DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES INFORMÁTICOS PARA EL CENTRO DE DATOS DE LA GOBERNACIÓN DEL DEPARTAMENTO DEL CHOCÓ

ENIER MANUEL MAYO RIOS

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA INGENIERÍAS
FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
MEDELLÍN
2020

DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRES INFORMÁTICOS PARA EL CENTRO DE DATOS DE LA GOBERNACIÓN DEL DEPARTAMENTO DEL CHOCÓ

ENIER MANUEL MAYO RIOS

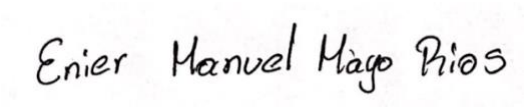
Trabajo de grado para optar al título de Maestría en Tecnología de Información y Comunicación

Asesor
DIEGO FERNANDO ESTARITA
Master en Ingeniería

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA INGENIERÍAS
FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
MEDELLÍN
2020

DECLARACIÓN ORIGINALIDAD

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad". Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR (ES) 

Medellín 07-09-2020

Dedicatoria

A DIOS, principalmente por darnos la vida, salud y por las oportunidades que nos brinda en todo momento.

A mi hija, por ser mi Fuente de inspiración y motivación para ser mejor persona en la sociedad.

A mi pareja, quien cada día me acompaña en los altibajos de la vida y apoyo incondicional.
A mis Padres, Hermanos y demás Familiares, quienes son mis mayores concederos para que cada día continúe en mis proyectos de vida.

A mi Departamento del Chocó, tierra de fuente de inspiración y motivación, que ha hecho que me encamine en una profesión con el propósito de llevar resultados para el desarrollo socioeconómico.

AGRADECIMIENTOS

Agradezco respetuosamente y principalmente a DIOS, ya que es quien me ha guiado, acompañado y brindado la fortaleza y el conocimiento necesario para culminar este proyecto de vida y esta carrera profesional.

A la Universidad Pontificia Bolivariana por permitir realizar mis estudios superiores en su Campus, a sus docentes y a mi tutor Diego Estarita, quienes se desempeñaron como personas actas y convenientes en este proceso, brindando sus conocimientos, experiencias, recomendaciones y fomentando en el desarrollo de este proyecto y mi carrera profesional.

A mis compañeros del posgrado, por brindarme ese ambiente amigable, momentos de superación, cordialidad y por la gran calidad humana y profesional dada en este ciclo de formación.

A mis Padres, Hermanos, mi Hija, mi Esposa y familiares, por contribuir en la motivación y confianza para desarrollar mis metas y objetivos propuestos.

Al proyecto Formación de alto nivel humano para un nuevo Chocó, quienes confiaron en mí, brindándome la oportunidad de ser parte de este programa para el proceso del cambio social en nuestra región.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Lista de anexos

GLOSARIO

Activo: La norma ISO 27001:2013 la define como: cualquier información o elemento relacionado con el tratamiento de la misma (persona, soportes, sistema tecnológico, hardware y software) que se relaciona con el entorno y sistemas funcionales que generen valor en la organización (ISO/IEC27001 2013).

Análisis de Riesgo: Para la ISO 27000, son los procesos para comprender la naturaleza del riesgo y determinar el nivel de riesgo (ISO27000 2014).

Backup: Se describe como la copia de seguridad de los archivos, bases de datos y/o aplicaciones, alojada en un componente magnético (generalmente en unidades de almacenamiento) para que pueda ser recuperada la información después que se presente un daño o borrado accidental (ISO/IEC27001 2013).

Centro de Dato (CPD): Conocido también como centro de procesamiento de datos, es donde se concentran los recursos necesarios para el procesamiento de la información automatizada de una organización.

Incidente: Evento o serie de eventos de seguridad de la información, no planeados, que afectan el correcto funcionamiento de los servicios (ISO/IEC27001 2013).

PHVA: Ciclo de Demning, Es una herramienta como diseñada para la mejora continua, la cual está basada en un ciclo de cuatro pasos, Planificar, Hacer, Verificar y Actuar. Diseñada por el Dr. Walter Shewhart en el año 1920 (ISO/IEC27001, 2013).

Amenaza: "Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización" (ISO/IEC27001 2013).

Riesgo: Probabilidad de que se materialice una amenaza en una brecha de seguridad, que genera un impacto negativo a un activo de información (ISO/IEC27001 2013).

Vulnerabilidad: La ISO 27001 describe que es la debilidad de un activo o de controles, los cuales pueden ser explotados por una o múltiples amenazas al tener conocimiento de ella (ISO/IEC27001 2013).

RESUMEN

Diseño del plan de recuperación de desastres informáticos en caso de ocurrencia de eventos de interrupción no previstos en los equipos críticos del Centro de Datos de la Gobernación del Departamento del Chocó, tomando las buenas prácticas del Modelos de Seguridad y Privacidad de la Información del MinTIC.

El plan de recuperación de desastres descrito en este documento es un apoyo que permitirá recuperar y proteger los procesos y sistemas tecnológicos que soportan las actividades esenciales, y hacer a esta área resilientes ante situaciones críticas.

***PALABRAS CLAVE*:** plan de recuperación de desastres; desastres tecnológicos; plan de continuidad; Backup; DRP.

ABSTRACT

Design of the computer disaster recovery plan in case of occurrence of interruption events not foreseen in the critical equipment of the Data Center of the Government of the Department of Chocó, taking the good practices of the Information Security and Privacy Models of the MinTIC.

The disaster recovery plan described in this document is a support that will allow the recovery and protection of the technological processes and systems that support the essential activities, and make this area resilient to critical situations.

***KEY WORDS*:** Disaster recovery plan; technological disasters; continuity plan; backup; DRP.

1 INTRODUCCIÓN

El siguiente trabajo de grado esta bajo la modalidad de reto empresarial, mediante el cual se busca mejorar los aspectos de fortalecimiento tecnológico en la Gobernación del Departamento del Chocó, en función a la continuidad de las operaciones del negocio y haciendo visibilizar lo imprescindible que son los equipos de seguridad de la información dentro de la organización.

Las tecnologías en conjunto con la información brindan un gran aporte al crecimiento de los servicios en las organizaciones, facilitando el acceso, disponibilidad y confiabilidad de los datos de forma estratégica y segura; por consiguiente, es importante que las organizaciones tengan un marco estratégico de seguridad mínimo en virtud a la continuidad del servicio y la mitigación de los riesgos. Es por esto que las organizaciones ven la necesidad de invertir en recursos económicos, humanos y tecnológicos para garantizar la continuidad de sus operaciones. (MinTIC, mintic.gov.co guía 10, 2017)

En relación con la descripción anterior, es imprescindible que las organizaciones cuenten con Planes de Continuidad de Negocio BCP al igual que Planes de Recuperación de Desastres - DRP, ya que estos planes son aliados estratégicos en las áreas de TI para mitigar el impacto negativo e indisponibilidad de los servicios; además, hacen a las organizaciones más resilientes en la continuidad de los servicios, puesto que estos incorporan personal calificado, procedimientos y procesos documentados que ayudan a recuperar los sistemas de TI afectados y garantizando la protección de datos, hardware y software crítico de las organizaciones (LOJÁN, 2017-02).

Así mismo, las empresas en Colombia deben acogerse de carácter urgente de estas estrategias DRP y aplicar los controles de seguridad mínimos para la protección y continuidad de sus servicios en situaciones críticas. (ARÉVALO, 2016, 14).

2 PLANTEAMIENTO DEL PROBLEMA

2.1 Problema

El Centro de Datos de la Gobernación del Departamento del Chocó GDC tiene la necesidad de invertir en la protección de su información y recursos tecnológicos para garantizar la disponibilidad continua de sus servicios, a través de esquemas o estándares de seguridad que permita mitigar las interrupciones de servicios no previstos por la falta de herramientas de seguridad e inexperiencia en la utilización de los recursos tecnológicos. La GDC a través de gobierno en línea busca crear y acoger los mecanismos de seguridad sugeridos y exigidos por MinTIC en el Modelo de Seguridad y Privacidad de la Información MSPI (MinTIC, mintic.gov.co 2017).

Sin embargo, el Grupo TIC de la GDC reconoce que los servicios del Centro de Datos de la GDC han presentado fallas en la disponibilidad del servicio por problemas técnicos tales como (1) errores en la configuración del software PCT, (2) lentitud en la red de comunicaciones, (3) problemas de instalación tecnológica, (4) variabilidad de voltaje en el flujo eléctrico, (5) manipulación de datos de información, (6) falta de mantenimiento en los recursos de TI e inversión tecnológica, (7) la ausencia de mecanismos efectivos y políticas para la protección de la información, entre otros. Un evento particular sucedió en el año 2017 periodo 1, donde se presentó una falla en el servicio de la base de datos que afectó el core de la organización y mantuvo sin acceso la comunicación con la base de datos de nómina de la GDC.

Por otra parte, en la GDC se identificó que los empleados realizan sus trabajos desde dispositivos personales (PC, email y dispositivos móviles), ya que a la fecha no se cuenta con mecanismos que regulen el acceso a la información, tales como controles de acceso a la red Network Access Control (NAC) ni políticas para el uso de correo corporativo; por tal razón, se presentan casos de fuga de información donde funcionarios que dejan de

laborar en la organización quedan con la información en sus equipos personales.

Hoy día, la GDC no cuenta con un Plan de Recuperación Ante Desastres Informáticos (DRP) que le permita recuperar información perdida o restablecer los servicios afectados; cabe resaltar que si cuenta con medidas de contingencia para respaldar el canal dedicado. Ante esta situación, es evidente el grado de exposición de riesgos que presenta la GDC en su centro de datos por no aplicar los lineamientos sugeridos y exigidos por el MinTIC, donde los entes públicos deben contar con medidas y políticas para salvaguardar los datos que las entidades crean, produzcan y almacenan en sus activos tecnológicos, ver (MinTIC, Políticas, Guía 2).

2.2 Justificación

Para la GDC es importante contar con una alta disponibilidad en sus servicios, dado que de ello depende el funcionamiento automatizado de sus actividades como: (1) procesos de contratación, (2) registros de nóminas, (3) pagos a funcionarios, (4) registros históricos de proyectos en ejecución y a futuros, (5) atención al ciudadano, (6) creación y publicación de políticas en función al cumplimiento de la población departamental, entre otros; por eso es importante mantener la información de forma accesible, integra y confidencial.

Dado la importancia que tiene para la GDC, el manejo adecuado de su información, uno de los pilares de los servicios del grupo TIC de la GDC es garantizar una alta disponibilidad en los servicios y mantener el respaldo de los activos de información que se consideran críticos, que le permitan garantizar el funcionamiento de las actividades esenciales; por lo tanto, es necesario que esta área cuente con los recursos necesarios para restaurar los sistemas de TI en el momento que se presenten eventos disruptivos. En vista al grado de exposición que se encuentran los activos de información y la falta de disponibilidad recurrente, se requiere diseñar un Plan de Recuperación de

Desastre informáticos para la GDC que mitigue los riesgos procedentes de los diferentes escenarios de interrupción y lograr el compromiso de la alta dirección para destinar recursos y priorizar esfuerzos en la estrategia de recuperación ante desastres o materialización de riesgos informáticos.

La ejecución de este proyecto es viable y alcanzable, puesto que el DRP es una estrategia que involucra personas calificadas, procesos, procedimientos y tecnología, a fin de reducir la ocurrencia de incidentes disruptivos. La estrategia hace parte de la restauración de los sistemas de TI afectados logrando que estas áreas sean resilientes antes, durante y después de la ocurrencia de un incidente, creando condiciones de continuidad en las operaciones corporativas (Arévalo, 2016). Este diseño se realiza en sinergia con el Grupo TIC de la GDC y personal calificado en seguridad informática, para identificar y establecer cada una de las funciones del despliegue de actividades para restaurar el servicio afectado en el menor tiempo posible.

Esta estrategia revisa los tiempos regulares, empleando técnicas como: el ciclo de Deming, espiral de mejora continua planificar, hacer, verificar y actuar (PHVA), (ver **Error! Reference source not found.**) donde se tienen en cuenta elementos y aspectos no incluidos desde la primera etapa, razón que se puede haber dado por el crecimiento de la organización. Posteriormente, se presentan las políticas de seguridad de la información, análisis y valoración de los riesgos, roles y responsabilidades, prevención, preparación y respuesta a los eventos críticos, dado que esta metodología postula que los planes estratégicos siempre están en estado de imperfección, citado de (LOJÁN, 2017-02).

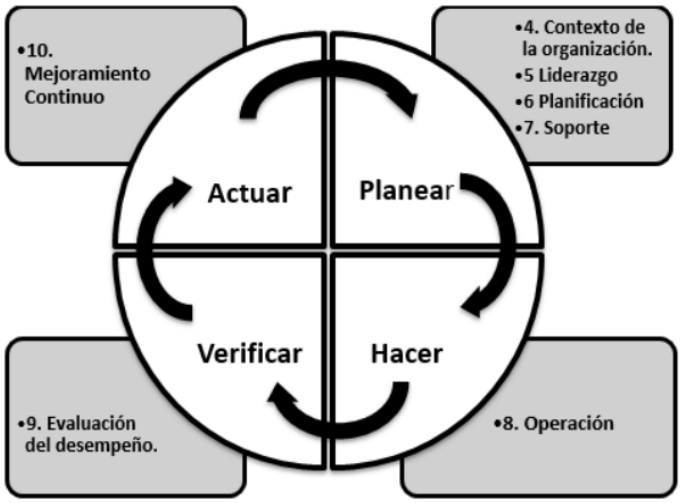


Figura 1: El ciclo Deming PHVA (LOJÁN 2017-02, 3).

En la Figura 1 del ciclo de Deming (Planear, Hacer, Verificar y Actuar), se ilustra el proceso de mejora continua para los planes estratégicos de continuidad de negocio tomado de la norma ISO 22301, el cual se puede emplear a los planes estratégicos de las organizaciones.

3 OBJETIVOS

3.1 Objetivo General

Diseñar el plan de recuperación de desastres Informáticos para el centro de datos de la GDC bajo el marco de referencia del MSPI del MinTIC.

3.2 Objetivos Específicos

1. Identificar los principales activos de TI de la GDC y los responsables.

2. Establecer políticas para el Grupo TIC y funcionarios públicos.

3. Definir los tiempos de recuperación en sinergia con el Grupo TIC para los recursos críticos de la GDC en función a la continuidad del negocio, tomando las buenas prácticas del BIA expuestos en el MSPI.

4. Elaborar el entregable acorde a las buenas prácticas propuestas por el MinTIC en el MSPI para contar con un Plan de Recuperación de Desastres en la GDC.

4 REFERENCIAL

4.1 Marco contextual

La GDC es un ente gubernamental y tiene como objetivo “cumplir con lo establecido por las autoridades gubernamentales, constitucionales, legales y reglamentarios sobre la necesidad de crear ocupaciones a los funcionarios que prestan servicio a la GDC y la responsabilidad de satisfacer las necesidades institucionales, y el complimiento de la misión y visión (Gobernación_Del_Chocó 2017).

La GDC ubicada a orillas del Rio Atrato, como se observa en **Error! Reference source not found.**, está conformada por un Despacho del Gobernador en turno, Jefatura de Gobierno, Jefatura de Gabinete y diez secretarías que son: Secretaria General, Secretaría de Salud, Secretaria de Hacienda, Secretaria del Interior, Secretaria de Cultura Recreación y Deporte, Secretaria de Integración Social, Secretaria de Educación, Secretaria de Desarrollo Económico y Recursos Naturales, Secretaria de Infraestructura Vivienda y Movilidad, y la Secretaria de Planeación y Desarrollo Étnico Territorial. El Grupo TIC depende en gran parte de la Secretaría de planeación para la ejecución de proyectos, dado que es la encargada de destinar los recursos económicos para llevar a cabo esta propuesta (Chocó 2017).

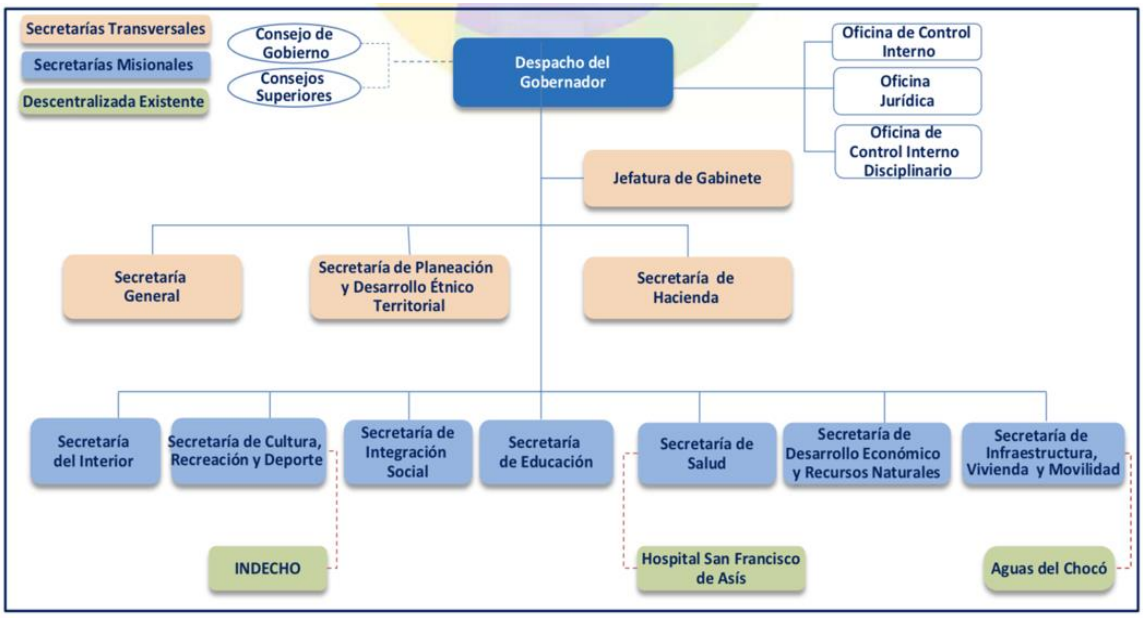


Figura 2: Organigrama de la GDC (Chocó 2017).

