver de peoplenet con la siguiente configuración:
Maquina:
Nombre del host: HP_NOMINA Ip: 1.1.1.30

Tabla 31. Ambientes de aplicación Nomina

Ambiente	**Identificador**	**Puertos**
Desarrollo	Desa-sigep	3002 (y 3003, 3004, 3005)
Desarrollo	Desa-sigep (dispatcher)	3102 (y 3103, 3104, 3105)
Desarrollo	Desa-sigep (controller)	3000, 3001

Ambiente	Identificador	Puertos
Pruebas	Sigep-prepro	4002,4003,4004,4005
Pruebas	Sigep-prepro (dispatcher)	4102,4103,4104,4105
Pruebas	Sigep-prepro (controller)	4000, 4001
Producción	Sigep-prod	5002,5003,5004,5005
Producción	Sigep-prod2	5012,5013,5014,5015
Producción	Sigep-prod3	5022,5023,5024,5025
Producción	Sigep-prod (dispatcher)	5102,5103,5104,5105
Producción	Sigep-prod (controller)	5000,5001

Fuente: La Entidad y el Autor

Realizar la configuración de dispatcher con los datos a continuación:

Puertos de administración:

- Desarrollo: 3104.
- Pruebas: 4104.
- Producción: 5104.

Crear las reglas para el firewall de windows para los puertos:

- Oracle: 1521.

- Peoplenet: 3102-3105, 4102-4105, 5102-5105.

Realizar la configuración de los servicios del appserver, direccionando a las siguientes configuraciones de base de datos:

- Servicio oracle (SID): SIGEP.
- usuario desarrollo: DESSIGEP.
- usuario pruebas: PRESIGEP.
- usuario producción: SIGEP.

Instalar herramienta de administración de servidores de peoplenet AppMonitor.

Instalar el servidor web JRUN para el portal de rich web con los siguientes usuarios:

usuario JRUN: admin

Instalar y configurar el servicio de IIS para el portal richweb con la siguiente configuración específica:

- Soporte aplicaciones IIS 6.
- Soporte ASP.net.
- compatibilidad 32 bit de IIS.

Para este punto se ejecuta la siguiente sentencia de configuración: %windir%\system32\inetsrv\appcmd set config -section:applicationPools -applicationPoolDefaults.enable32BitAppOnWin64:true

Descargar en un cliente dentro de la misma red de la entidad, el portal de richweb para probar la instalación.

9.3.1.6 Procedimiento para recuperación en el sitio alterno. La entidad cuenta con sitio alterno con servidores propios con lo cual puede hacerle frente a estas contingencias.

Tabla 32. Procedimiento recuperación en Sitio Alterno

PASO	¿QUE HACER?	¿COMO HACERLO?	¿QUIEN?
1	Comunicar el estado del sitio alterno	Presenta informe al Jefe de la Oficina, indicando si las maquinas están disponibles	Ingeniero de Infraestructura
2	Dar acceso por red	Realiza cambios en las configuraciones de internet para desviar el trafico	Ingeniero de Redes
3	Verificar el estado de las aplicaciones	Presenta informe al Jefe de la Oficina del estado de las aplicaciones, las cuales previamente fueron instaladas, probadas y se les han hecho las actualizaciones	Ingeniero de aplicativos
4	Gestionar la entrega del Backup	Buscar el backup de las Bases de Datos y del File System que se entrega en custodia, cada semana y se encuentra fuera de la Entidad. Debe realizar una solicitud de préstamo a la empresa custodia.	Ingeniero de B.D.
5	Restaurar los datos	Aplicar el procedimiento de restauración que existe en la Entidad,	Ingeniero de B.D.
6	Verificar la restauración	Realiza las pruebas para verificar que la restauración quedo bien	Ingeniero de B.D.
7	Pruebas a los aplicativos	. Realizar la pruebas verticales y horizontales a los aplicativos . Verificar el estado y tiempo que quedo la aplicación	Usuario líder de cada aplicación Ingeniero de Aplicativos

Fuente: La Entidad y el Autor

9.3.2 Estructura organizacional para la contingencia. En este capítulo se define la estructura organizacional para formar una administración paralela de contingencia y acción que se encargará de llevar a cabo las acciones en la emergencia con comunicaciones ya definidas.

Para definir la estructura organizacional que se encargue de restablecer los sistemas en caso de un siniestro, lo primero a realizar es buscar la protección de la integridad del personal que puede estar en las áreas cercanas a los centros de cómputo.

Después del siniestro deben de existir dos equipos de personas que actúen directamente, un equipo se encargara de combatir el siniestro y otro que tratara de salvar los recursos informáticos.

A continuación, se presenta los integrantes que deben estar formados para que paralelamente puedan ayudar con las labores de restauración del sistema.

9.3.2.1 Comité de emergencia tecnológica. Es la estructura responsable de coordinar las actividades en caso de emergencia o desastre

Estará conformado por:

- Jefe oficina de Tecnología.
- Ingeniero de infraestructura.
- Ingeniero de Redes y comunicaciones.
- Ingeniero DBA.
- Ingeniero de aplicaciones.

Este comité realizara las siguientes tareas:

- Tomar el inventario de activos afectados y generar el cuadro evaluación de activos de información.
- Se llenará el cuadro de escenario del desastre con:
  Fallas de energía eléctrica
  Estado de los servidores críticos

Estado de la red local
Estado de las telecomunicaciones
Estado de las Bases de Datos
Estado de las aplicaciones criticas

- Realizaran un balance de la situación y determinaran con base en el plan de contingencia en que paso se debe comenzar.
- Gestionar para el inicio lo más pronto posible de la recuperación y puesta en marcha de los servicios informáticos

9.3.2.2 Ingeniero de infraestructura. Este ingeniero estará a cargo básicamente de los servidores y el almacenamiento y debe contar con el siguiente perfil:

- Ingeniero de sistemas, telemática y afines.
- Conocimientos certificados en administración de Sistemas operativos.
- Conocimientos certificados en tecnologías open source.
- Conocimientos certificados en servidores y almacenamiento.

Tiene las siguientes funciones:

- Administrar los Servidores.
- Administrar el Sistema de Almacenamiento SAN.
- Administrar el Sistema de los backups o copias de respaldo.

Realiza las siguientes tareas en el sitio principal

- Con la energía funcionando, se procede a verificar el estado de los servidores en el cuadro de evaluación de activos.
- Revisa los servidores críticos para determinar su estado. Si están bien se procede a encenderlos, igualmente realiza con el almacenamiento SAN.

Realiza las siguientes tareas en el sitio alterno:

- Encender los servidores y arrancar el sistema.
- Comunicar el estado de los servidores, indicando si las máquinas están disponibles.

9.3.2.3 Ingeniero redes y comunicaciones. Este ingeniero estará a cargo de la red y transmisión de información y debe contar con el siguiente perfil:

- Ingeniero de sistemas, telemática y afines.
- Conocimientos certificados en Telecomunicaciones.
- Conocimientos certificados en tecnologías open source.
- Conocimientos certificados en switch y router.

Tiene las siguientes funciones:

- Administrara de la red de área local (switch de borde y core).
- Administrara los enlaces de conectividad.
- Administrara el Firewall de Navegación Internet.

Realiza las siguientes tareas en el sitio principal para verificar el estado de la red local y las telecomunicaciones:

- Revisar los switch de Borde y el switchcore.
- Verificar si hay red en las estaciones.
- Si hay puertos dañados se procede a reconfigurar los swiches o cargar el archivo de backup de la configuración.

- Si no hay salida a internet se debe verificar el estado de la fibra óptica y del canal redundante.
- gestionar y reportar el incidente ante el proveedor los cuales deben restablecer el servicio en un tiempo máximo de 4 horas.

Realizar lo siguiente en el sitio alterno para dar acceso a la red:

- Realiza cambios en las configuraciones de internet para desviar el trafico.

9.3.2.4 Ingeniero dba, administrador de las bases de datos. Este ingeniero estará a cargo de las bases datos de la entidad y debe contar con el siguiente perfil

- Ingeniero de sistemas, telemática y afines.
- Conocimientos certificados en administración de base de datos.
- Conocimientos certificados en almacenamiento.
- Conocimientos certificados en seguridad informática.

Tiene las siguientes funciones:

- Administración de las bases de datos en ORACLE, POSTGRES, MYSQL.

Realiza las siguientes tareas en el sitio principal:

Procede a restaurar las bases de datos con el procedimiento de restauración descrito en la Tabla 31.

- Restaurar la bd Oracle, ejecutando el import de la información.

- Después del import se debe revisar el log que no haya errores. Si hay errores se deben resolver y volver a ejecutar el paso anterior hasta que la operación sea ejecutada con éxito sin errores.
- Restaurar BD Sybase Reinicio del servidor.
- Ejecutar la importación de los datos de Sybase.

En el sitio alterno realizara lo siguiente:

- Gestionar la entrega del Backup. Debe realizar una solicitud de préstamo a la empresa custodia.
- Buscar el backup de las Bases de Datos y del File System que se entrega en custodia, cada semana y se encuentra fuera de la Entidad.
- Aplicar el procedimiento de restauración descrito en la tabla 29.
- Realiza las pruebas para verificar que la restauración quedo bien.

9.3.2.5 Ingeniero administrador de aplicativos. Este ingeniero estará a cargo de las aplicaciones y debe contar con el siguiente perfil:

- Ingeniero de sistemas, telemática y afines.
- Conocimientos certificados en arquitectura de software.
- Conocimientos certificados en tecnologías open source.
- Conocimientos certificados en análisis, diseño y desarrollo de soluciones informáticas.