En lo que concierne a la dirección de sistemas (Grupo TIC) es liderada por el coordinador (asesor TIC), el cual debe contar con buena trayectoria profesional y excelente hoja de vida para el ejercicio de este cargo, debido que es de alta responsabilidad. Esta área tiene entre sus funciones: (1) revisión y desarrollo de todos los proyectos que se planteen en la dirección de sistemas (Grupo TIC), (2) velar por la gestión estratégica de las TIC, (3) administración de las necesidades del servicio tecnológico, (4) salvaguardar y proteger los activos de información que se creen, se tengan y se produzca en la GDC (Chocó, 2017).

4.2 Marco conceptual

El plan de recuperación de desastres será un aliado estratégico para la Gobernación del Departamento del Chocó, ya que permitirá a la alta dirección de TI ilustrar la importancia y la sensibilidad que tiene la información. El Grupo TIC deberá elaborar los manuales de seguridad para la GDC, los cuales deben estar soportados por políticas y procedimientos que permitan proteger los activos de información. Por eso es importante que para el desarrollo de este proyecto se tenga en cuenta las siguientes teorías y estándares

internacionales, las cuales proporcionan información útil para cumplir con la objetividad de la investigación (MinTIC, mintic.gov.co Guía 10, 2017).

4.2.1 Seguridad de la Información:

La norma ISO 27001 define la seguridad de la información como “la preservación de la confidencialidad, integridad y disponibilidad de la información” (ISO/IEC27001 2013).

Pilares de la seguridad de la información

Para poder conseguir el modo de brindar seguridad de la información en el gobierno de las TI de una organización, según (ISO/IEC27001 2013), es necesario garantizar una serie de servicios o funciones descritos a continuación:

- ✓ *Integridad:* Consisten en garantizar que el mensaje, información o archivo no ha sido modificado y garantizar su exactitud desde su creación y durante la transmisión a través de un canal de comunicación por la red de forma segura.

- ✓ *Confidencialidad:* Es garantizar que los datos, mensajes trasferidos o almacenados en un sistema informático solo pueden ser usados o leídos por su legítimo destinatario, garantizando su confidencialidad.

- ✓ *Disponibilidad:* Es de gran importancia contar con la disponibilidad del sistema informático para garantizar el cumplimiento de sus objetivos y que los que estén autorizados puedan acceder a la información disponible, y esto se logra mediante un sistema suficientemente robusto frente a amenazas.

- ✓ *Autenticación:* Es garantiza que la identidad del creador de un mensaje o archivo es legítima, demostrando la legitimidad de una información y garantizando que el trasmisor es quien dice ser.

4.2.2 Plan de Continuidad del Negocio (BCP)

Se refiere a un plan que contiene procesos y procedimientos logísticos que guían y orientan a las empresas como respaldar, responder, recuperar los activos de información críticos parcial o totalmente interrumpidos, dentro de un tiempo preestablecido después de una interrupción o desastre no deseado. El BCP demuestra cómo la entidad de servicio está preparada para afrontar futuros incidentes que ponen en peligro los recursos de información críticos y la consecución de los objetivos misionales del negocio (MinTIC, mintic.gov.co Guía 10 2017, 9).

Pilares de los planes de continuidad del negocio (BCP)

Holísticamente existen diferentes planes que en conjunto conforman los BCP, los cuales contienen guías, procesos y procedimientos para reaccionar ante situaciones que pongan en peligro las actividades económicas de una organización a través de recursos humanos y herramientas como:

- ✓ *Sistema de Gestión y Continuidad de Negocio*: Guía documentada que apalancan a las organizaciones a reaccionar, recuperar, reanudar y restaurar sus actividades operacionales a un nivel predefinido debido a las interrupciones. Esta guía normalmente incluye los recursos, servicios y actividades indispensables para garantizar la continuidad de los procesos críticos o que hacen parte de ellos (ICONTEC, NTC-ISO 22301:2012, 2012).

- ✓ *Plan de Recuperación de Desastre*: es una guía técnica enfocada a la recuperación de activos de información críticos de TI (Tecnologías de Información) para la continuidad de las operaciones tecnológicas, en caso de que exista una interrupción o parálisis temporal en las operaciones, y se debe elaborar políticas para planificar contingencias en los servicios tecnológicos mediante un grupo de procedimientos de respuestas ante emergencia relativos a la infraestructura tecnológica de información, siendo esta un subconjunto del BCP (LOJÁN, 2017-02).

- ✓ *Plan de contingencia:* Estrategias que ayudan a administrar las TIC y su correcta gestión en el buen funcionamiento, lo cual permite soportar los procesos tecnológicos gobernados por medio de procesos técnicos y humanos, lo cual garantiza la continuidad operativa de la organización; además, el plan debe ser revisado en tiempos regulares, dando lugar a replantear o agregar nuevos análisis de riesgos para ser revisado en caso de sufrir situaciones adversas (ACOSTA, 2017).

Con referencia de lo anterior, se alinean modelos o guías que se sustentan en diferentes estándares de seguridad para acoplarlos a las necesidades que se presentan en algunas entidades institucionales como las públicas.

4.2.3 Modelo de Seguridad y Privacidad de la Información (MSPI)

Diseñada por MinTIC para los entes gubernamentales en Colombia y empresas privadas, el cual se encuentra alineado con el marco de referencia de Arquitectura de TI con el fin de identificar el nivel de madurez en la implementación del MSPI, este modelo está acorde con las buenas prácticas de seguridad mediante las 21 guías anexas que ayudan a las entidades a cumplir lo exigido en el marco de la seguridad de la información (MinTIC 2017).

4.2.3.1 **Análisis del impacto en el negocio (BIA)**

Para el (MinTIC, mintic.gov.co Guía 11, 2017) se debe tener como propósito fundamental la identificación de roles y responsabilidades, los activos tecnológicos críticos, identificar qué áreas sufrirán pérdidas financieras y el cálculo de posibles impactos en el negocio en caso de interrupción, calculando el tiempo que la compañía puede tolerar una interrupción por medio de los componentes:

- ✓ *Punto de recuperación objetivo (RPO)*: Lapso de tiempo en que una organización u empresa soporta la pérdida de datos en situación crítica. Se determina identificando la posible pérdida máxima de información introducida desde el último respaldo (backup), hasta la caída del sistema (MinTIC, mintic.gov.co Guía 11 2017).

- ✓ *Tiempo de recuperación objetivo (RTO*): Tiempo trascurrido entre la afectación y la recuperación del servicio. Tiempo que se dispone para restaurar sistemas y recursos afectados a términos aceptables, sin afectar la continuidad del negocio (MinTIC, mintic.gov.co Guía 11 2017).

  Este proceso de recuperación solo se puede llevar a cabo para la restauración de servicio si se identifican los roles y responsabilidades de los implicados del área de las TIC para la segregación de actividades.

- ✓ *Matriz RACI o Matriz de Responsabilidades*: herramienta útil para la gestión de responsabilidades de cada actor en el proyecto con respecto a la selección de actividades. Se llama RACI por las letras iniciales de cada responsabilidad en ella y se usa para ilustrar las relaciones entre las actividades y los miembros del equipo del proyecto. El nombre proviene de las palabras Responsable, Aprueba, Consultado e Informado, cuatro letras codificadas en el tipo de relación con un proceso que tiene cada agente,

en caso de necesitarlo se pueden anexar las letras S y Q, “S” significa Soporte o “Q” de Quality quienes hacen revisión de la tarea.

R: Responsible / Responsable Quien se encarga de hacer las actividades o completar el trabajo del proyecto aprobado o calificado por A.

A: Accounteble / Persona a cargo. Persona responsable de que la tarea esta hecha, debe cerciorarse de que la tarea se realizó correctamente por R.

C: Consulted / Consultar. Persona a la que se le debe consultar datos o decisiones con respecto a la actividad o proceso que se determina, ya que son expertos en la materia.

I: Informed / Informar. Persona que se le debe informar de las decisiones que se toman, resultados que se producen, estado o avances del servicio.

S: Soporte. Pueden existir actores que den soporte al desarrollo de la tarea.

4.2.4 Ciclo Deming o PDCA

Herramienta de mejora continua, diseñada por Dr. Walter Shewhart en el año 1920 y presentado por Edwards Deming en 1950. Esta herramienta ayuda a realizar las actividades de una manera más organizada y eficaz, mediante su proceso de mejora continua para las planes o estrategias de seguridad, mediante su ciclo Planificar – Hacer – Verificar – Actuar; es una guía para la gestión de actividades y procesos (Bustamante, 2014).

Planificar: Se establecen los objetivos, procedimientos y procesos en función a la continuidad de las estrategias, para dar alcance a los resultados obtenidos y así lograr los requisitos establecidos por la alta dirección y definidos en las políticas de la entidad.

Hacer: Poner en marcha los procesos y procedimientos establecidos en la planificación para alcanzar los objetivos.

Verificar: Se realiza una revisión minuciosa, a los procesos, procedimientos conforme a lo prestablecidos en la fase de planificación, reportando los resultados logrados, en el que se obtienen hallazgos que permitan tomar acciones de mejora.

Actuar: Acciones, en función de promover la mejora de los procesos, implementando las acciones correctivas, y dando pasó a iniciar nuevamente el ciclo con un nuevo plan de mejora.

4.3 Marco legal

Resolución Numeral del 2014, por medio del cual se adoptan las políticas de seguridad de la información de la Gobernación del departamento del Chocó aprobada en el acta de reunión Nº 05 del 03 de julio de 2013, donde se señala que el departamento del Chocó protegerá la información generada, procesada o resguardada por los procesos estratégicos, misionales y de apoyo de la entidad, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros, garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información y la disponibilidad de sus procesos (Ver Anexo A).

DECRETO 1377 DE 2013: La protección de los datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012" (DECRETO1377 2013).

Ley estatutaria 1581 de 2012 "Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional" (Bogotá 2012).

Ley n° 1273 5 enero 2009 **“**por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" (Alcaldiabogota, LEY 1273 2009)

(MinTIC, Decreto 2693 de 2012) “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones” (Alcaldiabogota, DECRETO 2012).

Ley estatutaria 1266 de 20081 **“**por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones” (Alcaldiabogota. 2008).

4.4 Estado del arte

A finales de los años sesenta en Estados Unidos se escuchó por primera vez el término de Continuidad del Negocio, asociado a los procesos de administración y gobierno de las TIC de las organizaciones, en ese momento las organizaciones de forma tímida fueron tomando conciencia de lo significativo que representan uno de los activos más importante de cualquier entidad, como lo es la información, y como lo viene siendo hasta la actualidad. Fue allí cuando se dieron a la tarea de comenzar a definir normas y regulaciones enfocadas a garantizar la protección de sus activos más valiosos, orientada a garantizar la continuidad de sus servicios sin importar la situación crítica que se presente en una interrupción de servicios (Villamil 2012, 3).

La protección de la información junto a los procesos y sistemas que hacen uso de ella son activos de información importantes en las empresas. La confidencialidad, la integridad y la disponibilidad de información sensible pueden llegar a ser fundamentales para mantener los niveles de competitividad, rentabilidad y conformidad legal e imagen popular, dado que son necesarios para lograr los objetivos de las empresas y el aseguramiento de los beneficios económicos (ISO27000 2014, 3).

En relación a lo anterior, hoy día las entidades buscan tener sus sistemas tecnológicos alineados en el contexto de las tecnologías de información apalancando paralelamente sus operaciones con ella para hacer a la entidad más competitiva y eficiente en el mercado. Según (Arévalo, 2016, 14)., las organizaciones no se están alineando y ni fortaleciendo en materia de seguridad de la información para facilitar la restauración o recuperación de sus sistemas a la hora de enfrentar situaciones adversas que pueden ser causados por la inexperiencia, naturaleza de una mala configuración o por el poco alcance en la administración de los sistemas de TI.

Las NIST (National Institute of Standards and Technology), brindan un gran aporte de forma holística a los planes de continuidad del negocio para emplear buenas prácticas de seguridad en las empresas. La guía 800-34 Rev. 1 con título Planificación de Contingencia para los Sistemas de Información Federales, está ayudando a las organizaciones a comprender el propósito, el proceso y el formato del desarrollo de la aplicación de la planificación de contingencia de los sistemas de información a través de directrices practicas del mundo real.

La Figura 1, tomada de (Ferrer 2015), presenta una versión holística de los diferentes tipos de planes relacionados con la atención de desastres referenciado de la publicación realizada por (Swanson 2010, 12), adicionalmente presenta los sucesos y emergencias que son interrelacionados

con los planes de continuidad del negocio, dando un gran apoyo y complemento en cada uno de ellos para este trabajo.

Figura 1: Planes relacionados a los BCP tomado de (Ferrer 2015, 5).

Partiendo de este conjunto de estudios realizados por entidades organizacionales y publicaciones de guías para los planes de recuperación de desastre. Como presenta. “La mayoría de las organizaciones en los Estados Unidos emplean la norma ISO 22301:2012 como estrategia para los planes de continuidad del negocio en el manejo de las emergencias, ya que las áreas de TI son susceptibles a interrupciones no planeadas y deben contar con planes estratégicos de recuperación (Tellez 2015).

Para contrarrestar y reducir los riesgos que representa la materialización de los diferentes escenarios se recomienda definir una Metodología para la Continuidad del Negocio que incluya los pasos requeridos para diseñar e implementar un proceso de Gestión de la Continuidad del Negocio, BCM (Business Continuity Management), que se adecue a diversas organizaciones en Colombia. La Gestión de Continuidad del Negocio también llamado GCN, es una parte fundamental del Gobierno y de la gestión del riesgo que se debe considerar como un proceso permanente dentro de la organización; y debe poseer las fases del PHVA. En la Figura 2 se presenta un esquema que represente un modelo para administrar los riesgos.

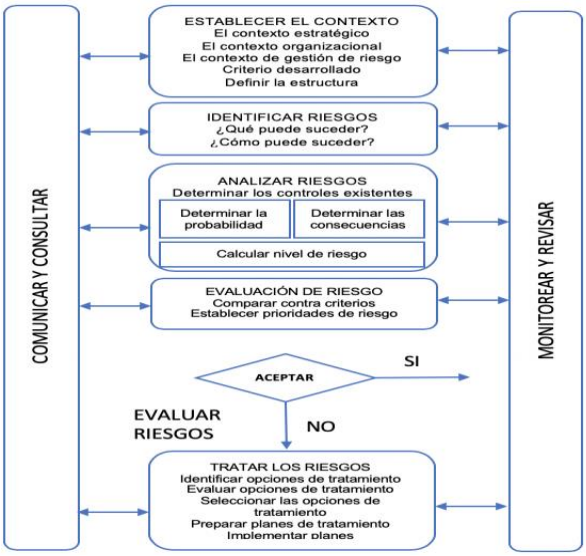


Figura 2: Gestión del Riesgo en seguridad de la información. (MinTIC, mintic.gov.co Guía 07 2017)

Sin embargo, en la publicación (LOJÁN, 2017-02)., titulado, Modelo de Evaluación de Gestión de Continuidad del Negocio basado en la norma ISO 22301:2012, el cual presenta el ciclo dinámico del PHVA y enfatiza en los nuevos conceptos agregados en la norma ISO 22301:2012. Dichos autores hacen énfasis en la importancia (1) del compromiso y entrega que debe tener la alta dirección en el aseguramiento de la compatibilidad del BCM con la dirección estratégica del negocio, (2) la integración de requerimientos de la norma en el plan de negocio y (3) la comunicación de la importancia de una eficaz gestión de la continuidad del negocio. También han adicionado requerimientos como los indicadores clave de desempeño KPI, modelos de madurez del BCM y contexto organizacional y liderazgo con el fin de simplificar y redefinir conceptos para su interpretación.

En este artículo, proponen un nuevo modelo de evaluación del Business Continuity Management System, (BCMS) para potenciar la capacidad de reacción y respuesta organizacional ante situaciones críticas del negocio de una forma holística en el que integran otros estándares y sistemas de diversos

propósitos de gestión, por el cual ayudan a medir la eficacia y la eficiencia de los BCPs mediante los métodos basados en la determinación y medición de Indicadores Claves de Desempeño (Key Performance Indicator) y basado en la Madurez de procesos.

Además, hacen énfasis en que los BCP no es igual al DRP, dado que estos facilitan la recuperación rápida de las operaciones críticas del negocio, incluyendo todas las partes o funciones de la organización; en cambio, el DRP viene siendo un subconjunto del BCP, siendo un grupo de procedimiento de respuestas de emergencia relativos a la infraestructura tecnológica de información de la organización (tomado de Lójan, 2017).

Revisando sobre estos temas anteriormente descritos de DRP y BCP. En Colombia; la alcaldía de **Santiago de Cali** diseñó el Plan de Continuidad del Negocio en los procesos administrativos de los recursos de TI para la oficina de informática y telemática de la alcaldía, el cual fue fundamentado en la norma ISO 22301 con el fin de lograr y mejorar la disponibilidad de sus servicios en las dependencias de la alcaldía, dedicadas a los cinco servicios críticos comprendidos en: (1) Canal de internet, (2) Intranet, (3) portal municipal, (4) sistema de gestión documental y (5) el correo institucional. También emplean el ciclo PHVA como estrategia de mejora continua (Tellez 2015). La metodología empleada por Tellez está comprendida en cuatro fases:

Fase de Identificación: fase inicial, en esta fase se identifica la composición de grupo de informática y telemática de la alcaldía de Cali en relación con el contexto organizacional, la cual conformada por cinco equipos de trabajos para las 17 dependencias en las que algunas trabajan de forma autónoma, estos equipos son: (1) Infraestructura de comunicación, (2) Centro de datos e infraestructura, (3) Sistema de información, (4) Apoyo aditivo, S.G.C y (5) Soporte técnico. También cuentan con el apoyo de seguridad informática

que es transversal a todos los cinco equipos. Dentro de los procesos identificados de la administración de la asesoría de informática y telemática hay tres subprocesos que son:

- ✓ Administración de sistema de información. (Proceso de apoyo) relacionado con los servicios de DHCP, DNS, Internet, Intranet, Portal municipal, Conectividad remota, Correo institucional, Gestión documental, Mensajería instantánea.

- ✓ Administración de infraestructura tecnológica. (Proceso de apoyo) contemplada en los servicios de mantenimiento del centro de datos y administración del soporte informático y tecnológico.

- ✓ Planeación estratégica del TIC. (Proceso estratégico) se contempla en los planes de mejora de las TIC, la estrategia y cumplimiento que se da a Gobierno en línea, y el sistema de gestión de seguridad de la información y de calidad.

Fase de Análisis: La información incluida aquí es una parte importante para el desarrollo de este trabajo porque muestra información indispensable para los planes de continuidad del negocio como lo es la Gestión del Riesgo, dado que el análisis que se realiza permite a la entidad conocer sus riesgos y como gestionarlos de forma adecuada mediante:

- ✓ La identificación de activos, se recomienda identificar los activos críticos que soportan los servicios esenciales.

- ✓ Contexto estratégico, identificar condiciones internas y del entorno, que pueden generar eventos que originen oportunidad o afecten negativamente el cumplimiento de la misión y objetivos de la asesoría.

- ✓ Identificación de riesgo, se realiza mediante la identificación de las causas que representan un impacto negativo en los objetivos institucionales con base en los factores internos y externos de la organización, y promoviendo la sensibilización de identificación de los riesgos a través de formato de identificación de riesgos, en el cual se puedan definir y presentar las posibles consecuencias que pueda representar en la organización.

- ✓ Análisis de riesgos, se realiza teniendo en cuenta dos aspectos fundamentales como lo son la probabilidad de recurrencia de eventos críticos y el impacto de esos eventos que causarían en la organización, bien sea económico o humano.

- ✓ Valoración de riesgo, inicialmente se tuvieron en cuenta todos los controles existentes para determinar que controles mitigan los riesgos ya descritos en fase de identificación, como producto de confrontar los resultados de la evaluación del riesgo con los controles identificados.

- ✓ Mapa de riesgos, se realiza como representación final de la probabilidad e impacto mediante el mapa de riesgos frente al proceso.

Fase de Diseño: Esta etapa es donde se definieron las estrategias para mitigar cada uno de los riesgos ya identificados en la fase anterior como medida de tratar o mitigar los riesgos. En esta actividad se tienen en cuenta las alternativas de respaldos o los tiempos de recuperación establecidos por el BIA, disponibilidad y costes de la organización.

Fase de Ejecución: Para llevar a cabo la ejecución del plan es necesario haber definido y establecido, el conocimiento de los procesos y servicios de la asesoría, valorando cuales son los procesos críticos para el funcionamiento de esta, la valoración de los riesgos que pueden afectar la administración de

la asesoría y que puede poner en marcha el plan de continuidad de negocio y la estrategia de continuidad más adecuada para el negocio.

Otro caso a evaluar se presenta en la región andina del Centro-Este de Colombia, con el fin de garantizar la continuidad de los servicios en los sistemas de información, bases de datos, y archivos de datos críticos y la recuperación de desastre en un tiempo prudente, la Gobernación de Boyacá crea las políticas de continuidad de servicios de TI y Recuperación de Desastres en la Gobernación de Boyacá (Boyacá, 2017), con el objetivo de definir las políticas de continuidad de servicios de TI y recuperación de desastres, apoyándose de los estándares ITIL V3, ISO 27001:2013 - punto A. 14.1.3 de la ISO 22301:2012, punto 8.4 y entre otros.

La Dirección de Sistemas debe ser responsable de crear y mantener actualizada las políticas de continuidad y recuperación, identificando estándares de seguridad, normas, directrices en la materia, documentarlas y publicarlas como lineamiento transversal para todos los procesos de la Gobernación de Boyacá. También es responsabilidad de Gestionar riesgos de TI y ejecutar el plan de continuidad y recuperación. Es responsable de mejorar las políticas al plan de continuidad y recuperación de desastres, conforme a la norma ISO 27001:2012, resaltando la responsabilidad y compromiso de la Alta Dirección en contar con el apoyo del plan o cambios vigentes que se realizan en el plan de continuidad y recuperación.

Las políticas creadas para la dirección de TI de Boyacá, se crearon con el fin de que los responsables del equipo de Gestión Tecnológicas de la Información creen y mantengan el plan de continuidad y recuperación de servicio actualizado y mostrar cada uno de los actores responsables o áreas responsables de los procesos. A continuación, se resaltan 9 de las 18 políticas creadas en Boyacá, las cuales se consideran fundamentales para este trabajo.

Políticas de continuidad

- ✓ Política 2. Se debe revisar y probar un plan de Continuidad de servicios de TI y recuperación de desastres, realizar mejoras de forma periódica o ante cambios significativos tales como procesos, tecnología o estructura organizativa; para lo cual deberán participar activamente en dicha revisión las distintas áreas de los procesos identificados como críticos.

- ✓ Política 3. La estrategia de continuidad de servicios de Tecnologías de Información y recuperación de la Gobernación de Boyacá deberá incluir el diseño e implementación de actividades de prevención y de recuperación que ofrezcan las garantías necesarias para el restablecimiento de las operaciones de la Entidad después de un desastre.

- ✓ Política 4. Los propietarios y administradores de la información en cada una de las dependencias de las Sectoriales deben identificar, clasificar y priorizar la información crítica de sus procesos.

- ✓ Política 6. Se debe establecer el tiempo aceptable para recuperar los datos que tiene la Entidad en caso de una interrupción o desastre (RPO), y garantizar una recuperación eficaz.

- ✓ Política 7. Se debe establecer el tiempo para retornar a las actividades normales después de la interrupción o desastre (RTO), y garantizar que los procesos críticos son recuperados dentro de los márgenes de tiempo requeridos en el Plan de Continuidad.

Políticas de recuperación de desastre

- ✓ Política 11. Se debe contar con una ubicación física desde la cual el plan de recuperación de desastres pueda ser ejecutado; es decir, un centro

de procesamiento alterno con capacidad para el respaldo de las operaciones críticas de la Entidad.

- ✓ Política 12. Se deberá establecer un protocolo de activación del plan y notificación oficial en la Gobernación de Boyacá ante la ocurrencia de un desastre. Una vez que la notificación se ha hecho, los responsables deberán informar al personal apropiado para realizar las actividades de verificación y evaluación.

- ✓ Política 14. Se debe realizar copia de seguridad (Backup) de las aplicaciones, bases de datos y bodegas de archivos alojados en servidores, con el propósito de salvaguardar la información. Estas se deben realizar periódicamente por profesionales de la Dirección de Sistemas de acuerdo a las indicaciones establecidas en el plan de continuidad y se deberán almacenar en un sitio alterno fuera del edificio donde se encuentra en centro de procesamiento principal.

- ✓ Política 16. Se deben almacenar las copias de seguridad de archivos relevantes de las dependencias, organizadas en archivos electrónicos de documentos, incluyendo sus metadatos a través de Tablas de Retención Documental (TRD) y preservar los documentos según se indique en la TRD de cada dependencia.

Para analizar también está el caso de la a Gobernación de Nariño, allí crean las Políticas de Seguridad y Privacidad de la Información de la Gobernación de Nariño en su versión 1.3-2014. Con el fin de salvaguardar la información, ya que la información es considerada como uno de los activos más importantes de la organización, haciendo necesaria la protección de esta frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, de gestión pública y legal. Estas políticas fueron creadas por el comité de seguridad de la información, en el que se comprometen a revisar

y actualizar anualmente contando con la aceptación del Gobernador del Departamento mediante la aprobación en un acto administrativo (Technologie 2015).

Las políticas de seguridad de la Gobernación de Nariño se resaltan aquí en este documento para tomarse como referencia para la creación de estas en la GDC, ya que es un documento de alto nivel que resalta el compromiso del Gobernador en turno con la seguridad de la información la cual es administrada por un comité de seguridad de la información. Las políticas aquí creadas resaltan el grado de importancia que juega el compromiso de la alta dirección y la cultura de las buenas prácticas en el uso de las herramientas y activos de la entidad. Se utiliza este trabajo realizado por la gobernación de Nariño para referenciar algunas políticas que podrían adaptarse para el centro de datos de la GDC como son:

- ✓ Identificación, clasificación y valoración de activos de información, cada área se responsabiliza de tener un inventario de los activos de información bajo la supervisión del Comité de Seguridad de la Información.

- ✓ Seguridad de la información en el Talento Humano, todos los funcionarios públicos de la Gobernación de Nariño deberán contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado y la oficina de Gestión Tecnológica debe mantener un directorio completo y actualizado de los perfiles creados.

- ✓ Responsabilidad de Usuarios Externos, este tipo de usuarios deberán tener un responsable y autorización por personal interno de la Gobernación de Nariño quien se responsabilice por toda la gestión realizada por el funcionario externo donde se incluye la supervisión del uso adecuado y acceso a la información y propender por la buena utilización de los recursos

tecnológicos. se debe aceptar por escrito los términos y condiciones del proceso a realizar y recursos a utilizar.

- ✓ Seguridad Física y del entorno, resaltan la importancia del acceso controlado y restringido al centro de datos y cuarto de comunicación principal. La oficina de gestión TIC se encargará de la elaboración de las normas, controles y registros de acceso a dichas áreas.

- ✓ Administración de las comunicaciones y operaciones, esta política es indispensable, dado que plasma el reporte y revisión de incidentes de seguridad. El personal vinculado deberá reportar con diligencia, eficiencia y responsabilidad las presuntas violaciones de seguridad a través de su jefe de dependencia a la oficina de gestión en TIC.

- ✓ Copias de Seguridad, toda información considerada de importancia para un proceso operativo o de misión crítica debe ser respaldada con copias de seguridad de acuerdo a los cronogramas definidos y publicados por el área encargada.

- ✓ Administración de redes de área local, en esta política resaltan la importancia de configurar las terminales de red, enrutadores, switches, firewall, sistemas de detección de intrusos, entre otros dispositivos de seguridad de red, los cuales deben ser documentados y respaldados por copia de seguridad. Dicha copia debe ser custodiada por la oficina de Gestión de TIC.

- ✓ Intercambios de información con Entidades Externas, la información solicitada o intercambio con terceros, debe ser autorizada y realizada utilizando de un medio valido que permita el registro de la solicitud, se identifique el remitente, el asunto y la fecha.

- ✓ Control de Acceso, se deben aplicar restricciones al acceso a información restringida y se recomienda el uso de sistemas automatizados de autenticación que manejen credenciales o firmas electrónicas.

Es importante destacar en esta investigación, qué para ofrecer seguridad de la información en la administración y gobierno de las TIC en las organizaciones, es indispensable conocer todos los activos de TI que se encuentren enlazados en la infraestructura de la organización, buscando tener un nivel alto de seguridad. Para el levantamiento de información de todos activos es recomendable usar herramientas automatizadas que permitan visibilizar todos los dispositivos (Appliances) que se encuentren interconectados en la infraestructura de la red de la organización.

5 METODOLOGÍA

El Plan de Recuperación de Desastres en la GDC está diseñado bajo las necesidades de la organización y las recomendaciones del Modelo de seguridad y Privacidad de la Información del MinTIC; por lo tanto, se toma como referencia las tres primeras fases de las buenas prácticas de la norma ISO 22301:2012; de manera que la GDC emplee políticas, técnicas y estrategias de seguridad de la información, con el fin de crear resiliencia en el área de infraestructura de TI apostando a la preservación de la confidencialidad, integridad y disponibilidad de los activos de información críticos, para prevenir interrupción de servicios que causen pérdidas financieras. Este trabajo se realizó en sinergia con el Grupo TIC de la GDC mediante las tres siguientes fases:

- ✓ Identificación: Análisis de Impacto del Negocio BIA, el cual se definen los pasos necesarios para identificar la magnitud del impacto de las interrupciones y las acciones que se deben tomar en los tiempos preestablecidos.

- ✓ Análisis: Gestión del Riesgo, referenciado en las buenas prácticas de la ISO 31000, el cual ayuda en el proceso de identificar y tratar los riesgos potenciales que se pueden materializar en la GDC y las recomendaciones necesarias para prevenir o mitigar los riesgos.

- ✓ Diseño: Selección de estrategias que se ajustan a las necesidades del centro de datos de la GDC con el fin de brindar un servicio continuo durante el ciclo de vida de las operaciones esenciales.

5.1 Etapa de Identificación

En esta etapa se realiza la descripción del contexto de los activos de TI, roles y responsabilidades, las áreas relacionadas con el centro de datos y se emplean las políticas para la gestión y administración del DRP:

- ✓ Política general del sistema del plan estratégico (DRP).
- ✓ Políticas de notificación de problemas e incidentes de TI.

Además, en esta fase se emplea la metodología del Análisis de Impacto del Negocio BIA, como elemento imprescindible en la identificación de los activos que representan un nivel de importancia en su funcionamiento, con la finalidad de estimar las consecuencias que traería en la organización y se emplea a través de los siguientes puntos:

- ✓ Criterios de interrupción.
- ✓ Identificación de procesos y activos críticos.
- ✓ Identificación de infraestructura.
- ✓ Identificación de recursos y servicios críticos.
- ✓ Disposición del RTO/RPO.
- ✓ Evaluación de impacto operacional.

5.2 Etapa de Análisis

En esta etapa se identifican los riesgos, la magnitud, y la posibilidad de ocurrencia de los riesgos en diferentes escenarios que puedan afectar los recursos lógicos o físicos de TI en representación al impacto operacional de las actividades esenciales de la GDC. A través de esta fase se define la

clasificación de los riesgos identificados para su tratamiento y a través de los resultados mitigar o reducir los mas potenciales. Esta fase se desarrolla mediante las siguientes actividades:

- ✓ Clasificación de escenarios de riesgos.
- ✓ Identificación de riesgos.
- ✓ Análisis de riesgos.
- ✓ Tratamiento del riesgo.
- ✓ Mapa de calor.

5.3 Etapa de diseño

En esta etapa se identificación y se definieron las alternativas en sinergia con el Grupo TIC de la GDC como medida de mitigación de los riesgos potenciales ya identificados en los recursos críticos del centro de datos de la GDC, con el fin de reducir o anular los riesgos a niveles no potenciales para garantizar la alta disponibilidad en los servicios esenciales y proteger los datos o activos de información mediante las siguientes actividades:

- ✓ Identificación de las alternativas.
- ✓ Evaluación de las alternativas.
- ✓ Estrategias de respaldo.
- ✓ Selección de respaldos.
- ✓ Definición de roles y responsabilidades.

6 RECURSOS UTILIZADOS

6.1 Recursos Humanos

- ✓ ING. HARLEM IBARGUEN MOSQUERA.
- ✓ ING. YOSIMAR PALACIO ROMAÑA.
- ✓ TEC. ANDRES DAVID MOSQUERA ASPRILLA.

6.2 Recursos Técnicos, Tecnológicos y Financieros.

En la **Error! Reference source not found.** Se describen los recursos requeridos para definición y ejecución de este proyecto, dichos recursos fueron asumidos en su totalidad por el autor del proyecto.

Recur	Cantidad	Nombre	Valor Unitario	Valor Total
Tecnológico	1	Computador Portátil	$ 2’000.000	$ 2’000.000
	1	Computador de Escritorio	$ 1’800.000	$ 1’800.000
	1	Impresora	$ 300.000	$ 300.000
Técnico	1	Fotocopias de Documentos	$ 20.000	$ 20.000
	4	Viajes, Transporte	$ 1’000.000	$ 1’000.000
	8	Teléfono, Cámara	$ 70.000	$ 70.000
	6	Otros Servicios	$ 150.000	$ 50.000
	6	Internet	$ 90.000	$ 90.000
TOTAL				$ 5’430.000

Tabla 1. Recursos utilizados.