Tiene las siguientes funciones:

Administrar las siguientes aplicaciones: expediente digital, nomina, direccionamiento estratégico.

Realiza las siguientes tareas en el sitio principal:

Para la aplicación expediente digital, realizar lo escrito en el numeral 9.3.1.3.
Para la aplicación nomina, realizar lo escrito en el numeral 9.3.1.5.
Para la aplicación de contratos, almacén e inventarios lo escrito en el numeral de 9.3.1.4.

En el sitio alterno, verifica el estado de las aplicaciones para esto:

- Presenta informe al Jefe de la Oficina del estado de las aplicaciones, las cuales previamente fueron instaladas, probadas y se mira el estado de las últimas actualizaciones para que queden iguales con lo que estaba en producción.
- Realizar la pruebas verticales y horizontales a los aplicativos.
- Verificar el estado y tiempo en que quedo la aplicación.

9.3.2.6 Tecnólogos de la mesa de ayuda. Los técnicos en computación estarán a cargo de los equipos de escritorio de los funcionarios de la entidad.

Tiene las siguientes funciones:

- Darán soporte a los equipos de escritorio y a los teléfonos IP.
- Gestionar para que se reestablezca la corriente eléctrica.
- Si el daño va a durar más de 2 días, debe informar al Jefe de Tecnologías de Información, quien tomara la decisión de pasar al sitio alterno.
- Gestiona y verifica el estado de la planta eléctrica del edificio.

9.4 CUARTA FASE: DIVULGACION PROCEDIMIENTOS

Una vez cumplido con el diseño del plan de contingencia para la Agencia ITRC, se procede a cumplir con la divulgación y la capacitación del personal del área de tecnología, en los procedimientos del plan de contingencia.

Además, se contempla un plan de promoción interna para dar conocer el plan de contingencia con que contara la Agencia ITRC en el cual se consideraran los siguientes aspectos:

- Se mostrará que para la implantación de dicho plan se cuenta con el apoyo de la Dirección General.
- Se mostrará también que se cuenta con temas específicos para los grupos objetivo que se definan para la capacitación.
- Se hará uso de los medios de promoción masivos.

9.4.1 Plan de Comunicación y divulgación. Para que la divulgación sea efectiva se van a presentar temas por grupos de funcionarios, los cuales se presentan a continuación:

- Director, Subdirectores, Jefes de oficina y Expertos Lideres de área.
- Funcionarios de la Oficina Asesora de Tecnologías de la información.
- Funcionarios que cumplen el rol de usuario final.

El temario que se presentara en la divulgación se muestra en resumen en la siguiente tabla:

Tabla 33. Temario divulgación plan de contingencia

TEMARIO	HORAS	FUNCIONARIOS
Sensibilización en seguridad de la información énfasis en planes de contingencia	4	Todos los funcionarios de la Agencia (140)
Implementación de los planes de contingencia	40	Funcionarios área tecnología (9)
Aplicación de buenas prácticas en la implementación de los planes de contingencia	16	Funcionarios área tecnología (9)

Fuente: El Autor.

De acuerdo con la anterior tabla en cada tema se tratará lo siguiente:

- Sensibilización en Seguridad de la información con énfasis en planes de contingencia. En este punto se pretende mostrar a todos los funcionarios de la agencia ITRC los diferentes escenarios cuando se presentan una contingencia, igualmente presentar los planes de contingencia con que cuenta la entidad.

- Implementación de los planes de contingencia. Presentar a los funcionarios del área de tecnologías de la Información el plan de contingencia diseñado. Este plan será implementado por área y por lo tanto es necesario saber lo que involucra a todo el grupo. Se presentará tal como está descrito en los objetivos de este proyecto.

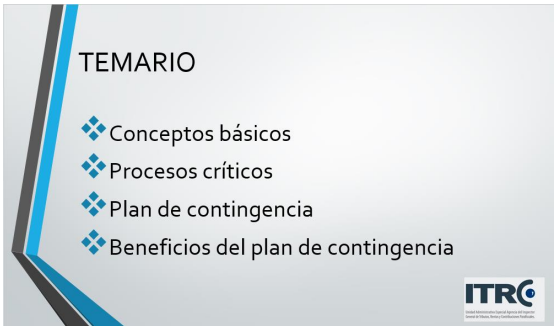
- Aplicación de buenas prácticas en la implementación de los planes de contingencia. Este tema es bien importante porque en él se explican las mejores prácticas en la implementación de los planes de contingencia con base en ITIL.

Para la Sensibilización en Seguridad de la información con énfasis en planes de contingencia a presentar a los funcionarios se realizara con la presentación que se muestra en el anexo E. Se presenta las dos primeras pantallas de esa presentación en las siguientes figuras.

Figura 8. Presentación a funcionarios

Fuente: El autor.

Figura 9. Temario



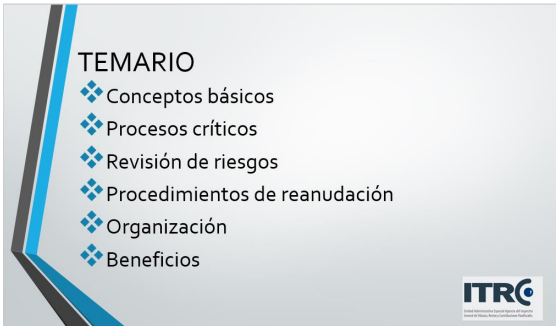
Fuente: El autor.

La presentación de los planes de contingencia a los funcionarios del área de tecnología será al comienzo igual a la anterior con adición al temario de la presentación que se muestra en el anexo F.

Figura 10. Presentación área de Tecnología

Fuente: El autor.

Figura 11. Temario presentación Tecnología



Fuente: El autor.

9.4.2 Medios de promoción masivos. Para la divulgación del plan de contingencia se identificación los siguientes recursos que pueden ser usados como medios de comunicación y divulgación durante las jornadas de sensibilización:

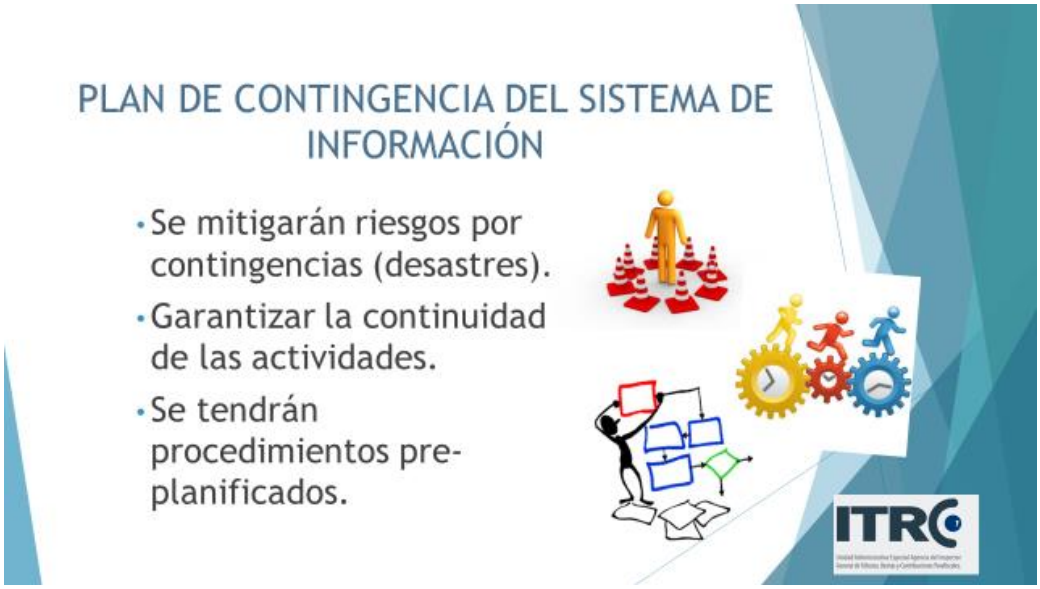
- Charlas
- Afiches dentro de las instalaciones
- Fondos de pantalla institucional, mostrando aspectos relacionados con el plan de contingencia. Estos mensajes en lo posible deben cambiarse cada 3 días, en los cuales se divulgue el plan de contingencia a ser puesto en marcha.
- Brochures

El modelo de los afiches serán los siguientes:

Figura 12. Modelo de afiche 1

Fuente: El autor

Figura 13. Modelo de afiche 2



Fuente: El autor.

Los fondos de pantalla serán los siguientes:

Figura 14. Modelo fondos de pantalla

Fuente: El Autor.

Figura 15. Modelo fondo de pantalla 2

Fuente: El Autor.

El modelo del Brochure será:

Figura 16. Modelo Brochure parte 1

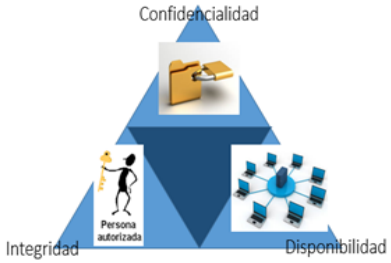
PLAN DE CONTIGENCIA DEL SISTEMA DE INFORMACIÓN

ITRC

Unidad Administrativa Especial Agencia del Inspector General de Tributos, Rentas y Contribuciones Parafiscales.