7 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

El diseño del DRP en el centro de datos de la Gobernación del Departamento del Chocó se realizó en sinergia con el Grupo TIC y la participación de la Secretaría de Planeación para el levantamiento de la información de los activos y servicios críticos de la organización, con el fin de establecer un marco de procedimientos, prioridad en la recuperación y guía de acción que reduzca la toma de decisiones durante el proceso de recuperación descritas en la etapa de análisis, a fin de disminuir los tiempos de reacción ante las interrupciones. Con este proyecto se realizó el análisis para identificar los riesgos y evaluar la posibilidad de mitigar dichos riesgos.

7.1 Etapa de Identificación

En una de las sesiones con el Grupo TIC para la revisión del estado actual en la Gobernación del Departamento del Chocó con relación al contexto organizacional, se logró tener acceso a información en la cual se identificaron antecedentes y situaciones críticas, planes de contingencias, planes de respaldos, las tecnologías empleadas y los responsables de las diferentes funcionalidades pertenecientes al grupo TIC. En esta etapa se concluyó que:

- ✓ Se tenía poco alcance en los procedimientos que se establecieron para la atención de incidentes.

- ✓ Se contaba con poco recursos tecnológicos y procedimientos para contrarrestar los riesgos informáticos que generan fallas en la disponibilidad de servicios en el centro de datos.

- ✓ Se disponía de poca inversión en recursos tecnológico para el mejoramiento de sus procesos y servicios automatizados.

7.1.1 Contexto organizacional del grupo TIC en la GDC.

Los servicios de la GDC dependen en gran parte del área de TI para mantener sus aplicaciones y servicios en funcionamiento y de esta manera cumplir con las actividades esenciales de las diferentes dependencias. El Grupo TIC tiene la misión de proveer servicios a todas las áreas, dado que en el centro de datos se alojan aplicaciones (PCT, SOLREDES, ControlDoc y otros) en los equipos de comunicaciones, el control de seguridad (Firewall) y demás recursos que son imprescindibles y transversales en los diferentes procesos de las dependencias. La oficina de informática del centro de datos está conformada para dar servicio y soporte en:

- ✓ Infraestructura de comunicación.
- ✓ Centro de operación e información.
- ✓ Sistema de Informática.
- ✓ Gestión técnica.

Existen otros equipos de trabajos alternos, que brindan apoyo y son trasversales en las actividades que se solicitan bajo demanda, entre estos están: (1) soporte de PCT Enterprise sistema de gestión de la Base de Datos, (2) SOLREDES que brinda servicios técnicos a distancia para el software de nómina de empleados y pensionados (SIAN), (3) NEXCOM S.A. quienes a la fecha han brindado servicios de instalación, soporte de TI, capacitación del personal para el uso de los recursos de TI de la Gobernación.

Servicio y gestión del Grupo TIC, el grupo TIC es el responsable de los procesos, procedimientos de administración de las TIC en la GDC y de garantizar de forma continua la integridad, disponibilidad y confidencialidad de los datos que allí se produzcan, se almacenan y se transfieran dentro de la

entidad, y aprovechando el uso de las TIC para ofrecer un mejor servicio dentro de las funciones esenciales de la. (Ver anexo B) portafolio de servicio.

Dentro del proceso de administración de las TIC en la GDC existen tres subprocesos indispensables en su competencia:

- ✓ Sub proceso de administración de sistemas de información: Dentro de ésta se establece una de las funciones más importante del Grupo TIC, brindar gestión de servicios a la organización relacionados con: Internet, portal web, correo institucional, proveer gestión de aplicativos y documental PCT, SOLREDES, Firewall, SIAN, Todod y Winbox,

- ✓ Sub proceso de administración de la infraestructura tecnológica: Encargado de administrar y gestionar los servicios de mantenimiento, soporte tecnológico e informático, conectividad remota, DHCP, DNS, integración de nuevas tecnologías y equipos externos.

- ✓ Sub proceso de planeación y estrategias de las TIC: relacionado con los planes estratégicos de las TIC publicados o actualizados por MinTIC o por los estándares internacionales, para dar cumplimiento a la estrategia de gobierno en línea en su MSPI.

Adicionalmente, en esta etapa se analizó la situación actual que tiene el grupo TIC en relación con el contexto organizacional para el gobierno y gestión de los planes estratégicos, y se identificó poco alcance para administrar y restablecer los servicios que podrían verse afectados por eventos no planeados. Además, se evidencia poco mecanismo estratégico para garantizar la continuidad de los servicios en caso de un evento disruptivo

7.1.2 Propósito del DRP en el Grupo TIC de la GDC

Se pretende con el diseño del Plan de Recuperación Desastre identificar y definir el plan de tratamiento de los riesgos y amenazas presentes en la entidad que pueden ocasionar interrupciones no previstas a la operación, y así proveer un marco de trabajo para implementar mecanismos de resiliencia que permitan mejorar la capacidad de respuesta y restablecimiento del servicio ante fallos que afecten la disponibilidad de los servicios de T.I y por ende la operación de la GDC.

Para dar con el cumplimiento en la descripción anterior, se analiza y se definen en sinergia con el Grupo TIC los siguientes puntos para la administración del DRP:

- ✓ Equipo de gestión de seguridad.
- ✓ Políticas generales para la gestión del DRP.
- ✓ Política de comunicación de incidente.
- ✓ Análisis de Impacto del Negocio BIA.

7.1.3 **Roles y responsabilidades para la administración del DRP**

La seguridad de la información es indispensable en todas las divisiones y dependencias de la GDC, ya que la implementación de una estructura de gobierno de seguridad para las estrategias y necesidades en la organización y en los procesos de continuidad del negocio, es necesario el liderazgo y compromiso continuo de la alta dirección para contar con un ecosistema de seguridad acorde a las necesidades de la organización.

En sinergia con el Grupo TIC de la GDC se define que el esquema de perfiles apropiado para el gobierno y administración del DRP es emplear el

esquema equivalente a los Roles y Responsabilidades ilustrados en el documento GINF-G 010 de la Superintendencia de Sociedad en su versión 002 (ver figura 5). Dado que, la administración y gestión del DRP en la GDC dependerá de los perfiles definidos para el cumplimiento de las metas establecidas en esta estrategia; además, es necesario tener personal idóneo con amplia experiencia en seguridad informática y análisis de riesgos, ya que actualmente la GDC no cuenta con una estructura o jerarquía organizacional completa para suplir las necesidades administrativas de seguridad informática, es por esto que se necesita establecer el siguiente esquema ilustrado en la siguiente figura.

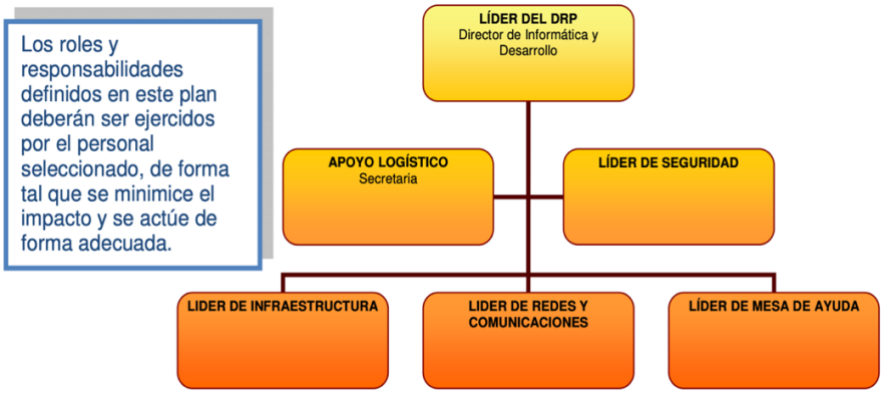


Figura 3: Equipo de Seguridad de la Información por: (Superintendecia_de_Sociedades 2011, 7)

A continuación, se describen cada una de las funciones propias del perfil para el rol en la administración y gestión del DRP:

Líder del DRP: Será quien se encarga de incorporar las estrategias de seguridad dentro del centro de datos de la GDC para que esta área cuente con los recursos requeridos en la distribución y administración de estrategias; por lo tanto, sus funciones son:

- ✓ Comunicar a las partes interesadas sobre el estado de las contingencias.

- ✓ Evaluar y activar el proceso de recuperación de desastres de acuerdo a los tiempos establecidos.

- ✓ Responder por el retorno a la normalidad de los servicios afectados.

Líder de Infraestructura: Es el encargado de responder por los recursos tecnológico en la administración de los equipos físicos y sus funciones son:

- ✓ Responder por el correcto funcionamiento del centro de datos.

- ✓ Validar que los reportes de los incidentes ingresan por la mesa de ayuda.

- ✓ Responder por la comunicación de las necesidades y cambios en la infraestructura.

- ✓ Responder por la ejecución de las pruebas y procedimientos de recuperación de incidentes de seguridad, entre estos están: acciones correctivas, comunicar y mantener informado al líder del DRP de los avances y de las actividades desarrolladas en el DRP.

Líder de Seguridad: es el responsable de ejecutar e implementar las siguientes funciones:

- ✓ Brindar acompañamiento y asesorar con su equipo de trabajo a toda la GDC en materia de seguridad informática para los procedimientos, procesos, pruebas, documentación, actualización y de identificar los recursos requeridos para la operación del DRP.

- ✓ Responder por las implementaciones de las estrategias de seguridad de la información que estén aprobadas por el Líder del DRP.

- ✓ Responder por la gestión de sitios alternos para las réplicas del centro de datos de la GDC para garantizar una alta disponibilidad de los servicios.

- ✓ Coordinar el desplazamiento al sitio alterno, de manera segura, de los equipos necesarios para la redundancia del centro de datos, a su vez debe mantener informado al Líder del DRP de las actividades realizadas.

Apoyo logístico: estos deben participar en la ejecución de las pruebas y apoyar en los inconvenientes, actividades administrativas y logística ante situaciones de contingencia, algunas de sus funciones son:

- ✓ Informar a los proveedores los inconvenientes presentados relacionados que los productos que ellos suministran a la organización.

- ✓ Reportar los inconvenientes y oportunidades de mejora del DRP desde la mesa de ayuda o visitas técnicas.

Para contar con una visión de administración y gestión efectiva de la seguridad de la información y las responsabilidades de la gerencia de ciberseguridad en la GDC, en el anexo C se ilustra el esquema completo de la gerencia de ciberseguridad que se recomienda tener en las organizaciones para un mejor gobierno y gestión de la seguridad de la información. Obtenida del Libro de Preparación a la Certificación CISM Certified Information Security Manager (ver anexo C).

7.1.4 Políticas generales para la gestión del DRP.

Las políticas generales definidas en sinergia con el Grupo TIC para la administración del DRP se crean para el personal a cargo de los recursos de las TIC de la GDC y para quienes hagan uso de la tecnología dentro de la infraestructura de la red de la GDC, en el que deberán estar conscientes de lo

expresado en ella. Estas políticas se definen con el fin de establecer un marco de trabajo apropiado que les permita la resiliencia necesaria en los sistemas tecnológicos parcial o totalmente afectados; además, contar con la capacidad de respuesta, recuperación y reanudación de los servicios a términos aceptables.

Políticas para el Grupo TIC.

El Líder del DRP es responsable de supervisar y coordinar las actividades de recuperación o activación del plan, también es el responsable de mantener, actualizar y aplicar las actividades descritas en el DRP. Para el cumplimiento del mismo se incluyen las siguientes políticas:

- ✓ Política 1. Se debe contar y revisar de manera periódica la estrategia del DRP en función a la continuidad del plan de recuperación de desastres en la gestión del Grupo TIC para el centro de datos de la GDC dado que el plan estará sujeto a simulaciones y cambios.

- ✓ Política 2. El Grupo TIC de la GDC identifica y documenta los procesos y servicios críticos del centro de datos que permiten soportan la continuidad de sus servicios y las actividades económicas.

- ✓ Política 3. El grupo TIC implementa mecanismos de redundancia y tolerancia a fallas en los servicios críticos de la GDC.

- ✓ Política 4. El coordinador del Grupo TIC es el encargado de la comunicación y presentación de resultados en materia de planes estratégicos para garantizar la continuidad de los servicios de información que soportan la GDC frente una situación crítica.

Política de comunicación de incidentes

Este grupo de políticas van dirigidas a los funcionarios de la GDC, con el objetivo de identificar los diferentes escenarios que pueden presentarse e impactar en los recursos de TI, con dichas políticas se facilitará la identificación de incidentes de seguridad que se pueden encontrar presentes en los activos de información. Es responsabilidad de todos los funcionarios de las dependencias reportar los incidentes de seguridad y aquellos problemas relacionados con la seguridad de los sistemas de TI.

- ✓ Política 5. Cualquier funcionario de la GDC puede y debe notificar de manera ágil los incidentes o hallazgos de situaciones que puedan poner en peligro la integridad o activo de información, mediante los canales de comunicación que allí se dispongan, como: un Email, una llamada telefónica, mediante el chat corporativo u otro medio disponible.

- ✓ Política 6. Los funcionarios públicos de la GDC deben participar en los programas de sensibilización de seguridad de la información, creados y formalizados por parte del Grupo TIC en materia de prevención.

- ✓ Política 7. Se debe delegar en las dependencias que lo requieran un líder de TI para apoyar los procesos de gestión de TI requeridos por el Grupo TIC de la GDC.

7.1.5 Análisis de Impacto en el Negocio BIA

Esta metodología se aplica a los recursos críticos de la GDC siguiendo los pasos aplicados en la guía 11 del MSPI del MinTIC, para identificar los activos de información que son indispensables en los procesos misionales; además, se definieron los tiempos y prioridades de recuperación (MinTIC, mintic.gov.co Guía 11 2017). Esta metodología se define con la participación de los funcionarios del Grupo TIC de la GDC mediante unos pasos requeridos con el

objetivo de identificar claramente los impactos negativos de una interrupción para la toma de decisiones en las acciones proactivas y reactivas en la GDC. A continuación, se muestran los pasos requeridos:

- ✓ Criterios de interrupción.
- ✓ Identificación de procesos y activos críticos.
- ✓ Identificación de infraestructura.
- ✓ Identificación de recursos y servicios críticos.
- ✓ Disposición del RTO/RPO.
- ✓ Evaluación de impacto operacional.

7.1.5.1 Criterios de interrupciones

La definición de los criterios de interrupción se realizó basados en los recursos y servicios críticos del centro de datos de la GDC y evaluados en dos formas:

- ✓ Impacto cuantitativo, se presenta por pérdidas económicas ocasionada por la interrupción (daños materiales o perdida de información).
- ✓ Impacto cualitativo o de reputación y está de cara a la comunidad (afectando en los procesos de contratación o en la no entrega de proyectos municipales).

A continuación, se describen escenarios o criterios de interrupción que pueden incidir de forma negativa en las operaciones esenciales de la organización.

- ✓ Pérdida de comunicación o caída de sistemas tecnológicos: se presenta al darse fallas o interrupción prolongada en el hardware y/o software, ocasionados por: malware (virus), degradación en la red (cableado de comunicación), daños en el fluido eléctrico, fallas en las aplicaciones o por error humano.

- ✓ Dependencia de operaciones realizadas por terceros (Proveedores): se presenta cuando las actividades de procesos críticos dependen del proveedor, generando retraso en las actividades por la ineficiencia de las mismas; en estos casos se debe constatar en el contrato del proveedor la existencia de un plan de contingencia que le permita a la entidad garantizar la continuidad de sus actividades críticas, y deben ser aprobada por el Grupo TIC de la GDC.

7.1.5.2 Identificación de procesos y activos críticos

Durante la visita presencial en las instalaciones de la GDC y en acompañamiento con el personal del grupo TIC, se plantearon cuestionarios y entrevistas a los funcionarios claves (personal antiguo y líderes de áreas) de las diferentes dependencias de la organización, ya que ellos ofrecen un mejor ámbito organizacional para identificar los servicios, procesos y herramientas fundamentales de los servicios de la GDC que son soportadas por el centro de datos, y así lograr calcular el impacto cuantitativo y cualitativo que permite determinar cómo impactaría una afectación de servicio; además, se rescata documentación que contiene información de los contratos por terceros, activos e información de la red y recursos operacionales.

Esta entrevista y revisión se realizó en sinergia con el Grupo TIC, en el que se determinaron los siguientes criterios:

- ✓ Análisis de criticidad: Se realiza el análisis e identificación de las actividades principales y esenciales que son soportadas y administrada por el centro de datos, con el fin de identificar cuales son los componentes y recursos tecnológicos que se deben contemplar como críticos dentro del DRP; adicional, se identificó fechas consideradas criticas, dado que son fechas de postulación y cambio de gobierno.

- ✓ Periodo de durabilidad de una interrupción: se determina al instante que ocurre la interrupción hasta el tiempo (horas/días) máximo que pueda estar inhabilitado el servicio, permitiendo saber si se sigue ofreciendo servicio o se recurre a contingencias.