Conceptos basicos

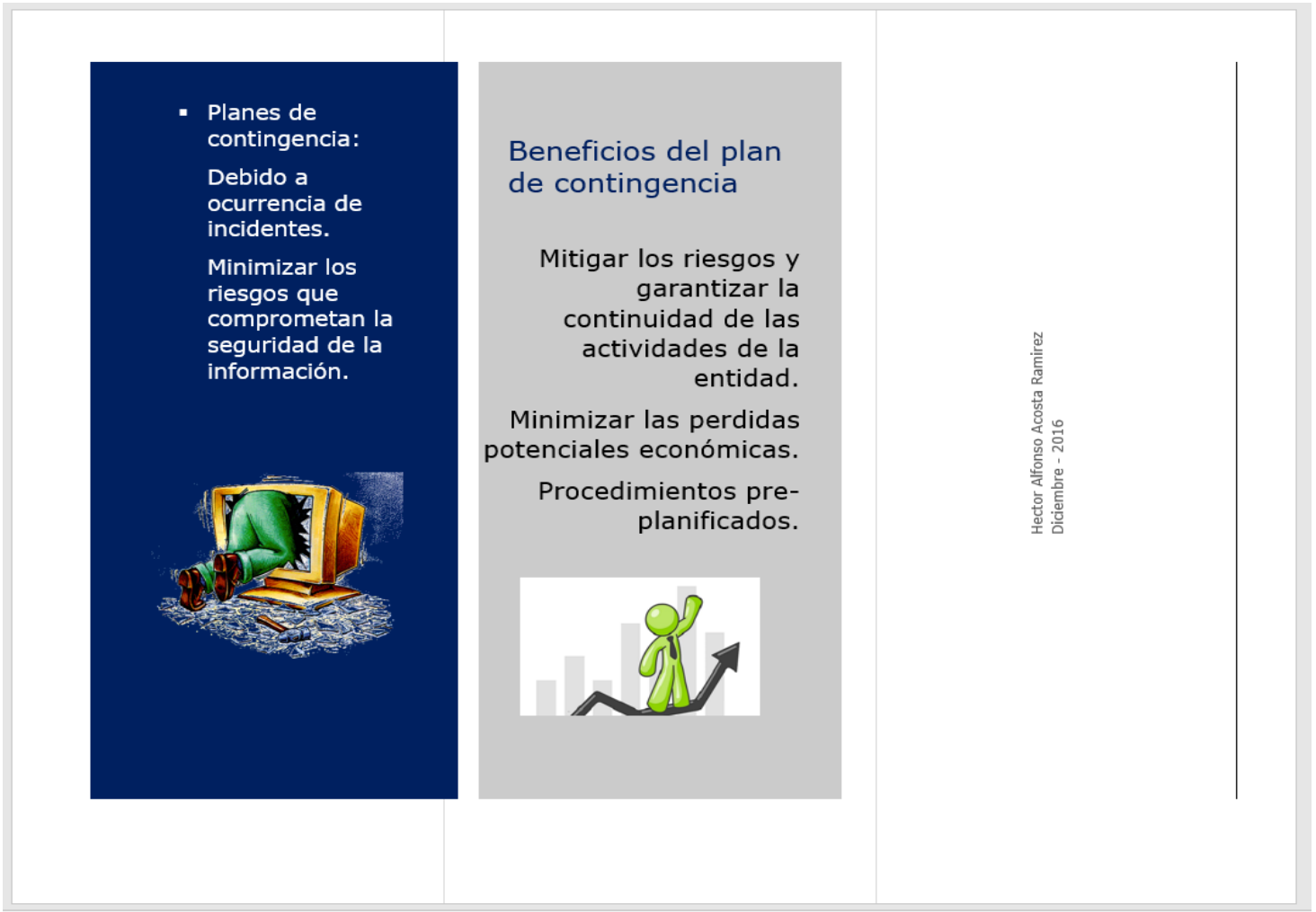
- La información es un bien que, como cualquier otro bien importante del negocio, tiene valor para la organización y consecuentemente necesita ser debidamente protegido.
- Seguridad de la Información, preservación de la confidencialidad, la integridad y la disponibilidad de la información.



- Activos informáticos, son todas las personas, instalaciones con equipos de Hardware, Software, componentes de comunicaciones de datos.
- Amenazas de los activos:
  - Incidentes.
  - Daños o perdidas de los activos informáticos.
- Riesgos informáticos:
  - Riesgos por atentados y/o amenazas.
  - Perdida de la información.

Fuente: El Autor.

Figura 17. Modelo Brochure parte 2



Fuente: El Autor.

10. RESULTADOS E IMPACTOS

En resumen, este plan de contingencia genera los siguientes beneficios:

- Con el diseño de este plan de contingencia se logrará mitigar los riesgos y garantizar la continuidad de las actividades de la entidad.

- Se realizaron rediseños en la red, almacenamiento, creación de máquinas virtuales réplicas de los servidores físicos.

- Con los procedimientos del plan de contingencia se puede saber que le corresponde hacer a cada integrante de la oficina de tecnología y que pasos debe seguir.

- Se puede saber los costos de no contar con el plan de contingencia.

- Minimizar las potenciales perdidas económicas.

- Mejorar la capacidad de recuperar las operaciones o actividades normales de entidad.

- Al proveer los procedimientos pre-planificados se minimiza el tiempo de toma de decisiones, como sucede en caso de desastre.

- Se elimina la confusión al saber cada persona que le toca hacer.

- Se reduce la probabilidad de error humano producto del estrés en esos casos de crisis.

- Se minimiza las potenciales responsabilidades legales.

11. CONCLUSIONES

En este proyecto, se realizó el diseño de un plan de contingencia para el sistema de información de la Agencia ITRC, se da cumplimiento al objetivo general y a los específicos, dentro de los cuales se realizó un análisis de riesgos, se definieron los procedimientos a realizar en caso de eventualidad, también se definió el grupo de personas que atenderán esas eventualidades. Igualmente se plantea la divulgación del plan de contingencia dentro de la Entidad.

En el análisis de riesgos siguiendo los pasos de la metodología 'MAGERIT' se encontró precisamente la necesidad de un plan de contingencia que le permita a la Entidad estar preparada en caso de siniestros que comprometan el normal funcionamiento del sistema de información a la vez que la red de información se requiere la aplicación de mayores controles.

En la definición de procedimientos se plantearon las actividades que se ejecutaran para recuperar todos los procesos en el sitio principal y también en el sitio alterno.

En la definición de la estructura organizacional para atender la contingencia, se definió el personal encargado de restablecer el sistema y las actividades que deben realizar.

Por último, se plantea la divulgación del plan de contingencia para todos los funcionarios de la Entidad.

Teniendo en cuenta lo anterior se concluye que lo expuesto en este proyecto es de gran ayuda para la Agencia ITRC porque permite tener el plan de contingencia con el cual se está preparado en caso de eventualidades.

BIBLIOGRAFIA

AUDISISTEMAS, “Riesgos informáticos”. Obtenido de http://audisistemas2009.galeon.com/productos2229079.html

BORGHELLO, C. (2000 - 2009). Segu.info Seguridad de la información. Obtenido de http://www.segu-info.com.ar/politicas/contingencia.htm

GASPAR, J, G. Planes de Contingencia la continuidad del Negocio en las organizaciones. Madrid: Díaz de Santos: D.L., 2004

ICONTEC. NTC-ISO-IEC 27001: 2013, Tecnología de la información- Técnicas de Seguridad- Sistemas de Gestión de Seguridad de la información- Requisitos. 2013

INTERNATIONAL ORGANIZATION FOR STANDARIZATION.ISO /IEC 27002:2013 Tecnología de la información-Técnicas de Seguridad- Código de conducta para los controles de seguridad de la información. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533

ISO 27000.ES. “El portal ISO 27001 En español”, Obtenido de http://www.iso27000.es/herramientas.html

ISO 27001 SECURITY. “Consejos de implantación y métrica de ISO/IEC 27001 Y 27002”
http://www.iso27000.es/download/ISO_27000_implementation_guidance_v1_Spanish.pdf

MALAGON, Chelo. MONSERRAT, Francisco. Recomendaciones de Seguridad. Definición de una Política de Seguridad. Obtenido: http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones.html

MAGERIT, Metodología de análisis y gestión de riesgos de los sistemas de información VI. Madrid, Ministerio de Administraciones Públicas, Manual 1997

PANDASECURITY. (2014). Panda Mediacenter. Obtenido de http://www.pandasecurity.com/mediacenter/panda-security/

UNAD. (s.f.). UNAD 3.2.1 Paso 1: Inventario de Activos. Obtenido de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/321_paso_1_inventario_de_activos.html

VILLALON HUERTA, A. Seguridad en Unix y redes, Versión 2.1, Free Software Foundation, Inc, 59 Temple Place, Suite 330, Boston, MA , 2002.

ANEXOS

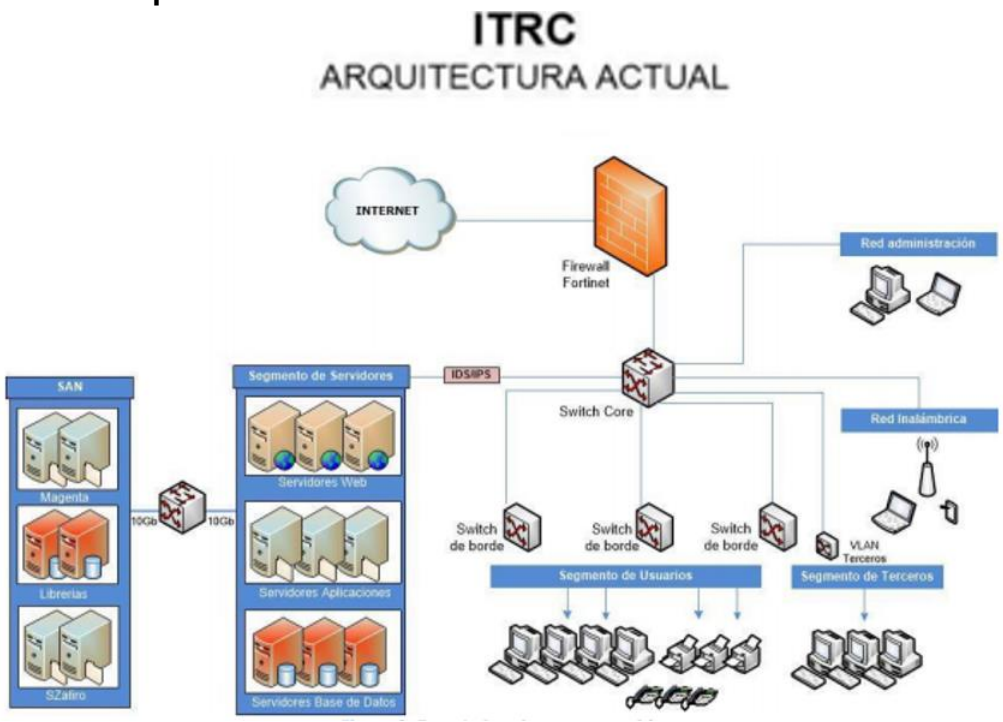
Anexo A. Organigrama de la Agencia ITRC

Figura 18. Organigrama de la Agencia ITRC

Fuente: Agencia ITRC

Anexo B. Arquitectura Informática

Figura 19. Arquitectura de la red



Fuente: Entidad Agencia ITRC.

Anexo C. Procesos críticos

Tabla 34. Procesos críticos

SISTEMA DE INFORMACION	AREA DUEÑA DE INFORMACION	TIEMPO MAX INTERRUPCION
Software automatización del proceso de gestión del expediente digital	Subdirección de Investigaciones Disciplinarias	4 horas
Bases de datos – Oracle. Sybase, SQL, Postgres	Todas las áreas	4 horas
CONTROL DE IMPRESIONES - Software de seguimiento y contabilidad de costos de impresión y control de los dispositivos de impresión	Oficina Tecnología de Información	1 día
Software para auditoria forense	Subdirección de Auditoria	1 día
Software – Análisis Investigativo	Subdirección de Investigaciones Disciplinarias	1 día
Correo Electrónico	Todas las áreas	1 día
internet	Todas las áreas	3 días
Microsoft Office	Todas las áreas	3 días
Software control de inventarios, almacenes, contratos, compras	Secretaria General	1 semana
NOMINA – GESTION DE PERSONAL - Software gestión del personal, y elaboración de la Nómina	Secretaria General - Talento Humano	3 semanas
Direccionamiento Estratégico - Software para la gestión del direccionamiento estratégico	Oficina Planeación	3 semanas

Fuente: Entidad Agencia ITRC.

Anexo D. Cuadro de evaluación de activos

Tabla 35. Cuadro evaluación de activos

ACTIVO	FUNCIONA	NO FUNCIONA	OBSERVACIONES
BLADE HP ProLiant BL460c Gen8			
BLADE HP ProLiant BL460c Gen8			
BLADE HP ProLiant BL460c Gen8			
BLADE HP ProLiant BL460c Gen8			
ENCLOUSER HP C7000			
HP MSL4048 Library HP HP Storages Works MSL 4048 Tape Library			
SERVIDOR HP Proliant DL360p Gen8			
SERVIDOR HP ProLiant DL380e Gen8			
SERVIDOR HP ProLiant DL380e Gen8			
ALMACENAMIENTO SAN HP 6300 EVA FC/ 1GB GBE DFF DE 22 Y 12 DISCOS SFR			
SOLUCION DE ALMACENAMIENTO SAN DELL			
DISCOS 480GB,SAS, 6GB, 2.5" SSD			
DISCOS 6TB SAS, 12GB, 3.5" 7K HHD			
DISCOS 600GB, SAS, 6GB, 2.5", 10K HDD			
DVR - CCTV SAMSUNG Samsung DVR SRD-1670DC			
FORTINET FORTINET D100			
CONTROLADORA HP MSM720			
SWITCH BORDE 6 HP MSM720			
SWITCH BORDE HP A5120			
SWITCH BORDE HP MSM720			
SWITCH CORE HP HP 7506			
SWITCH DE 8 PUERTOS HP N/A			
ACCES POINT HP MSM430			
ROUTER ETB HUAWEI N/A			
Aire Acondicionado APC APC In Row ACSC100 APC			
UPS Titan TITAN Titan EA9920 Cabinet			
Detección de Incendios			
control acceso			