- ✓ Impacto legal: se da si la interrupción impacta en el incumplimiento de servicio por la no entrega de reportes o contratos y por irregularidades en la información almacenada, el cual generan procesos disciplinarios.

- ✓ Impacto en la reputación o imagen organizacional: se presentará si se afecta un activo crítico que interrumpa la entrega o finalidad de un proceso o servicio, haciendo que esta no se cumpla en las fechas acuerdas y como consecuencia esto se lleve a procesos legales.

- ✓ Impacto operativo: afectación del servicio de la GDC, el cual deja inoperativa toda la planta en los sistemas de comunicación.

- ✓ Comunicaciones: especifica si el servicio afectado impacta las funciones críticas del negocio, incurriendo a procesos legales y daño en la imagen.

- ✓ Seguridad de los empleados: este representa ser el activo más valioso en la entidad y se debe aplicar normas que les permitan a estas garantizar la integridad física y mental, dado que ellos poseen el conocimiento y trayectoria en el ciclo de vida de la organización.

Posterior a las actividades de estas visitas y reuniones con los funcionarios claves de la GDC, se pudo definir en sinergia con el Grupo TIC los aplicativos que se consideran críticos dentro de la organización y que aran parte de los recursos críticos dentro del DRP. La tabla 2 describe cada uno de los aplicativos que se consideran críticos dentro de la organización.

Aplicativos	Descripción
PCT Enterprise	Software Financiero Bases de Datos (Modular).
SIAN	Software de Nomina de empleados y pensionados.
Portal Web	Espacio disponible para la ciudadanía e interesados.
Todod	Permite brindar soporte a nivel de Software por script a la Herramienta PCT Enterprise
PFsense	Permite la administración y controlar el Firewall de la entidad
Outlook	Gestión de notificación y entrega de resultados vía E-mail
Winbox	Permite controlar y administrar el enrutador de la organización.
ControlDoc (en proceso de implementación)	Software de gestión documental.

Tabla 2. Softwares críticos para el negocio.

7.1.6 Identificación de los activos

Con el fin de conocer y aportar en la gestión del riesgo se realiza la identificación de los principales activos que soportan los servicios críticos en el centro de datos para los servicios de la GDC. En esta sección se encontraron los activos clasificados en las categorías que corresponden a:

datos, servicios de aplicaciones, infraestructura, equipamiento auxiliar. Esto con el fin de obtener registros completos y precisos de los activos de información.

Actualmente en la GDC no se cuenta con un proceso completo de inventario de activos que permita tener la información básica y real de aquellos activos de información que ingresan, salen o que se encuentran en producción, al igual que los activos de información clasificada (Alta, Media, Baja y No Clasificada) para dar un apropiado manejo y seguimiento. Se recomienda realizar la recolección de información básica de los activos de información de la entidad, de acuerdo a la forma establecida en la guía cinco del MSPI del Min TIC, Gestión y Clasificación de Activos (ver figura 6) para contar con un apropiado cumplimiento gestión de activos (MinTIC, mintic.gov.co Guia 05 2017):

- ✓ Inventario de activos.
- ✓ Propiedad de los activos.
- ✓ Uso aceptable de información.
- ✓ Devolución de activos.
- ✓ Clasificación de la información.
- ✓ Etiquetado de la información.
- ✓ Manejo de activo de información.

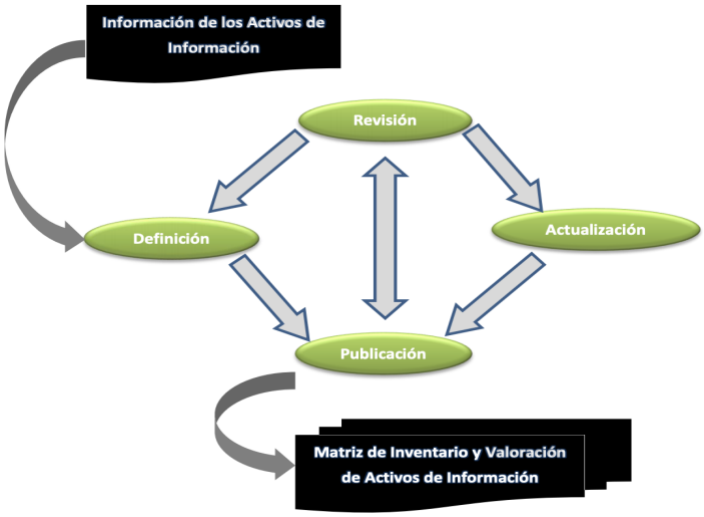


Figura 6: Procedimiento para Inventario de Activos (MinTIC, mintic.gov.co Guia 05 2017).

El anterior esquema ilustra el procedimiento para el levantamiento de inventariado de activos de la GDC, el cual contiene los pasos deseados para esta necesidad. Para el DRP es imprescindible contar con esta información, ya que permite una mayor efectividad en la gestión de eventos disruptivos.

7.1.6.1 Registro de activos en producción

Dentro del proceso de identificación y registro de los activos presentes en la Guía 5 del MinTIC (MinTIC, mintic.gov.co Guia 05 2017). Es conveniente que estos tengan como mínimo los siguientes contenidos de información básica que muestre las características de cada uno de ellos:

- ✓ Identificador: Registro único de identificación consecutivo que identifique al activo en el inventario.

- ✓ Nombre del activo: Nombre de identificación del activo dentro del proceso al que hace parte.

- ✓ Proceso: Nombre del proceso al que pertenece el activo.

- ✓ Observaciones: Pequeña descripción del activo de forma clara para que el activo pueda ser identificado en el proceso.

- ✓ Tipo: Definir el tipo al cual pertenece el activo (información, software, hardware, servicio).

- ✓ Ubicación: Descripción física y/o electrónica del activo de información.

- ✓ Clasificación: Referente a la protección de información en relación a la Confidencialidad, Integridad y Disponibilidad.

- ✓ Criticidad: Definir la criticidad en el proceso (Alta – Media – Baja).

7.1.6.2 Identificación de Infraestructura

En el proceso del levantamiento de información se obtiene un aproximado de un total de 250 activos en la GDC incluyendo máquinas de escritorios y portátiles, el cual son fundamentales para sus actividades automatizadas. Dentro de las funciones se encuentran 2 aplicaciones fundamentales de gestión pública que son fundamentales para los procesos de la GDC: programa de sistema financiero modular PCT Enterprise (ver anexo D), al igual que el de nómina de empleados y pensionados “SIAN” creado por SOLREDES (ver anexo E).

A continuación, se describen los recursos tecnológicos que hacen parte de la infraestructura tecnológica de la GDC y son administrados por el Grupo TIC para garantizar su funcionamiento y serán parte del DRP por su importancia y validez en los procesos y funciones de la GDC, en el anexo F se muestra el esquema de red de la Infraestructura de la GDC (ver anexo F). En la siguiente tabla 3 se describen los equipos tecnológicos del centro de datos de la GDC.

	Equipo	Descripción
Aplicación de Usuario	1 PCT Enterprise	Sistema de Gestión de la Base de datos
	1 Todod	Ejecutor de Script PCT (Soporte)
	1 SIAN	Software de nomina y pensionados
	1 control Doc.	Software de notificación
	2 portal Web	Portal publico de la GDC
	1 Outlook	Proveer correos institucionales
Centro de Datos	1 PFsense	Firewall
	1 Winbox	Controlador de la Mikro TIC
	1 Ubiquti Discovery	Controlador de Radio Enlace
	4 -Windows Server 2012	Plataformas que soporta servicios y aplicativos críticos
	1 -Linux Centos	Plataforma de pruebas (no productivo)
	1 -Oracle Linux	Bases de Datos
	1 -VMWare	Ambiente de pruebas
	Avaya Ipofice 500 V2	Software de administración de VoIP
	4 servidores físicos	DELL - Power EDG R720
	D-Link Share Center	Copia de seguridad Modelo DS-320
	8 Switches	Equipo de conectividad
	10 cámaras	Dispositivos de seguridad visual
	2 UPS - 300	Equipo para controlar los cambios de voltaje en los equipos de cómputos
	3 RAC	Estructura física que alberga los equipos tecnológicos
	10 Access Point	Dispositivos que permiten el acceso inalámbrico
	23 impresoras	Equipo para imprimir documentos
	40 teléfonos IP	Equipo de comunicación
	130 PC escritorios	Equipos de escritorio
	1 SAN	Red de Área de Almacenamiento
	2 modem ADSL	Equipo de comunicación dedicado

Tabla 3. Equipos tecnológicos en el centro de datos de la GDC.

La identificación de los componentes tecnológicos dentro del centro de datos, permitió levantar la información pertinente para la administración de los recursos que se considerarán críticos dentro del DRP y que serán contemplados dentro de la clasificación y priorización en los procedimientos de recuperación, La siguiente tabla ilustra dichos componentes.

7.1.6.3 Identificación de recursos críticos

Categoría (Función Crítica del Negocio)	**Procesos críticos (Servicios)**	**Identificación de recursos críticos de Sistemas TI**
Aplicaciones (PCT, SOLREDES, ControlDoc).	Sistema de nómina y sistema de gestión documental.	Sistema de entradas de novedades administrativas. Interfaces con el Sistema Financiero y bases de datos
Seguridad de Información (PFsense)	Firewall – Seguridad perimetral	Reglas de entradas y salida de puertos. Reglas NAT/PAT. Direccionamiento IP público.
Comunicaciones.	Servicio de conectividad.	Control de identificación de usuarios con Portal Cautivo. Control de usuarios locales Vs Invitados
Cuartos de Máquinas (Rack - Servidores – Swichet – Aire acondicionado – UPS - Otros).	Centro de Datos – Centro de Procesamiento de Datos.	Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de Backups, Aire Acondicionado, Acometidas Eléctricas.

Tabla 4. Identificación de recursos críticos de Sistema TI.

La identificación de los recursos críticos dentro de estos componentes de la administración del centro de datos, permitió categorizar las funciones, procesos y recursos críticos del negocio dentro de la GDC y de esta forma lograr dar el avance a la evaluación de impacto operacional.

7.1.6.4 Evaluación de Impacto Operacionales

Ahora bien, conociendo los elementos operacionales de la GDC, evaluamos el nivele de impacto de una interrupción dentro de la organización,

y se mide con el esquema de valoración, contando con los siguientes niveles empleados en la guía 11 del MinTIC (MinTIC, mintic.gov.co Guía 11 2017):

- ✓ **Nivel A:** La operación es crítica para el negocio; y al no contar con ella, las funciones del negocio no se pueden realizar.

- ✓ **Nivel B:** La operación es parte integral del negocio, sin ella el negocio no podría operar normalmente, pero la función no se considera crítica.

- ✓ **Nivel C:** La operación no es una parte integral del negocio.

A continuación, se muestran los resultados obtenidos de acuerdo con los niveles de criticidad de la organización junto con el sistema de tolerancia a fallas por horas, cuya propiedad muestra los tiempos de restauración de los servicios antes de que presenten un impacto negativo.

Categoría (Función del Negocio)	Procesos (servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
ControlDoc	Sistema de gestión documental	**B**	**3**	Proceso de documentación de incidentes, y gestión de soportes
PCT	Sistema de nominas	**B**	**3**	Herramienta modular que sirve para el control de la base de datos DB
Solredes)	Sistema de nominas	**B**	**3**	Herramienta modular que sirve para la gestión de nóminas de empleados y pensionados
Web	Sitio web de Entidad	**A**	**1**	Capa de presentación (Portales web)
Base de Datos	Oracle (Nómina)	**A**	**4**	Contenedor de aplicaciones en Oracle (DB)
Seguridad de la Información	Servicio de seguridad	**A**	**1**	Seguridad perimetral Firewall, Proxy,

	perimetral Firewall (físico)			Filtrado y visualización de navegación, Antivirus, DNS, IDS, VPN, SSH, Backup de PFSENSE
Sistema de Almacenamiento	SAN (Storage Área Network)	**A**	**3**	Mejora el rendimiento y disponibilidad en las aplicaciones por la segregación del tráfico en la red.
Comunicaciones	Acceso (Intranet, internet u otros)	**B**	**1**	Servicio de internet para el usuario local y/o comunicación local
Cuartos de Máquinas	Centro de Datos	**A**	**1**	Servidores, Switches, UPS, Router en producción
Proveedores de Aplicaciones y/o Comunicaciones	Interno/Externo	**B**	**4**	Desarrollo Interno o contratado por externos. Canales de comunicaciones
Recursos Humanos	Interno/Externo	**C**	**3**	Profesionales encargados de administrar las infraestructuras de la Entidad

Tabla 5**.** Valoración Operacional por niveles de criticidad.

A través de la anterior tabla, se pretende contemplar la categorización de las funciones criticas del negocio junto con su nivel de tolerancia a fallos y así conocer los niveles de importancia que deben tener ante una situación disruptiva.

7.1.6.5 Establecimiento de Tiempos de Recuperación

Se establece los tiempos de recuperación basados en la identificación de los procesos y actividades esenciales críticas del negocio que son una serie de componentes que corresponden al tiempo disponible para recuperarse de una interrupción no planeada dentro de los servicios, los tiempos de recuperación se describen a continuación en relación con la siguiente tabla:

Tiempo de recuperación	Descripción
RPO	Tiempo máximo Aceptable o Tolerable de pérdida de datos, medida en periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo máximo Tolerable para Recuperar Sistemas y/o Recursos que han sufrido una alteración para que vuelvan a estar en línea.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los Sistemas y/o Recursos están reparados. Tiempo de Recuperación de Trabajo; es decir, vuelta a la normalidad.
MTD	Tiempo de Inactividad máximo que puede tolerar la Entidad sin entrar en colapso; ejemplo, la suma de RTO y WRT

Tabla 6. Descripción de tiempos de recuperación. Tomado de (MinTIC, mintic.gov.co Guía 11 2017).

Es importante tener claro los tiempos de recuperación para tener un nivel de respuesta adecuado a las necesidades de la organización; además, permite brindar un adecuado reporte de los tiempos de afectación del servicio y respuesta ante los incidentes de seguridad.

A continuación, la figura 7 contempla una representación del inicio y fin de una interrupción por etapas, tomado de la publicación (Obaid 2013):

- ✓ Etapa 1: Representa el estado normal de las operaciones del negocio antes de una interrupción no planeada.

- ✓ Etapa 2: Inicio de la interrupción no planeada, el cual representa el momento exacto en que inicia el evento de interrupción o desastre. Y es donde se debe contemplar el punto objetivo de recuperación RPO dentro del nivel de tolerancia a perdida de datos e información de la GDC.

- ✓ Etapa 3: Es el tiempo objetivo de recuperación RTO, el cual contempla el tiempo de tolerancia para recuperar un servicio o sistema tecnológico que a sufrido alteración y debe ser restablecido dentro de los tiempos preestablecidos.

- ✓ Etapa 4: Corresponde al tiempo de recuperación del trabajo WRT, el cual se estima que se recuperen los datos perdidos y/o sistemas afectados una vez que los recursos de TI estén recuperados.

El MTD Representa el tiempo de inactividad máximo que puede tolerar la organización sin entrar a un colapso, y corresponde a la sumatoria del RTO y WRT.

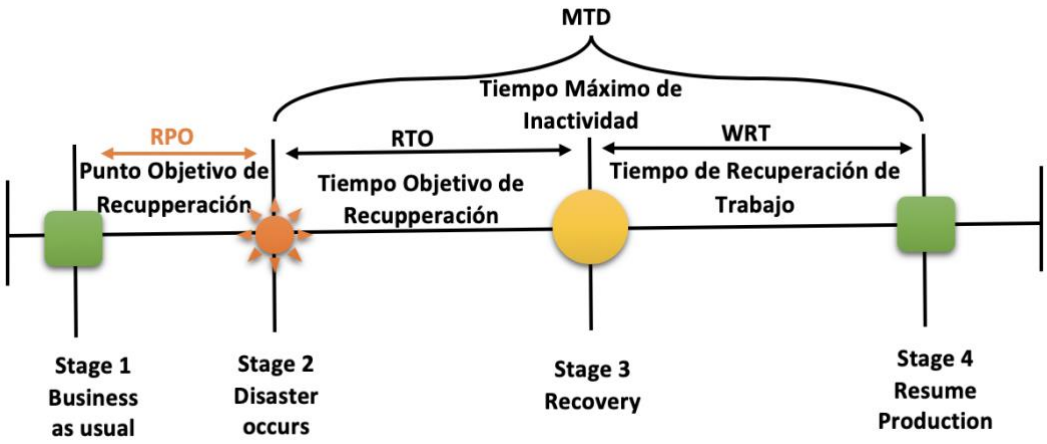


Figura 7: Grafica de los tiempos de recuperación, por (Obaid 2013).

Después de la identificación de los procesos críticos del negocio, se define el MTD correspondiente al tiempo máximo de inactividad que puede tolerar la GDC antes de sufrir un impacto negativo, a fin de priorizar la recuperación de los procesos afectados, y se definieron con el siguiente criterio:

- ✓ Periodo máximo de tiempo MTD de un (1) día, que debe tener un nivel de prioridad alta para iniciar el evento de recuperación frente a otro que tenga mayor tolerancia, por el poco tiempo de tolerancia de inactividad.