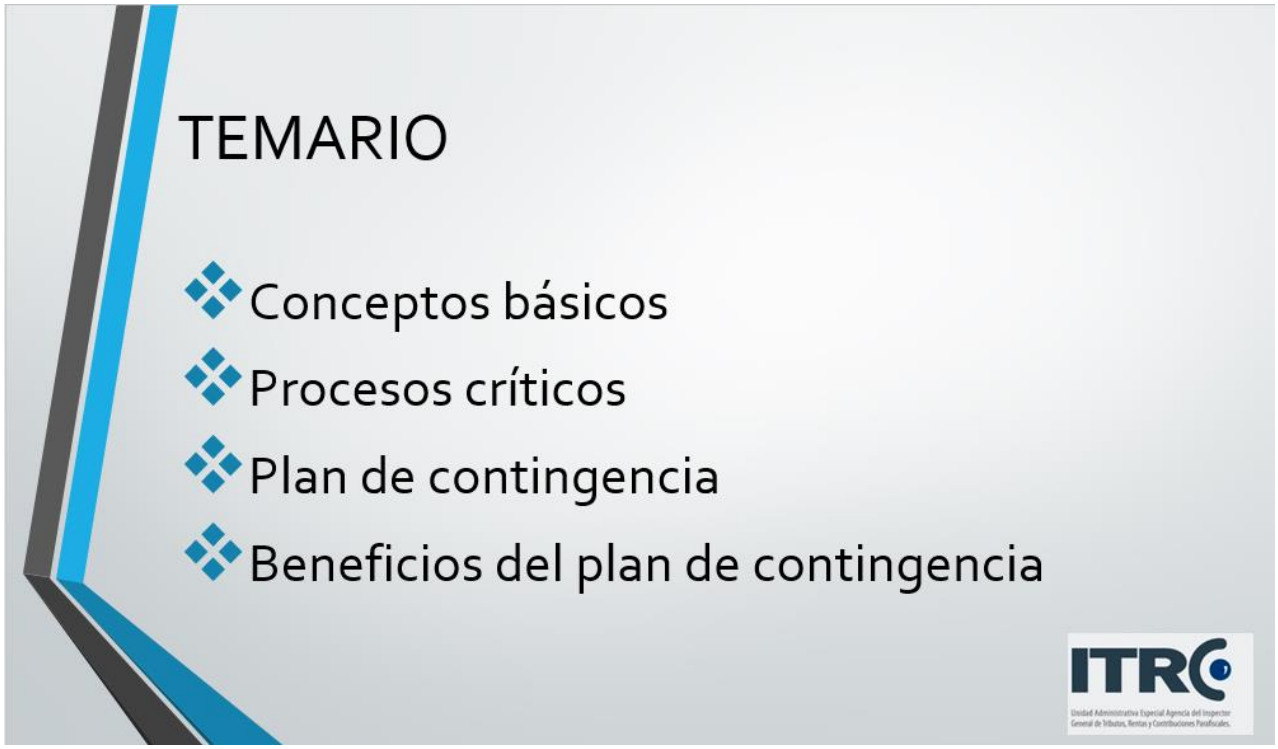
Fuente: Entidad Agencia ITRC**.**

Anexo E. Presentación a funcionarios

Figura 20. Detalle de la presentación a funcionarios

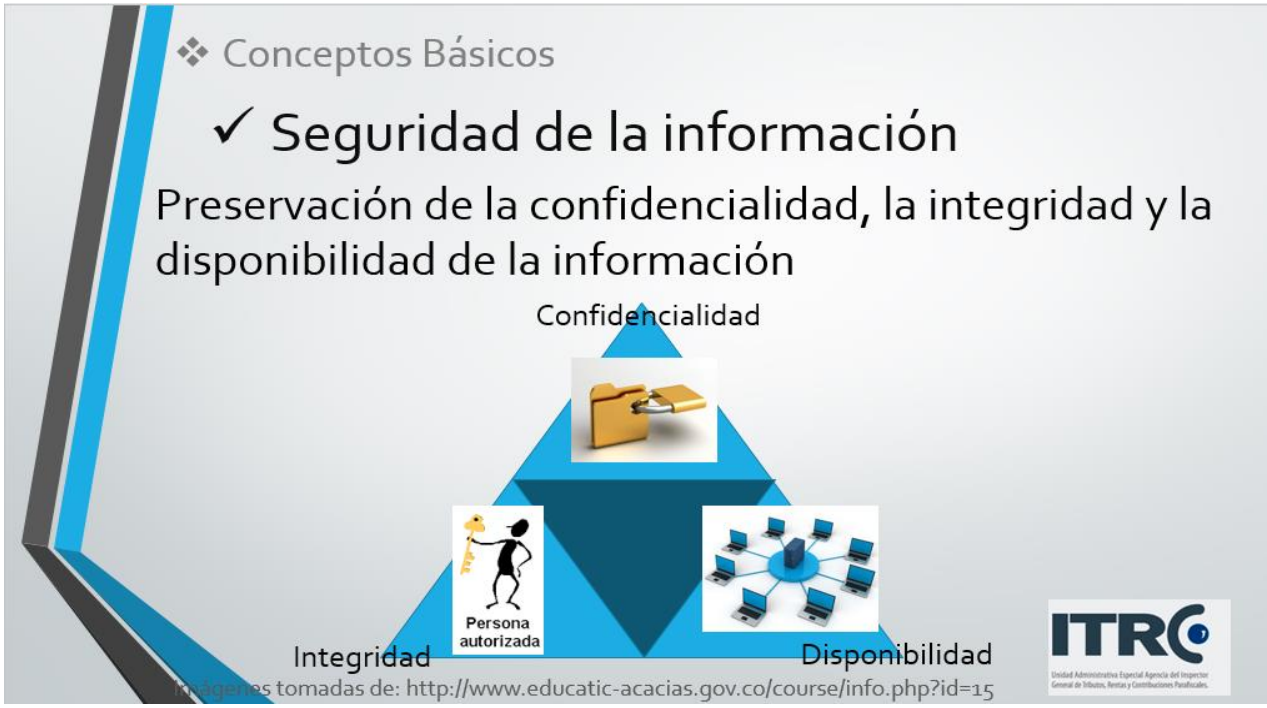
Fuente: El Autor**.**

Figura 21. Presentación a funcionarios temario



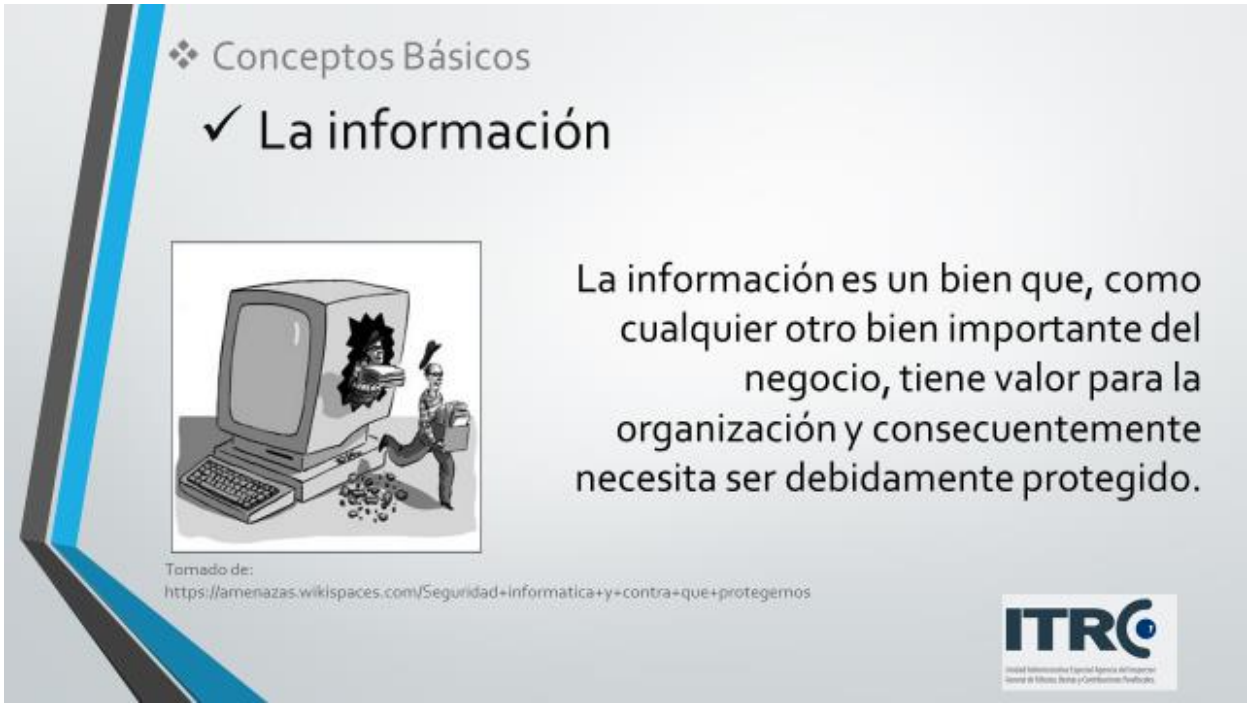
Fuente: El Autor**.**

Figura 22. Presentación funcionarios conceptos



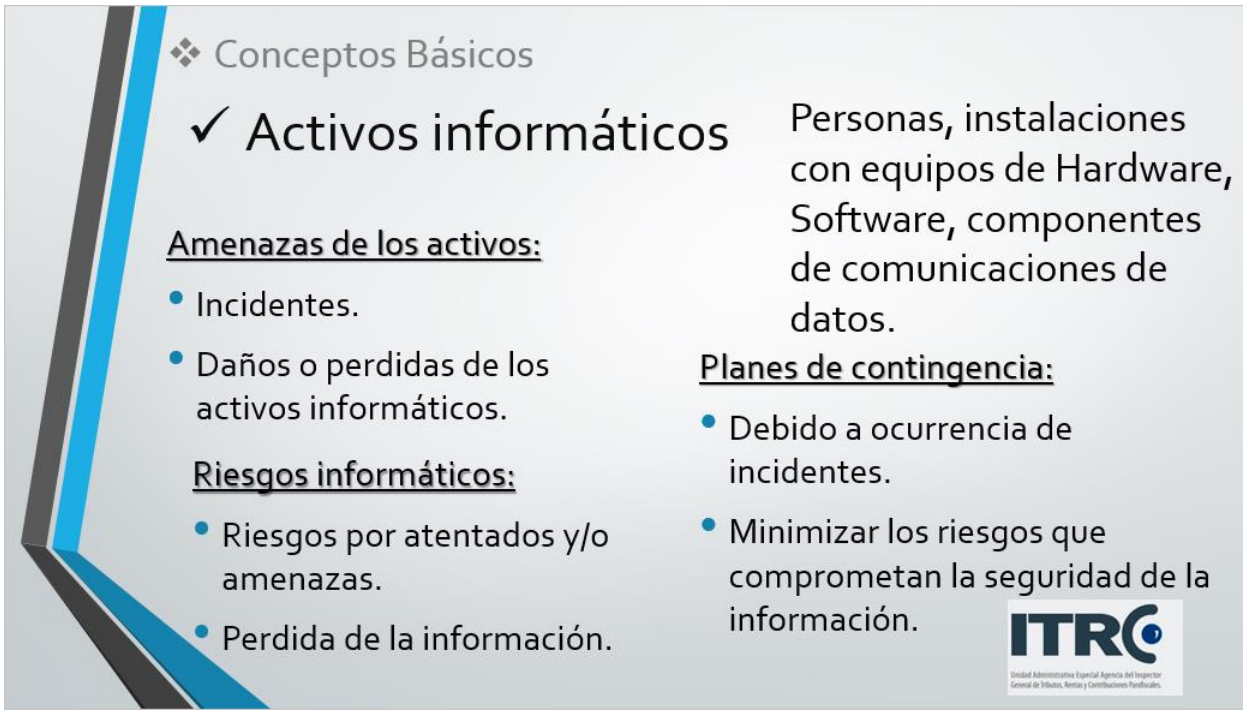
Fuente: El Autor**.**

Figura 23. Presentación funcionarios conceptos básicos



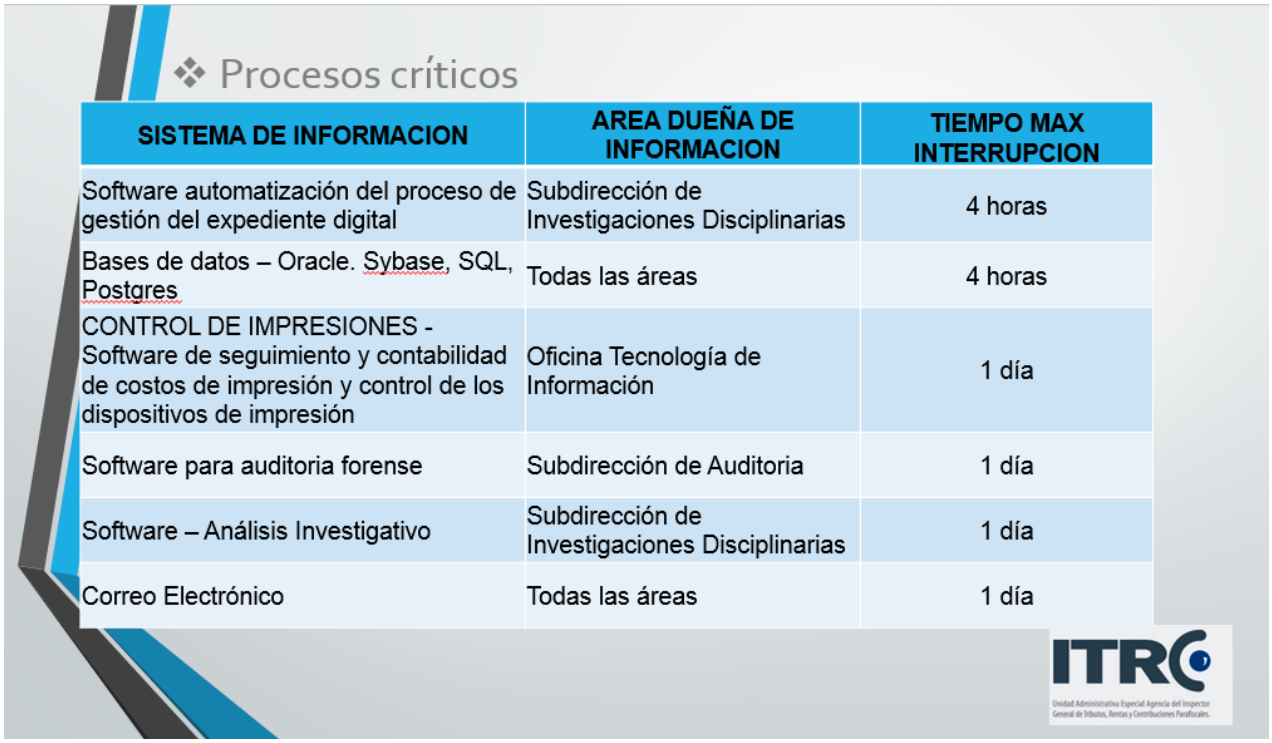
Fuente: El Autor**.**

Figura 24. Presentación funcionarios conceptos 2



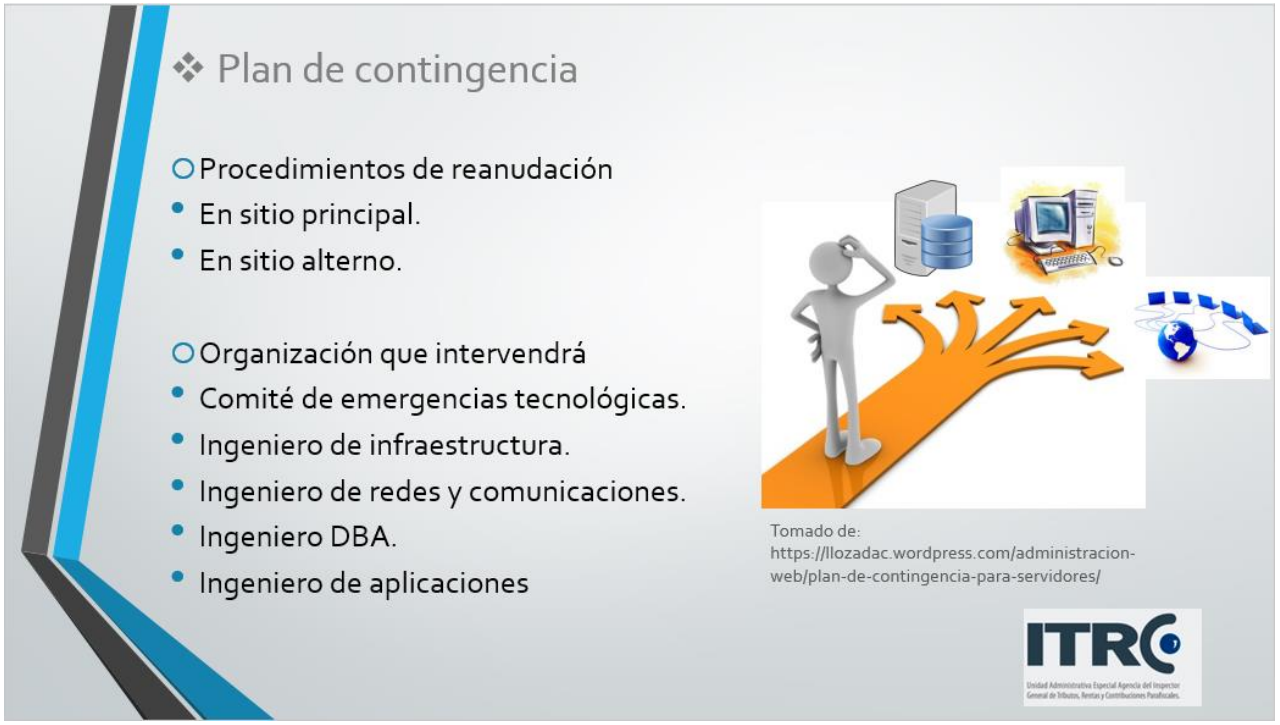
Fuente: El Autor**.**

Figura 25. Presentación funcionarios procesos críticos



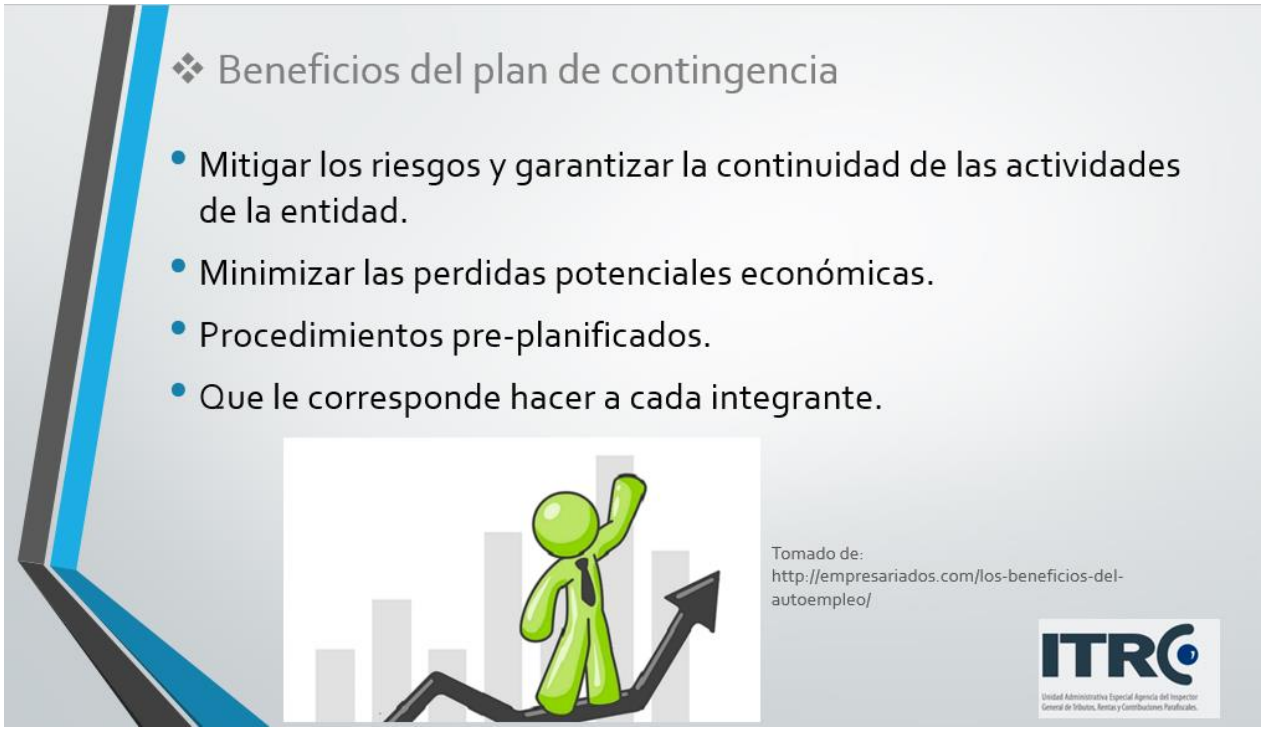
Fuente: El Autor**.**

Figura 26. Presentación funcionarios contingencia



Fuente: El Autor**.**

Figura 27. Presentación funcionarios plan contingencia beneficios



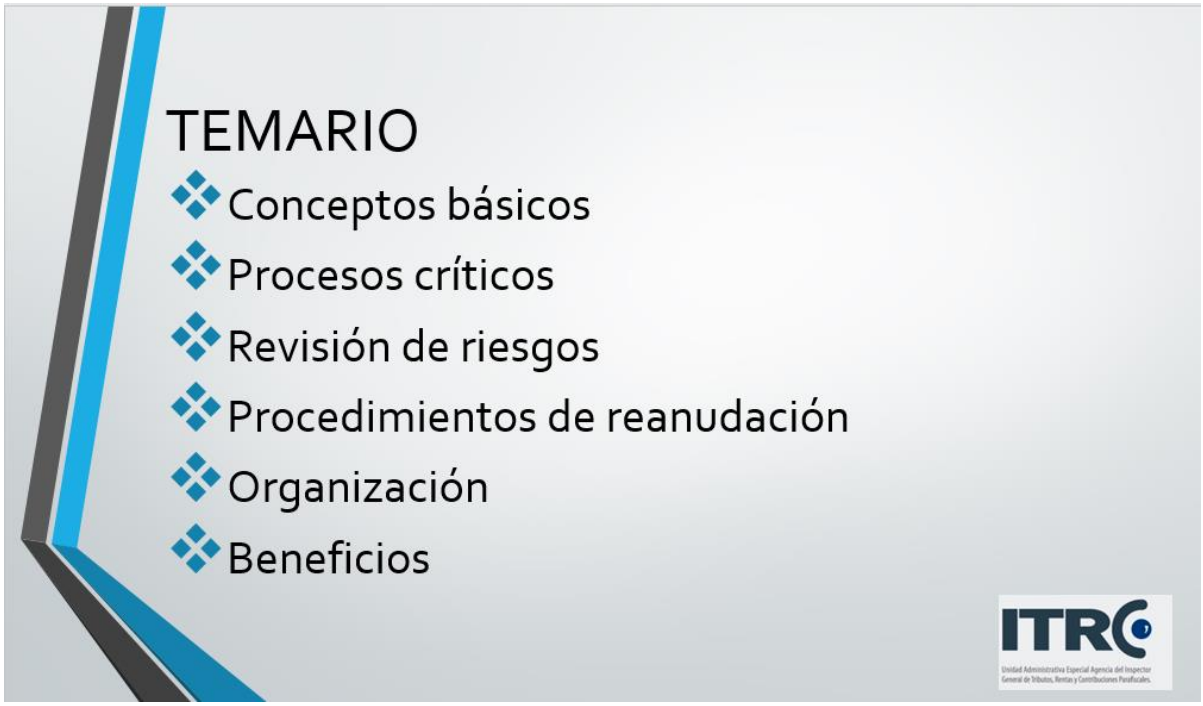
Fuente: El Autor**.**

Anexo F. Presentación a funcionarios del área de Tecnología

Figura 28. Presentación tecnología

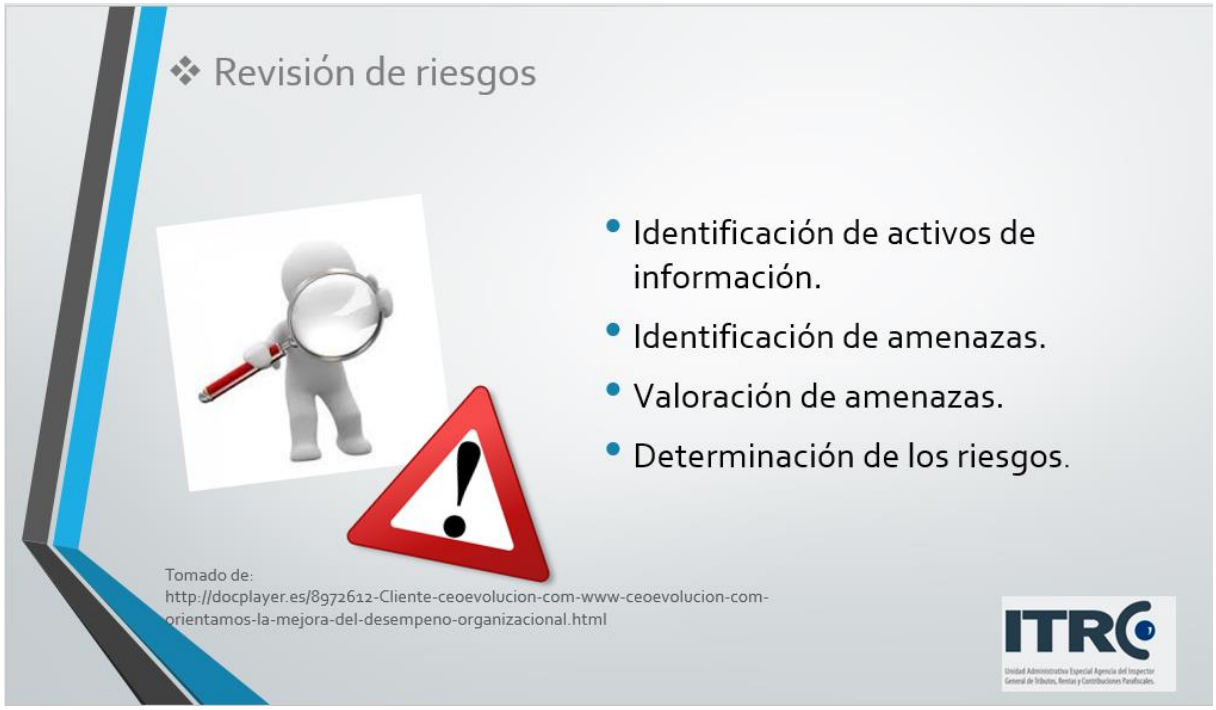
Fuente: El Autor**.**

Figura 29. Presentación Tecnología- temario



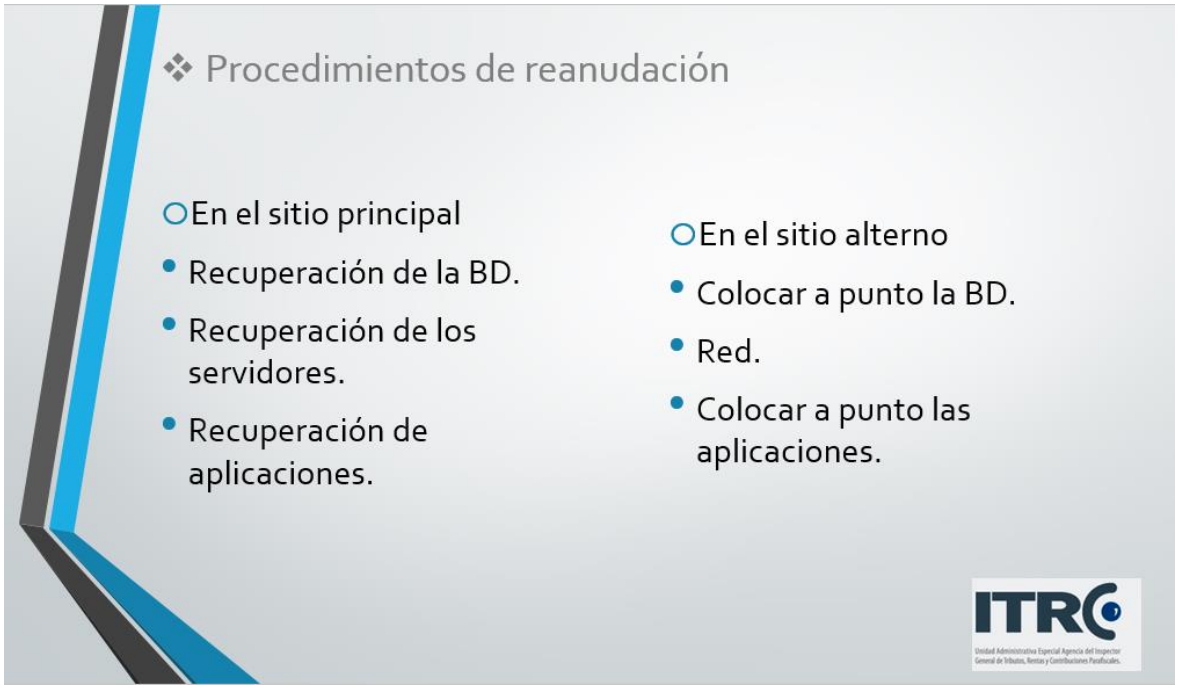
Fuente: El Autor**.**

Figura 30. Presentación tecnología riesgos



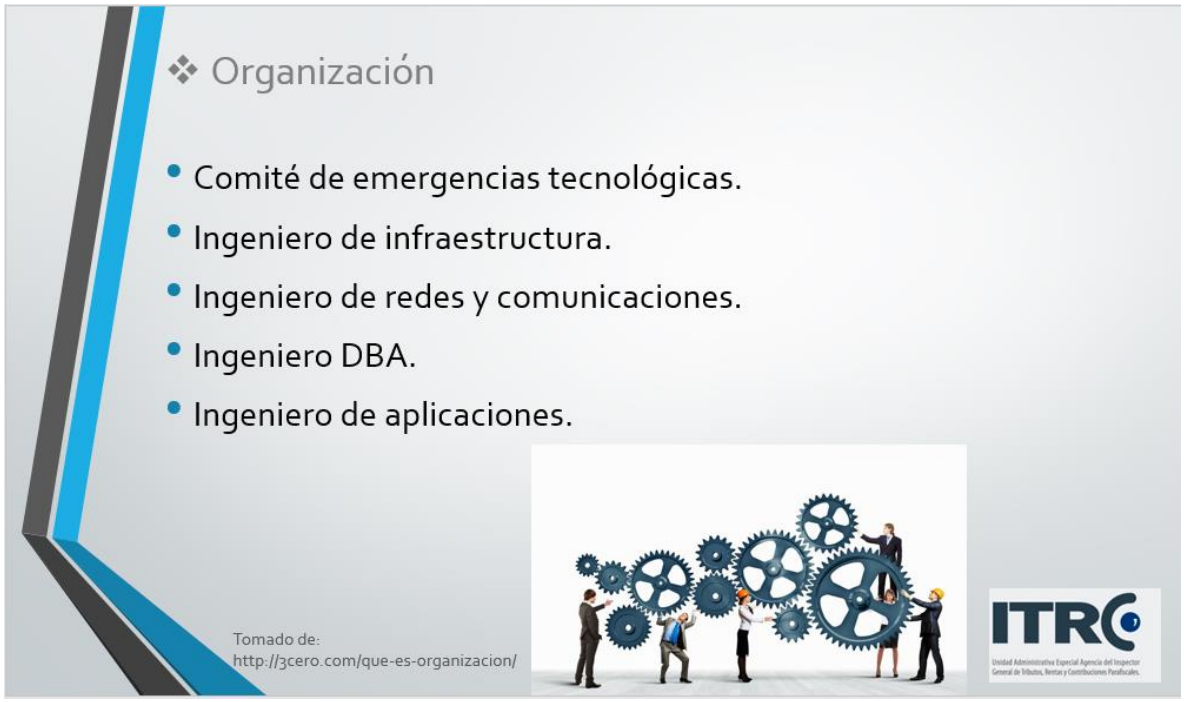
Fuente: El Autor**.**

Figura 31. Presentación tecnología procedimientos



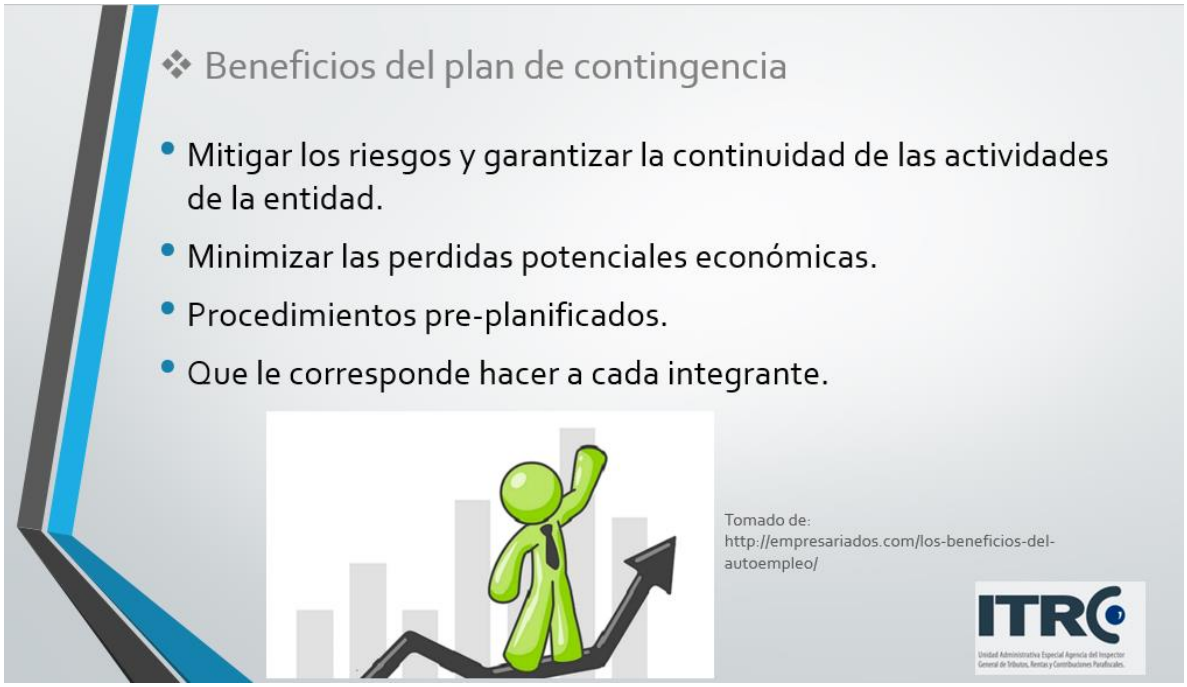
Fuente: El Autor**.**

Figura 32. Presentación tecnología organización



Fuente: El Autor**.**

Figura 33. Presentación tecnología- plan de contingencia



Fuente: El autor.

Anexo G. Resumen Analítico RAE

Título del Documento.	DISEÑO DE UN PLAN DE CONTINGENCIA DEL SISTEMA DE INFORMACIÓN PARA LA ENTIDAD ITRC
Autor	ACOSTA RAMIREZ, Hector Alfonso
Palabras Claves	Contingencia, riesgos, interrupciones, plan de contingencia.
Descripción Este proyecto se realiza para hacerle frente a la contingencia relacionada con la interrupción de actividades debida a la suspensión de los servicios informáticos, en donde se ve la necesidad de elaborar un plan de contingencias para la Agencia ITRC el cual comprende desde realizar un análisis de los riesgos a los cuales están expuestos los sistemas informáticos y aplicar medidas de seguridad para afrontar las diferentes contingencias.	
Fuentes Bibliográficas	BORGHELLO, C. (2000 - 2009). Segu.info Seguridad de la información. Obtenido de http://www.segu-info.com.ar/politicas/contingencia.htm GASPAR, J, G. Planes de Contingencia la continuidad del Negocio en las organizaciones. Madrid: Díaz de Santos: D.L., 2004 ICONTEC. NTC-ISO-IEC 27001:2013, Tecnología de la información- Técnicas de Seguridad- Sistemas de Gestión de Seguridad de la información- Requisitos. 2013 MALAGON, Chelo. MONSERRAT, Francisco. Recomendaciones de Seguridad. Definición de una Política de Seguridad. Obtenido: http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones.html MAGERIT, Metodología de análisis y gestión de riesgos de los sistemas de información VI. Madrid, Ministerio de Administraciones Publicas, Manual 1997
Contenido::	

a)Descripción del problema:

La Unidad Administrativa Especial Agencia del Inspector de Tributos, Rentas y Contribuciones (ITRC) es una entidad del gobierno creada para realizar detección del fraude en la DIAN, COLJUEGOS y UGPP. Para cumplir con sus objetivos realiza investigaciones, auditorías y recomendaciones que conllevan a evitar el fraude. Es por esto que la ITRC debe actuar de manera oportuna con acciones preventivas y correctivas frente al riesgo de fugas de dinero.
Los procesos implantados dependen totalmente de la plataforma tecnológica, los cuales hacen que la ITRC dependa 100% de los sistemas de información. Actualmente se tienen aplicaciones críticas, las cuales tienen que estar disponibles, junto con todo el sistema informático. Una aplicación crítica es el expediente digital para atender las investigaciones disciplinarias en la cual se lleva el control totalmente digital con plazos legales y con fechas que se deben cumplir. Lo cual hace que se tenga que prever que los servicios informáticos en la ITRC no dejen de funcionar y garantizar la continuidad del negocio.

b)Objetivo General.

Diseñar un Plan de contingencia para el sistema de información de la entidad Agencia ITRC ubicada en la ciudad de Bogotá, basado en las normas ISO/IEC 27001 e ISO/IEC 27002

c)Objetivos Específicos.