- ✓ El símbolo (*) indica el tiempo de inactividad de proceso crítico, que tomaría menos de un (1) día de tolerancia de inactividad.

Categoría (Función crítica del negocio)	Procesos críticos (Servicios)	MTD (Horas)	Prioridad de recuperación
Aplicación (SIAN)	Sistemas de nómina, SOLREDES (SIAN)	**12 H***	**1**
Aplicación (PCT)	Sistema de gestión de la Base de Datos (Software) PCT Enterprise	**12 H***	**1**
Aplicación (Control Doc.)	Software de gestión de sistemas de gestión con solución vía web. Gestión de control de flujo de documentos.	**48 H**	**2**
Aplicación (Correo Institucional)	Sistema de notificación y comunicación	**12 H***	**1**
Soporte Informático	Equipo PC de Usuario final	**48 H**	**4**
Comunicaciones (Intranet, internet u otros)	Servicio a conectividad a la red.	**24 H**	**2**
Sistemas de almacenamiento (Red de Almacenamiento)	SAN (Storage Área Network)	**24 H**	**1**
Seguridad de información (Seguridad perimetral)	Máquina virtual. Firewall, Proxy, Filtrado y visualización de navegación, Antivirus, DNS, IDS, VPN, SSH, Backup de PFSENSE	**12 H***	**1**
Cuarto de Máquinas de la GDC	Centro de Datos	**12 H***	**1**
Portal departamental	Noticias, Impuestos en línea, notificaciones de actos administrativos y sistema virtual de Solicitudes, quejas y reclamos.	**24 H**	**3**

DHCP	Servicio DHCP, asignación dinámica de direcciones IP, y entre otros parámetros de configuración de red.	**12 H***	**3**

Tabla 7. Prioridades de Recuperación de procesos críticos.

Con la priorización de cada uno de los procesos críticos de las categorías incluida en la tabla 7, permite facilitar el orden de recuperación de los recursos críticos afectado de forma organizada de acuerdo a los tiempos predefinidos y nivel de tolerancia.

7.1.6.6 Tiempos de recuperación RTO/RPO

Al entender la visión del negocio en los procesos que lo componen y la criticidad de los mismos, se comienza a establecer junto con el personal del Grupo TIC los tiempos de recuperación (RTO/RPO), teniendo en cuenta que el objetivo del DRP es recuperar los recursos y servicios críticos de TI que sostienen las actividades esenciales para evitando pérdidas financieras, dado que el RPO corresponde a la magnitud de pérdida de datos (de acuerdo al cronograma de realización de respaldos) medidos en términos de un periodo de tiempo que puede tolerar un proceso de negocio. RTO será el tiempo disponible de recuperación de los sistemas y/o recursos que sufrieron alteración.

A demás, se aplica el Tiempo de Recuperación de Trabajo WRT que determina la cantidad máxima de tiempo tolerable requerido para comprobar la integridad del sistema o datos alterados, definiendo la cantidad total de tiempo que puede interrumpirse un proceso de negocio sin causar consecuencias inaceptables. La siguiente muestra los valores RTO/WRT.

Categoría (Función Crítica	**Procesos críticos (Servicios)**	**Identificación de recursos críticos de Sistemas TI**	**Tiempo de recuperació**	**Tiempo de Recuperación**

del Negocio)			n Objetivo - RTO	de Trabajo - WRT
Cuartos de máquinas	Control de operación de Servicio, equipos de comunicaciones	Sistema de Almacenamiento.	**12 H***	**24 H**
		Sistemas de Backup	**12 H***	**24 H**
		Aire Acondicionado	**24 H**	**36 H**
		Acometida Eléctrica	**12 H***	**12 H**
		Cableado de Datos y Voz	**12 H***	**24 H**
		Red Lógica	**12 H***	**24 H**
		Servidores - Conmutadores – Router -	**12 H***	**24 H**
Equipos de seguridad físicos	Medidas de Seguridad en caso de incendio o inundaciones	Sistemas de drenajes	**24 H**	**24 H**
		Extintores	**72 H**	**72 H**
		Vías de evacuación despejadas	**72 H**	**72 H**
		Puertas ignifugas	**96 H**	**96 H**
		Control de temperatura y humedad con SNMP (Solicitar)	**72 H**	**72 H**

Tabla 8. Valores RTO y WRT por cada proceso crítico.

A través de la tabla de valoración de los RTO y WRT se pretende ilustrar los tiempos de recuperación de los procesos críticos del negocio y el nivel máximo de tolerancia a fallos y perdida de datos en la GDC, brindando información clara sobre la administración y gestión del DRP.

7.2 Etapa de Análisis

7.2.1 Gestión del Riesgo

La gestión de los riesgos permite que el líder de seguridad de la información calcule la magnitud y la anticipación de los riesgos, comprendiendo el impacto

en el negocio y la posibilidad de ocurrencia; así mismo, él contará con las capacidades necesarias para reducir o anular la recurrencia de los eventos disruptivos a niveles aceptable. Se precisa que la buena estrategia de controlar los riesgos genera valor al crecimiento y desarrollo de la organización.

El objetivo de la gestión del riesgo es definir, analizar, cuantificar, reportar y administrar el riesgo en relación a la seguridad de la información de la GDC para lograr los objetivos del negocio, a través de una serie de tareas que requieran de la habilidad del líder de seguridad de la información mediante las técnicas de administración del riesgo. La estrategia de gestión de riesgos fue tomada de las recomendaciones y buenas practicas del MSPI del MinTIC, el cual referencian la norma ISO 31000:2009, esta norma contiene información de los pasos a seguir para una buena administración de los riesgos (MinTIC, mintic.gov.co Guía 07 2017).

Figura 8: Administración o gestión del Riesgo.

La norma ISO 31000:2009 permitió a través de sus etapas, identificar, analizar, valorar y definir las alternativas requeridas para la gestión de los riesgos, y a su vez las acciones pertinentes para mitigar los riesgos contando con el desarrollo de los elementos descritos en la anterior figura 8 de (ICONTEC - NTC-ISO31000:2009).

7.2.2 Clasificación de escenarios de riesgo

A fin de identificar los riesgos potenciales de la prestación de servicios tecnológicos en la GDC, se realiza la clasificación de los escenarios de riesgos que pueden materializarse en la administración del centro de datos y recursos humanos que impactarían en la confidencialidad, integridad y disponibilidad de la información. En la siguiente tabla se describen las diferentes categorías y subcategorías desarrolladas en la GDC.

Categorías	Escenarios	Subcategoría	Descripción Impacto
Red eléctrica	Racionamientos constantes en flujo eléctrico por la entidad prestadora del servicio.	Ausencia de planta eléctrica de respaldo para flujo eléctrico.	Indisponibilidad del servicio en el centro de datos de la GDC.
			Degradación en los equipos de capa 3 del centro de datos (Appliance, Switches Routers, otros).
Red de datos e Internet	Acceso no autorizado en la red y la información.	Ausencia de herramientas de monitoreo de los eventos y alertas de seguridad en la red.	Indisponibilidad del servicio en la red de comunicación por alto consumo de red.
	Conexión de equipos no autorizados.		
	Intermitencia en la comunicación y transmisión de Voz y Datos.	Incumplimiento de normas (TIA-568B) que regulan el correcto despliegue y montaje de cable estructurados y acometidas en los data center.	Indisponibilidad de servicio de comunicación en el centro de datos de la GDC.
	Manipulación errónea de los cables físicos por no estar etiquetados correctamente.		
	Bajo control de seguridad en el tráfico y la vigilancia de los eventos de seguridad en la red.	Ausencia en la administración	Infiltración de personas no idónea en la red y robo de información sensible.

Seguridad lógica	Ausencia de control en la navegación web (Internet).	del Control de Acceso en la Red (NAC) en conjunto con Firewall, IPS/IDS, Proxy y Antivirus.	Robo de información sensible, navegación en sitios web inseguros
	Ausencia del control de detección de comportamientos extraños de los usuarios, equipos y software no autorizados.		Infección de equipos (Malware) que afecten la integridad de la entidad.
Hardware	Accesos de personas no autorizadas al centro de datos de la GDC.	Ausencia de políticas de control de cambio para los accesos autorizados.	Indisponibilidad del servicio de los equipos que soportan las aplicaciones (PCT, SIAN, Todoc y otros) de la GDC.
	Ausencia de mantenimientos en los equipos de TI del Centro de Datos de la GDC.	Ausencia de políticas para el mantenimiento de los equipos de TI del Centro de Datos.	
	Equipo de Backup con baja capacidad para el almacenamiento de la información sensible.	Ausencia de políticas de seguridad para los procedimientos de Backup.	Perdida de información sensible que Impacta en la disponibilidad de la información.
Aplicaciones infraestructura distribuida	Ausencia de protocolos de seguridad (TLS/SSL) en el transporte de la información por la red.	Ausencia de políticas de seguridad en los protocolos de comunicación.	Impacto en la integridad, disponibilidad y confidencialidad de la información, debido a la posibilidad de interceptación de la comunicación por terceros.
	Manipulación técnica de los equipos de comunicación del centro de datos sin autorización u órdenes de cambios.	Ausencia de políticas de control de cambio que permita la autorización de cambios en la infraestructura.	Impacto legal, Indisponibilidad del servicio y perdida de información sensible.

Desarrollo de aplicaciones	Actualizaciones con errores en el funcionamiento de las aplicaciones críticas de la GDC.	Ausencia de correcto soporte técnico en las aplicaciones críticas.	Falla en las aplicaciones (PCT, SOLREDES y otras) críticas de la GDC.
Recursos humanos	Ausencia incapacidades, rotación de funcionarios.	Ausencia de capacitaciones a personal alternativo para suplir el rol de otro un funcionario ausente.	Reducción en la capacidad de atención al ciudadano o los requerimientos de los objetivos de la organización.

Tabla 9. Clasificación por categorías de escenarios de riesgo.

A través de las reuniones y seguimientos de las actividades realizadas en sinergia con el Grupo TIC, se logro la clasificación de las categoría y subcategoría de los escenarios de riesgos en la GDC, el cual se describieron en la anterior tabla 9, permitiendo una visibilidad de los escenarios de riesgos que representan un impacto negativo en la promesa del negocio.

7.2.3 Identificación de riesgos potenciales

Los riesgos se identificaron determinando las causas internas y/o externas que pueden afectar el logro de los objetivos planteados en la entidad, con base a los factores relacionados a los servicios del centro de datos de la GDC. De esta manera se centró en los riesgos más significativos que al materializarse traerían consecuencias negativas. Dentro de la visita técnica al centro de datos e instalaciones de la GDC, se identificaron cinco (5) riesgos potenciales clasificados en los diferentes recursos de los activos identificados en el BIA.

ID	Riesgo	Descripción	Agente generador	Causa	Efecto

R1	Perdida de información sensible.	Uso inadecuado de los recursos de TI y la información.	Ausencia de sensibilización políticas de ciberseguridad.	Acceso abusivo a la red con privilegios, generando pérdidas irreparables de la información.	Indisponibilidad de la información
		Procedimientos indebidos en las copias de seguridad de la información sensible.	Ausencia de políticas para la administración de información sensible.	Malos procedimientos en las copias de seguridad de información primordial para los RTO y RPO.	
R2	Acceso no autorizado por personal no idóneo a los recursos de TI..	Acto hostil y acceso no autorizado en la red y la información.	Ausencia de Control de Acceso a la Red (NAC) que impida el acceso a la red.	Acceso y robo de información sensible que comprometen la imagen de la GDC.	Daño en la imagen pública
R3	Modificación no autorizada de la información.	Información sensible en papel implica: la modificación, pérdida y robo de información sensible.	Ausencia de políticas de gestión documental de la información que se crea, se transfiera y se guarda.	Actos hostiles, robo y divulgación de información sensible por personal no idóneo.	Perdida de integridad de la información, el cual llevan a problemas legales.
R4	Perdida en la confidencialidad.	Recepción de Phishing, Malware Spamming o correos de procedencias desconocidas.	Ausencia de equipos y herramientas de monitoreo que alerten los eventos de seguridad en la red.	Brechas de seguridad persistentes, presencia de software malicioso en la red.	Impacto negativo en la confidencialidad de la información

R5	Perdida de servicio en el centro de datos de la GDC.	Manipulación indebida de los equipos críticos del centro de datos.	Ausencia de control de cambio para cambios en la infraestructura.	Interrupciones no programadas en los servicios de los equipos que soportan las aplicaciones.	Indisponibilidad total del servicio del centro de datos.

Tabla 10. Identificación de riesgos.

Es importante resaltar la fase de identificación de riesgo, ya que a través de ello se pudo contar con el apoyo de funcionarios claves en administración de riesgos operacionales y en las soluciones a fallas de hardware y software que ya se han presentado en la entidad. En esta etapa se debió enfocar en los riesgos más significativos de la organización relacionados con los procesos y objetivos institucionales que se consideren críticos, junto con la proactividad de la alta dirección.

7.2.4 Análisis de riesgos

Se establece las probabilidades de ocurrencia del riesgo y sus consecuencias, el cual permite la recolección de información que contribuye en la clasificación del riesgo y metodologías para su evaluación, con el objetivo de establecer el nivel de riesgo y las acciones que se deben implementar como alternativas, y esta depende de la información obtenida en la fase de identificación de riesgos. A pesar de la existencia de diversos métodos, es recomendable comenzar con los más sencillos que forman parte de lo que denominamos análisis previos. Una primera aproximación es la de establecer un conjunto de causas que pueden generar dificultades, tales como:

- ✓ Red eléctrica o fluido eléctrico: Razonamientos no programados que impiden el correcto funcionamiento de los equipos que soportan las aplicaciones y actividades esenciales del centro de datos de la GDC, debido a la falta de equipos de respaldos de fluido eléctrico que causan la no disponibilidad del servicio que afectan la promesa del negocio.

- ✓ Red de datos, Internet: Ausencia de cumplimiento de norma TIA-568-B que garantizan la correcta implementación de acometidas y etiquetado de cable estructurado que permitan el correcto funcionamiento del centro de datos. Además, se requiere de herramientas que permitan alertar los eventos de seguridad en la red.

- ✓ Seguridad: Ausencia en la administración del control de acceso a la red (NAC) que en conjunto con los controles de seguridad (Firewall, IPS/IDS, Proxy y Antivirus) permitan la administración del tráfico, comportamientos, navegación en la Internet y el bloqueo de archivos malicioso.

- ✓ Hardware: Ausencia de políticas de seguridad para el acceso autorizado al centro de datos de la GDC mediante una orden de control de cambio, con el fin de evitar daños, robos o acto hostiles que generen indisponibilidad del servicio. Adicionalmente, se requiere contar con políticas para los procedimientos de copias de seguridad y mantenimiento en los equipos del centro de datos de la GDC.
- ✓ Aplicaciones e Infraestructura Distribuida: aumentar el nivel en los protocolos de seguridad para la trasmisión o comunicación de los datos entre la comunicación de los equipos en la red y así evitar impactar en la integridad, confidencialidad y disponibilidad de los mismos; adicionalmente contar con un sistema de gestión documental que les permita la autorización en los cambios que se requieren realizar en la infraestructura del centro de la GDC.

- ✓ Desarrollo de aplicaciones: Hacer cumplir el correcto soporte técnico de las aplicaciones en el momento de realizar cambios y actualizaciones.

- ✓ Recursos humanos: contar con los perfiles competentes y entrenamientos para los remplazos de personal en caso de presentarse

alguna incapacidad o necesidad de remplazar algún funcionario, y así evitar impactar negativamente la disponibilidad del servicio.

En la identificación de riesgo se han determinado dos categorías fundamentales que se deben tener en cuenta para el análisis de riesgo, probabilidad e impacto.

- ✓ Comprendiendo la probabilidad como la posibilidad de ocurrencia de un evento de riesgo, se mide con criterios de frecuencia (las veces que se ha presentado el riesgo en un periodo de tiempo) o por la factibilidad (factores internos o externos que hacen que el riesgo se materialice).

- ✓ Comprendiendo el impacto como las consecuencias que podrían generar a la entidad si se llegara a materializar el riesgo, y para dar un análisis de riesgo se deben considerar la evaluación del riesgo y calificación del riesgo

Calificación del riesgo: es dada al comprender la probabilidad de ocurrencia y el impacto que puede generarse al materializarse el riesgo. A continuación, se muestra la matriz de análisis cualitativo, la cual muestra la magnitud de las consecuencias potenciales (Impacto) y la posibilidad de ocurrencia (Probabilidad). Las categorías relacionadas con el impacto son: insignificante, menor, moderado, mayor y catastrófico. Las categorías relacionadas con la probabilidad son: raro, improbable, posible, probable y casi seguro.

De acuerdo a los criterios de probabilidad, el riesgo es calculado siguiendo las especificaciones descritas en la siguiente tabla.

Nivel	Descriptor	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años

2	Improbable	El evento puede ocurrir en algún momento.	Se presenta una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento.	Se presenta una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Se presenta una vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Se ha presentado más de una vez al año

Tabla 11. Tabla de probabilidad del riesgo tomada de (Tellez 2015, 71).