Identificar los riesgos a que están expuestos los sistemas y recursos informáticos de la entidad, los cuales se tendrán en cuenta en el diseño del plan de contingencia.

Establecer los procedimientos con los cuales se protegerá la información y garanticen el acceso a la información luego de siniestros de energía eléctrica, inundación, terremotos u otro tipo de fenómenos ambientales.

Definir la estructura organizacional para formar una administración paralela de contingencia y acción que se encargará de llevar a cabo las acciones en la emergencia con comunicaciones ya definidas.

Plantear la divulgación y el entrenamiento en los procedimientos del plan de contingencia para fomentar el conocimiento del plan. (buen manejo y aplicación del plan).

d)Resumen de lo desarrollado en el proyecto.

En este proyecto, se realizó el diseño de un plan de contingencia para el sistema

de información de la Agencia ITRC, se da cumplimiento al objetivo general y a los específicos, dentro de los cuales se realizó un análisis de riesgos, se definieron los procedimientos a realizar en caso de eventualidad, también se definió el grupo de personas que atenderán esas eventualidades. Igualmente se plantea la divulgación del plan de contingencia dentro de la Entidad.

En el análisis de riesgos siguiendo los pasos de la metodología 'Magerit' se encontró precisamente la necesidad de un plan de contingencia que le permita a la Entidad estar preparada en caso de siniestros que comprometan el normal funcionamiento del sistema de información a la vez que la red de información se requiere la aplicación de mayores controles.

En la definición de procedimientos se plantearon las actividades que se ejecutaran para recuperar todos los procesos en el sitio principal y también en el sitio alterno.

En la definición de la estructura organizacional para atender la contingencia se definió el personal encargado de restablecer el sistema y las actividades que debe realizar.

Por último, se plantea la divulgación del plan de contingencia para todos los funcionarios de la Entidad.

Metodología

El diseño metodológico para el desarrollo del proyecto es de tipo analítico-descriptivo porque los resultados se basarán en la observación y análisis descriptivo de lo encontrado. Además, se basa en lo propuesto en la norma internacional ISO/IEC 27001, para el diseño de un Sistema de Gestión de Seguridad de la Información

Para realizar el análisis de riesgos se utilizó la metodología "Magerit", con la cual se logró establecer, cuáles son los activos de información de la Agencia ITRC que están expuestos a un mayor riesgo y cuáles son los activos de información que producirían un gran impacto en caso dado que se materialicen las amenazas que lo puedan afectar.

Conclusiones

En este proyecto, se realizó el diseño de un plan de contingencia para el sistema de información de la Agencia ITRC, se da cumplimiento al objetivo general y a los específicos, dentro de los cuales se realizó un análisis de riesgos, se definieron los procedimientos a realizar en caso de eventualidad, también se definió el grupo

de personas que atenderán esas eventualidades. Igualmente se plantea la divulgación del plan de contingencia dentro de la Entidad.

En resumen, este plan de contingencia genera los siguientes beneficios:

- Con el diseño de este plan de contingencia se logrará mitigar los riesgos y garantizar la continuidad de las actividades de la entidad.
- Se realizaron rediseños en la red, almacenamiento, creación de máquinas virtuales réplicas de los servidores físicos
- Con los procedimientos del plan de contingencia se puede saber que le corresponde hacer a cada integrante de la oficina de tecnología y que pasos debe seguir.
- Se puede saber los costos de no contar con el plan de contingencia
- Minimizar las potenciales perdidas económicas
- Mejorar la capacidad de recuperar las operaciones o actividades normales de entidad
- Al proveer los procedimientos pre-planificados se minimiza el tiempo de toma de decisiones, como sucede en caso de desastre
- Se elimina la confusión al saber cada persona que le toca hacer
- Se reduce la probabilidad de error humano producto del estrés en esos casos de crisis

Recomendaciones.

Después de aceptado este diseño del plan de contingencia, se debe proceder a conformar un grupo para la implantación, a la vez se debe actualizar como mínimo cada 6 meses, incluyendo en el documento los activos que se adquieran y los que se dan de baja.