Estos valores se definen de acuerdo a las referencias de la metodología de la ISO 31000:2009 para la etapa de análisis del riesgo, ya que con base a esto se realizan las valoraciones. Bajo el criterio del impacto, el riesgo se mide a partir de las siguientes especificaciones plasmadas en la siguiente tabla**.**

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad. Circunstancias excepcionales.
2	Menor	Si el hecho llegara presentarse, tendría bajo impacto o efecto sobre la entidad. Momento.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad. momento
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la reputación de la entidad.

Tabla 12. Tabla de impactos del riesgo tomada de (Tellez 2015, 71).

En la tabla siguiente, se presenta una matriz de priorización, con la que se calificaron los riesgos de acuerdo a la magnitud del riesgo.

- ✓ Magnitud A: Nivel Alto de riesgo.

- ✓ Magnitud B: Nivel Medio de riesgo.

✓ Magnitud C: Nivel Bajo de Riesgo.

Probabilidad				
	Bajo	C	B	B
	Medio	B	B	A
	Alto	B	A	A
		Bajo	Medio	Alto
		Impacto		

Tabla 13. Matriz de priorización

A continuación, se presenta la tabla que contiene información sobre la magnitud de los riesgos analizados. La cual será imprescindible para la etapa de evaluación, donde se priorizarán o clasificarán según los criterios definidos para la reacción dentro del plan de recuperación de desastres DRP.

ID	Riesgo	Control existente	Probabilidad	Impacto	Magnitud
R1	Perdida de información sensible.	-Inexistente.	Medio	Alta	B
R2	Acceso no autorizado por personal no idóneo a los recursos de TI.	-Inexistente.	Baja	Medio	A
R3	Modificación no autorizada de la información.	-Inexistente	Medio	Alta	A
R4	Perdida en la confidencialidad.	-Inexistente	Medio	Alta	B
R5	Perdida de servicio en el centro de datos de la GDC.	-Inexistente	Alta	Alta	A

Tabla 14. Análisis de riesgos.

La anterior tabla 14 emplea el análisis de riesgos dentro de la GDC el cual se realizo un levantamiento de información de los controles que pudieran

mitigar los cinco riesgos identificados, y se evidencio que no se contaba con controles de seguridad que mitigara loa riesgos identificado.

Evaluación del riesgo: en la tabla de evaluación de riesgo se establecieron los criterios de priorización para su tratamiento de acuerdo a la magnitud frente a los controles existentes y se definieron los criterios con un SI/NO si el riesgo representaba ser tratado, en función a la magnitud que representa al no ser tratado a tiempo.

ID	Riesgo	Criterio	Tratar el riesgo
R1	Perdida de información sensible.	2	SI
R2	Acceso no autorizado por personal no idóneo a los recursos de TI.	1	SI
R3	Modificación no autorizada de la información.	1	SI
R4	Perdida en la confidencialidad.	2	SI
R5	Perdida de servicio en el centro de datos de la GDC.	1	SI

Tabla 15. Evaluación de riesgos.

La evaluación de los riesgos fue realizada teniendo en cuenta el impacto negativo que representa la materialización de las amenazas presentes en los recursos críticos y fue evaluado contra las acciones de respuesta existentes dentro de la GDC.

7.2.5 Tratamiento del Riesgo

Valoración del riesgo

En esta fase se examinaron los resultados de la evaluación del riesgo con los controles identificados, para determinar las principales prioridades del manejo y de esa forma plantear alternativas de mitigación, cabe resaltar que se debe tener en cuenta los puntos de control existentes en los procesos que

nos permitan obtener información relevante en efecto para la toma de decisiones. Para realizar la valoración de los controles ya existentes se deben clasificar en dos tipos, preventivos y correctivos:

- ✓ Preventivos: se clasifican en aquellos controles que permiten reducir la causa de los riesgos potenciales para evitar su materialización. Si se identifica como preventivo, significa que el control desplazará los cuadrantes de la probabilidad en el mapa de calor mejorando la valoración inicial.

- ✓ Correctivos: se clasifican en aquellos controles que permiten la reanudación de proceso detenidos por una interrupción, permitiendo modificar las fallas que propiciaron el evento, si se identifica como correctivo, significa que el control desplazará los cuadrantes del impacto en el mapa de calor mejorando la valoración inicial.

Valoración del control

Se presenta la objetividad de los controles para poder definir el desplazamiento dentro de la matriz de calificación, evaluación y respuesta a los riesgos a través de las siguientes tablas 16 y 17.

La tabla 16 corresponde a una herramienta que permite realizar una valoración de los controles confrontándolos con los criterios de la herramienta, el cual nos arroja una puntuación con el fin de disminuir la probabilidad o el impacto de los riesgos.

Parámetros	Criterios	Tipos de control		Puntaje
		Probabilidad	Impacto	
	Poseen de herramientas para ejercer el control.	Valor del control	Valor del control	10

Herramientas para ejercer el control	Existen manuales, instructivos o procedimientos para el manejo de la herramienta.	Valor del control	Valor del control	20
	En el tiempo que lleva la herramienta ha demostrado su efectividad.	Valor del control	Valor del control	30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.	Valor del control	Valor del control	10
	La frecuencia de ejecución del control y del seguimiento es adecuada.	Valor del control	Valor del control	30
	Total			

Tabla 16. Tabla de valoración de controles. Tomada de (MinTIC, mintic.gov.co Guía 07 2017).

El valor total de la valoración de los controles, se confronta contra los rangos de calificación de controles para determinar la disminución de la probabilidad e impacto dentro del mapa de calor que se encuentra en el punto 7.2.6. Como resultado final, se genera una segunda evaluación de riesgo.

Posterior a los resultados de la valoración de riesgo se obtiene el rango de calificación de los controles a través de la tabla 17, el cual determina la cantidad de posiciones a disminuir dentro de los cuadrantes del mapa de calor.

Rango de calificación de los controles	Dependiendo si el control afecta probabilidad o impacto desplaza en la matriz de calificación, evaluación y respuesta a los riesgos	
	Cuadrantes a disminuir en la probabilidad	Cuadrante a disminuir en el impacto

Entre 0 - 50	0	0
Entre 51 - 75	1	1
Entre 76 - 100	2	2

Tabla 17. Puntaje de disminución de riesgo. Tomado de (MinTIC, mintic.gov.co Guía 07 2017).

- ✓ Los resultados por de bajo o igual a 50 no disminuyen el riesgo (no existen desplazamiento dentro de los cuadrantes del mapa de calor).

- ✓ Los resultados por encima de 50 a 75 permite correr el riesgo un (1) cuadrante dentro del mapa de calor (permitiendo realizar un (1) desplazamiento).

- ✓ Los resultados por encima de 76 a 100 permite disminuir el riesgo dos (2) cuadrante dentro del mapa de calor (permitiendo realizar dos (2) desplazamiento).

El resultado obtenido a través de la valoración del riesgo, es denominado tratamiento del riesgo, ya que estos involucran la selección de uno o más opciones para modificar los riesgos y la ejecución de acciones, así que el desplazamiento dentro de la matriz de evaluación y calificación determinará la selección de las opciones para tratar el riesgo de la siguiente manera:

- ✓ Prevenir el riesgo: Llevar acabo las acciones correctas para prevenir la materialización del riesgo. Siempre es la primera alternativa a considerar, y son toda acción que al interior de los procesos creen cambios sustanciales para el mejoramiento, rediseño o depuración del riesgo y se obtengan resultados eficientes por adecuados controles.

- ✓ Mitigar el riesgo: Acciones que son encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de

protección). Prevenir los riesgos es quizás la metodología más sencillas y económicas para superar las falencias antes de optar por las medidas más costosas y difíciles.

- ✓ Transferir el riesgo: Reducir el efecto a través del traspaso de las pérdidas a otras entidad u organizaciones, una medida puede ser, el contrato con otras entidades de confianza para tener más confiabilidad y una reducción en los gastos o los contratos de seguros, el cual permita distribuir el riesgo para un mejor tratamiento.

- ✓ Asumir el riesgo: Luego que el riesgo ha sido manejado (reducido o transferido) pero han quedado vestigios de riesgo, se establecen planes de contingencia para su tratamiento o seguimiento.

7.2.6 Mapa de Calor del Riesgo

La realización del mapa de riesgo permite comprender la magnitud de las amenazas en la organización y para la factibilidad de toma de decisiones a través de la prevención de los posibles riesgos. A continuación, se presenta la comparación entre probabilidad e impacto de los riesgos identificados, donde se ilustra el mapa de calor de los 5 riesgos identificados dentro de la administración del centro de datos de la GDC.

Impacto / Probabilidad		**Insignificante**	**Menor**	**Moderada**	**Mayor**	**Catastrófico**
		1	2	3	4	5
Raro	1					
Improbable	2					
Moderado	3			R1	R3	
Probable	4			R4	R5	R2

Casi seguro	5					

Tabla 18. Confrontación entre Probabilidad e Impacto (Mapa de calor del riesgo).

La anterior tabla 18 muestra el estado actual de los cinco riesgos críticos identificados dentro de la administración del centro de datos de la GDC, y que serán analizados y clasificados para definir las alternativas que permitan mitigar o anular los cinco riesgos identificados en la GDC.

7.2.7 Análisis y clasificación de riesgos

De acuerdo con el análisis realizado en sinergia con el Grupo TIC de la GDC, empleando la metodología de la ISO 31000:2009 para la gestión de los riesgos, el cual se le aplicó una matriz de priorización según su magnitud. Se obtuvieron los siguientes resultados a la identificación y valoración de 5 riesgos, de los cuales 2 riesgo (R1-R4) fueron catalogados como Medios y 3 riesgos (R2-R3-R5) como Altos. En base a lo descrito anterior los riesgos de categoría Medios se les dará respuesta media asumiéndolos o reduciéndolos, los riesgos de categoría Alta se les dará como medidas de respuestas, prevenir el riesgo, reducir el riesgo, compartir el riesgo o transferirlo y los riesgos de categoría catastrófico se les dará respuesta, prevenir el riesgo, reducir el riesgo, compartir el riesgo o transferirlo.

7.3 Etapa de Diseño

Para esta fase de diseño se define las estrategias para mitigar los posibles impactos negativos de interrupción, se buscarán alternativas de mitigación adecuado según al tipo de riesgo que se busca controlar; partiendo de los posibles riesgos identificados en la fase de análisis, y para eso se tienen en cuenta los tiempos de recuperación establecidos por el BIA, disponibilidad y costes asociados a la entidad.

7.3.1 Identificación de las alternativas

A continuación, se muestran las alternativas y estrategias de manejo para mitigar o reducir el impacto de interrupciones no planeadas. Cada una de estas alternativas que se muestran en la tabla 19, puede contemplar parámetros de tiempo, disponibilidad y costes asociados que serán apropiados dependiendo de las funciones del negocio.

Alternativa de manejo	Descripción
Reducir probabilidad	Disminuir la cantidad de veces que se presente el riesgo.
Reducir impacto	Contrarrestar las consecuencias negativas del riesgo.
Transferir el riesgo	Pasar el riesgo a aliados estratégicos (Outsourcing).
Compartir el riesgo	Extender el riesgo entre áreas o diferentes secciones con el fin de frenar la pérdida de todo el negocio.
Evitar el riesgo	SI son prestados los servicios a terceros, estos pueden paralizar las actividades si dejan de entregar el servicio.

Tabla 19. Alternativas de manejo de riesgos.

Estas alternativas permiten una mejor administración de los riesgos, ya que pueden ser reducidos, transmitidos, compartidos o anulados. Haciendo que estas tengan una mejor gestión dentro de las operaciones del equipo de seguridad de la información de la GDC.

7.3.2 Evaluación de alternativas

Las alternativas o controles identificados para disminuir los riesgos debieron ser evaluados sobre la base de la efectividad o alcance para mitigar o reducir los riesgos, teniendo en cuanta los criterios desarrollados. Estas alternativas pueden aplicarse de acuerdo a la posibilidad de forma individual o combinada. A continuación, se ilustran las definiciones de las alternativas.

ID	Riesgo	Alternativas de manejo	Alternativa	Área responsable
R1	Perdida de información sensible.	Reducir probabilidad e Impacto.	✓ Crear programas de capacitación y entrenamientos para los funcionarios sobre los riesgos con el uso de la información. ✓ Crear las políticas para el copiado de seguridad de la información.	Sistema Informático e Infraestructura
R2	Acceso no autorizado por personal no idóneo a los recursos de TI.	Reducir la probabilidad e Impacto	✓ Implementar control de acceso a la red NAC, que permita el control de la Red en la GDC, mediante la integración de controles de seguridad como: Firewall, IPS/IDS y Antivirus	Sistema Informático e Infraestructura
R3	Modificación no autorizada de la información.	Reducir el Impacto y la probabilidad	✓ Crear políticas de gestión documental para los funcionarios que permita la tabulación de la información que crean, transfieran y resguarden.	Sistema Informático e Infraestructura

R4	Perdida en la confidencialidad.	Reducir el Impacto y la probabilidad	✓ Implementar herramienta que les permita monitorear el trafico en la red y las alertas de seguridad.	Sistema Informático e Infraestructura
R5	Perdida de servicio en el centro de datos de la GDC.	Reducir el Impacto y la probabilidad	✓ Implementar un sistema de control de cambio que permita gestionar la autorización para los cambios en el centro de datos de la GDC.	Coordinación, Sistema Informático e Infraestructura

Tabla 20. Evaluación de las alternativas.

La evaluación de las alternativas permitió que se identificara la efectividad de los controles o alternativas aplicados para reducir los riesgos identificados los cuales serán ilustrados en el mapa de calor (Tabla 22. Resultados esperados por las alternativas).

La siguiente tabla 21 contiene el comparativo de los riesgos antes del tratamiento y después de aplicar las alternativas definidas. Esto ayuda a ilustrar gráficamente la magnitud y el nivel de criticidad de los riesgos antes del tratamiento y después del tratamiento, permitiendo garantizar la efectividad de las alternativas aplicados a estos riesgos dentro de la organización, el cual garantiza el nivel de disponibilidad de la GDC.

ID	**Riesgo**	**Sin tratamiento**		**Con tratamiento**	
		Magnitud	**Prioridad**	**Magnitud**	**Prioridad**
R1	Perdida de información sensible.	B	2	C	3

R2	Acceso no autorizado por personal no idóneo a los recursos de TI.	A	1	B	2
R3	Modificación no autorizada de la información.	A	1	B	2
R4	Perdida en la confidencialidad.	B	2	C	3
R5	Perdida de servicio en el centro de datos de la GDC.	A	1	B	2

Tabla 21. Índices de magnitud y prioridad esperado.

A través del resultado de los riesgos ilustrados en la tabla 21 después de aplicar las alternativas, se logra evidenciar la reducción considerable de los cinco riesgos potenciales identificados en la GDC a términos aceptable. Aportando a las necesidades de cumplir con la seguridad de los datos, software, hardware de GDC y con el cumplimiento de las exigencias del MinTIC en el MSPI.

A continuación, en la siguiente tabla 22 se muestran el resultado del tratamiento de los riesgos después de aplicar las alternativas, el cual reducen los riesgos a términos aceptables.

Impacto / Probabilidad		**Insignificante**	**Menor**	**Moderada**	**Mayor**	**Catastrófico**
		1	2	3	4	5
Raro	1					
Improbable	2		R1	R3		
Moderado	3	R4		R2		
Probable	4			R5		
Casi seguro	5					

Tabla 22. Resultados esperados por las alternativas (Mapa de calor del riesgo).

La tabla 22 ilustra el resultado de la reducción de los cinco riesgos a términos aceptables, el cual se obtuvo después de haberse aplicado la valoración de los controles a las alternativas definidas para la mitigación de los riesgos, de esta forma se logra una puntuación que pasaría por la tabla de rango de valores (descrito en la tabla 17) que define la cantidad de desplazamiento de cuadrantes dentro del mapa calor, y así de esta forma obtener los resultados que permitan reducir la probabilidad e Impacto dentro de la GDC. De esa manera se obtuvo el siguiente resultado en la valoración de controles de las alternativas definidas:

- ✓ El riesgo uno (R1): obtuvo dos puntos de desplazamiento en la reducción de impacto y probabilidad.

- ✓ El riesgo dos (R2): obtuvo dos (2) puntos de desplazamiento en la reducción de probabilidad y un (1) punto de desplazamiento en la reducción de impacto.

- ✓ El riesgo tres (R3): obtuvo un (1) punto de desplazamiento en la reducción de impacto y probabilidad.

- ✓ El riesgo cuatro (R4): obtuvo dos (2) puntos de desplazamiento en reducción de probabilidad y un (1) punto de desplazamiento en la reducción de impacto.

- ✓ El riesgo cinco (R5): obtuvo un (1) punto de desplazamiento en la reducción de probabilidad.

7.3.3 Estrategia de respaldo

Actualmente existen diferentes estrategias que permiten mitigar el impacto negativo de una interrupción; sin embargo, cada una de estas estrategias tiene

parámetros de tiempos, costes y disponibilidad relacionados a las funciones y operaciones del negocio.

- ✓ Utilización de espacios y recursos propios: Utilización de espacios y recursos propios del ente público, como: salas de conferencias o formación, colegios (en disponibilidad), coliseos.

- ✓ Teletrabajo: Optar por la modalidad que emplea el trabajo remoto, que permite realizar labores desde lugares externos a las instalaciones de la entidad mediante conexiones remota.

- ✓ Reutilización de recursos: Reubicación de personal con funciones no urgentes en tareas que requieran una mayor prioridad con el fin de apoyar la demanda de tareas y funciones urgentes. Esta actividad se debe hacer con cautela al momento de convertir las funciones no urgentes en actividades con prioridad alta**.**

- ✓ Acuerdo reciproco: Acuerdo entre 2 entidades con características de equipamiento y especificaciones técnicas similares que permita a cada una de las partes recuperar funciones en otras instalaciones.

Subcontratación de sitios alternos: Subcontratar servicios por demanda que permitan contar con replicas de los recursos tecnológicos que soporten los servicios críticos de la GDC como segunda instancia de respaldo, para que estos entren en funcionamiento al momento de una situación disruptiva. Por consiguiente, el Grupo TIC de la GDC debería tomar como alternativas alguna de las siguientes estrategias de reacción inmediata para la recuperación y reactivación de los servicios a través de acuerdos y contrataciones.

- ✓ Acuerdo Reciproco: con el centro de datos de otra dependencia donde le permitan el traslado de sus servicios y operaciones críticas, el cual los

puedan tener en estado pasivo y volverlo activo en caso de la existencia de una situación adversa en el centro de datos de la GDC.

- ✓ Servicios en la nube: La nube ofrece servicios por demanda (infraestructura como servicio), este tipo de servicio son atractivas para las empresas ya que se garantiza una alta disponibilidad del servicio prestado; además, la seguridad se brinda como un modelo de seguridad compartida, donde el cliente se responsabiliza de la seguridad de los datos y la seguridad de la infraestructura es responsabilidad de quien preste el servicio; por lo tanto, se puede optar por este servicio para la GDC en modo pasivo/activo para poder mitigar el impacto negativo de una interrupción.

7.3.4 Selección de Respaldos

Estas estrategias de respaldos fueron seleccionadas de acuerdo con la necesidad con base a los tiempos de recuperación establecidos por el BIA, partiendo de los riesgos establecidos en la Gestión de Riesgos. A demás se debe tener en cuenta que la selección debe estar relacionada con la necesidad de recuperación de los servicios críticos; y la evaluación del costo en representación para el Grupo TIC. En seguida se ilustra la Tabla 6 que muestra la relación entre el Tiempo Objetivo de recuperación y la solución de continuidad más adecuada según el evento.

Tiempo objetivo de recuperación	Internas	Contratados
Meses	Reconstrucción/Reubicación	No Reacción
Semanas	Utilización de espacios propios	Contratación de otros espacios
Días	Reutilización de recursos	Teletrabajo
Horas	Acuerdos recíprocos	Subcontratación de sitios alternos a terceros
Inmediato	Contingencia interna dentro de la organización.	Centro espejo

Tabla 23. Estrategias de respaldo interna y externa, según los tiempos de recuperación.

La necesidad de la gran inversión económica en recursos auxiliares, es debido a los tiempos establecidos por el BIA, por lo planteado para la recuperación de los servicios críticos que están estimado por horas, y de recuperación inmediata por poca tolerancia de indisponibilidad, por lo que tiene que elevar sus costos de inversión económicos en recursos (Software, Hardware, Infraestructura, Datos de Respaldos, Comunicaciones), Recursos Humanos necesarios (recursos materiales y de Infraestructura, servicios auxiliares, tiempos de activación), etc. Para poder dar con el objetivo de recuperación aceptable.

Como recomendación, el principio para las copias de seguridad de datos regulares es respaldar datos diariamente, y esas copias de seguridad podrían ser para medios (ejemplo, cintas o disco duro externo), o una de las mejores alternativas, es la ubicación remota a través de la nube (internet); pero también este principio recomienda realizar las copias de seguridad en diferentes medios al final de la semana y al final del mes (y este conjunto de practica de

copias de seguridad, diarias, semanales y mensuales es llamada “Abuelo-Padre-Hijo”) (Berman 2017, 22).

Esta recomendación de respaldo de datos no solo implica el respaldo en el menor tiempo posible, sino el respaldo de forma organizada y adecuada de acuerdo a las prioridades que estén asociada a ellos en las necesidades de la entidad para optar por una mejor administración propicia que impacte positivamente en los procesos de los planes de recuperación de desastres informáticos a partir de una copia de seguridad.

Para los tiempos de recuperación inmediata:

- ✓ Contingencia interna: Se recomienda adoptar como medida de respaldo, la virtualización de cada uno de los servicios dentro de los servidores tipo Blade, en caso de la existencia de una situación adversa los servicios puedan ser trasladados, ya que estas cuentan con herramientas software para el traslado automático e inmediato asegurando la disponibilidad de servicio, Esta tecnología es económica en el mercado.

- ✓ Centro espejo: esta estrategia es de costo elevado ya que consiste en hacer una réplica del centro de datos parecida a la actual para disponerla en caso de emergencia.

7.3.5 Definiciones de Roles y Responsabilidades

De acuerdo a la Matriz RACI, se definen los roles y responsabilidades para la administración del DRP en la GDC y la gestión de actividades que están relacionadas con las TIC. La matriz RACI se define en sinergia con el Grupo TIC de la GDC, dado que es facilita la identificación de las responsabilidades en los proyectos y servicio, debido al esquema que muestra en los roles y

responsabilidades de cada uno de los procesos de trabajos de las TIC en la GDC (ver anexo G).

ID de la actividad: Se ingresa el identificador de la actividad (ID) de la actividad del proyecto, el mismo número que se usa para identificar la actividad del trabajo.

Actividad: Colocar el nombre del trabajo.

Colaboradores: Sustituir el texto por el nombre y apellido del integrante del equipo del trabajo que se asignaran las responsabilidades.

Roles/Responsables por actividad: En cada fila se especifica el tipo de responsabilidad asociado al colaborador de la columna, con los siguientes valores: **R**: Comprometido, **A:** Responsable, **C:** Consultado, **I:** Informado, **S:** Soporte y **Q:** Qualys.

8 LIMITACIONES O DIFICULTADES

Dentro de la etapa inicial en la recopilación de información se tuvieron diferentes limitantes que dificultaron un poco el desarrollo de este trabajo.

- ✓ No se contaba con formatos de inventariado de activos de información de los recursos de TI del centro de datos de la GDC. Esto dificulto el proceso de identificación de recursos críticos para emplearlos dentro del DRP.

- ✓ Al tratar de obtener información de parte de los funcionarios públicos de la GDC a través de una encuesta sobre la experiencia del servicio de las TIC para contemplarlos dentro del DRP, pero no fue posible obtener resultados ya que no contaban con la disponibilidad del correo institucional por falta de renovación de las licencias del correo institucional.

- ✓ El centro de datos de la GDC no contaba con la identificación de los riesgos potenciales existentes dentro de su operación, y de la existencia de procesos y procedimientos que les permita la gestión de los riesgos potenciales.

- ✓ Dentro del desarrollo de esta propuesta se identifico bajo interés en materia de inversión en las TIC para mejorar la administración de los servicios del centro de datos de la GDC por la falta de recursos económicos que les permita el sostenimiento de esta área.

- ✓ Dentro de las actividades realizadas con los funcionarios de la GDC, no se identifico un plan estratégico de las tecnologías de Información PETI y framework de arquitectura empresarial que les permita la gestión de los servicios de forma eficaz en los procesos de continuidad de negocio y administración de recursos tecnológicos que apoyan la seguridad de la información.

9 CONCLUSIONES

- ✓ El Modelo de Seguridad y Privacidad de la Información creado por el Ministerio de las TIC es una estrategia apropiada y acorde a las buenas prácticas de seguridad que emplean los estándares de seguridad internacionales, ofreciendo componentes adecuados para garantizar una alta disponibilidad en los servicios de TI de la GDC. A continuación, se describen algunas guías sugeridas por MinTIC del MSPI para la GDC (MinTIC, mintic.gov.co 2017):

  - Guía 2, Política General MSPI v1.
  - Guía 4, Roles y responsabilidades.
  - Guía 5, Gestión y clasificación de Activos.
  - Guía 7, Gestión del Riesgo.
  - Guía 10 Continuidad de Negocio.

- ✓ La identificación de los activos de información administrados por el grupo TIC y las responsabilidades dentro del centro de dato de la GDC permitió obtener información relevante de los riesgos potenciales del servicio de las TIC y el alcance que deben tener para contar con una alta disponibilidad del servicio como lo sugiere el MSPI del MinTIC.

- ✓ Contar con políticas de seguridad y políticas de administración de las TIC en la GDC brinda un alto grado de protección de los datos y activos de información contra las diferentes amenazas existentes la red publica.

- ✓ Al realizar el diseño del Plan de Recuperación de Desastres informático en la GDC se definen los tiempos de recuperación de eso recursos considerados críticos en las actividades esenciales para brindar una respuesta oportuna en el momento de un evento disruptivo antes de llegar a un colapso organizacional.

- ✓ La realización de la etapa de identificación y Análisis de riesgos, después de emplear la estrategia del Análisis de Impacto del Negocio BIA, permitió desarrollar la estrategia adecuada a las necesidades para la administración de los recursos tecnológicos en el centro de datos de la GDC con un balance de reducción de los riesgos significativos; Además, permitió establecer cuales serian las prioridades en los procesos de recuperación de los servicios.

- ✓ La ejecución de este trabajo es viable y alcanzable ya que se puede ejecutar la cuarta fase de la ISO 22301:2012 como estrategia para mitigar los diferentes riesgos identificados en la Etapa de Análisis y así contar con equipo de seguridad comprometido en la administración de la seguridad de la información en la GDC.

- ✓ La estrategia del plan de recuperación de desastres, ofrece al Grupo TIC de la GDC un marco de referencia en respuesta a los eventos disruptivos que se puedan presentar en los sistemas de TI de la GDC.

- ✓ Con la implementación de este trabajo, el centro de datos de la GDC demostrará a la alta dirección el grado de importancia que debe tener el área de las TI en el manejo de los recursos tecnológicos de la GDC; además, cabe resaltar que las alternativas identificadas en este trabajo aportan en la reducción de riesgos potenciales de activos de información de forma significativa.

10 REFERENCIAS

10.1 Bibliografía

ACOSTA, hector alfonso. «diseño de un plan de contingencia del sistema de información para la entidad itrc.» *repository.unad.edu*, 2017: https://repository.unad.edu.co/bitstream/10596/13868/1/19306734.pdf.

Alcaldiabogota. «decreto.» *decreto, (2012). decreto 2693 de 2012*, 2012: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=51198.

Alcaldiabogota. «ley 1266.» *ley (2008). ley estatutaria 1266 de 2008*, 2008: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488.

Alcaldiabogota. «ley 1273.» *ley 1273, (2009). ley 1273 de 2009. Bogotá, Colombia*, 2009: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

Alcaldíadebogotá. «ley estatutaria 1581.» *ley 1581 estatutaria (2012)*, 2012: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

Arévalo, ligia patricia. «repository.ucatolica.» *Trabajo de Grado*. 2016. http://repository.ucatolica.edu.co/bitstream/10983/13914/4/trabajo%20de%20grado.pdf.

Berman, Joel. «Acronis.» *Simplifique sus copias de seguridad* , 2017: 22.

Boyaca. «www.boyaca.gov.co.» *Gobernación de Boyaca*. 31 de Julio de 2017. https://www.boyaca.gov.co/images/politicas/politica_continuidad_servicios_ti%202017.pdf.

Bustamante, Giovanny. «Metodología de la seguridad de la información como medidade protección en pequeñas empresas.» *Activa*, 2014: http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202/206.

decreto1377. «alcaldiabogota.gov.» *Alcaldía de Bogotá*. 2013. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

Ferrer, Rodrigo. «Metodología para la Gestión de la Continuidad del Negocio.» *cintel.org.co*, 2015: https://cintel.co/wp-content/uploads/2013/05/Metodolog%C3%ADa-para-la-Gesti%C3%B3n-de-la-Continuidad-del-Negocio.pdf.

Gobernación_Del_Chocó. «Nuestra Gobernación ¿Quiénes somos?» *Gobernación del Departamento del Chocó*. 2017. http://www.choco.gov.co/quienes_somos.shtml (último acceso: 2017).

ICONTEC - NTC-ISO31000:2009, Norma Técnica de Colombia. «icontec internacional.» *Gestión del Riesgo - Principios y Directrices - ISO31000:2009.* 16 de 02 de 2011. https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf (último acceso: febrero de 2018).

ICONTEC. «norma técnica ntc-iso-iec colombiana 27001.» *tienda.icontec.org/*, 2013: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.

ICONTEC. «NTC-ISO 22301:2012.» *tienda.icontec.org*, 2012: https://tienda.icontec.org/wp-content/uploads/pdfs/NTC5722.pdf.

isaca. *isaca.org.ar*. Colombia: ISACA Certified, 2013.

ISO/IEC27001. *ISO/IEC 27001:2013.* 2013. http://www.iso27001security.com/html/27001.html.

ISO27000. «Sistema de Gestión de la Seguridad de la Información.» *ISO 27000*, 2014: http://www.iso27000.es/download/doc_sgsi_all.pdf.

Loján, Ernesto Max. «Modelo de Evaluación de Gestión de Continuidad del Negocio basado en la norma ISO 22301:2012.» *http://repositorio.uees.edu.ec/handle/123456789/1433?mode=full*, 2017-02: 3.

MinTIC. «Decreto 1078.» *decreto, (2015). decreto numero1078 del 2015*, 2015: http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf.

MinTIC. «Decreto 2693 de 2012.» *Decreto 2693*, 2012: https://www.mintic.gov.co/portal/604/w3-article-3586.html.

MinTIC. «mintic.gov.co Guia 05.» *Guía para la Gestión y Clasificación de Activos de Información.* 2017. https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf (último acceso: 2017).

MinTIC. «mintic.gov.co Guía 07.» *Guía de gestión de riesgos.* 2017. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

MinTIC. «mintic.gov.co Guia 10.» *Seguridad y Privacidad de la Información.* 2017. http://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf.

MinTIC. «mintic.gov.co Guía 11.» *Seguridad y Privacidad de la Información.* 2017. https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf.

MinTIC. «Políticas de Seguridad.» *Seguridad y Privacidad de la Información, Guia 2*, 2017: http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf.

MinTIC. *mintic.gov.co.* 2017. https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Obaid. *https://defaultreasoning.com.* 11 de 12 de 2013. https://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/ (último acceso: enero de 2018).

Reavis, Jim. *Qulays, Inc.* 30 de 7 de 2019. https://www.qualys.com/apps/asset-inventory/.

Superintendecia_de_Sociedades. «Supersociedades.gov.» *guia: Plan de Recuperación ante Desastres – DRP - Gestión_de_Infraestructura*,. 06 de Diciembre de 2011. https://www.supersociedades.gov.co/nuestra_entidad/Planeacion/SistemaIntegradode%20Gestion/Documentos%20Infraestructura/documentos/ginf-g-010%20Guia_%20DRP.pdf.

Swanson. «csrc.nist.gov.» *csrc.nist.gov sp_800_34_rev_1.* Mayo de 2010. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf (último acceso: enero de 2018).

Technologie, New. *nariño.gov.co.* 2015. https://xn--nario-rta.gov.co/inicio/files/GestionAdmnistrativa/Politicas/poltica_seguridad_y_privacidad_de_la_informacin-gobnar-V1_3-2014.pdf.

Tellez, Carlos Andres. «red.uao.edu.co - diseñar un plan de continuidad del negocio en el proceso de administracion de recursos de ti de la oficina de informatica y telematica de la alcaldia de santiago de cali.» *red.uao.edu.co.* 2015. https://red.uao.edu.co/bitstream/10614/8037/1/T06040.pdf (último acceso: 2017).

unisdr. «unisdr.org.» *unisdr.org Campaña Mundial 2010-2015.* 2012. http://www.unisdr.org/files/26462_manualparalideresdelosgobiernosloca.pdf.

Villamil, Leoncio Felipe. «repository.unimilitar.edu.co.» *http://repository.unimilitar.edu.co.* 2012. http://repository.unimilitar.edu.co/bitstream/10654/10790/1/trabajo%20de%20grado%20especializacion%20en%20alta%20generencia%20umng.pdf.

11 ANEXO 1

Anexo A. Acta de reunión de adopción de las políticas de seguridad de la información de la GDC. Tomado de la *(Gobernación_Del_Chocó 2017)***.**

UNIDOS
Construyendo Desarrollo GOBERNACIÓN DEL CHOCÓ

REPUBLICA DE COLOMBIA
DEPARTAMENTO DEL CHOCO
NIT 891.680.010-3
DESPACHO DEL GOBERNADOR DEL CHOCO

RESOLUCION Nº DE 2014

Por medio del cual se adoptan las políticas de seguridad de la información de la gobernación del departamento del choco

EL GOBERNADOR DEL DEPARTAMENTO DEL CHOCO

En uso de sus atribuciones constitucionales y legales en especial las conferidas en el Numeral 3º Articulo 316 de la Constitución, y el Literal d, Numeral 7º del Articulo 91 de la Ley 136/1994, la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto Nº 4107 de 2011, demás normas concordantes y:

CONSIDERANDO:

1. Que la Gobernación del Departamento del Choco siguiendo los lineamientos de la Estrategia de Gobierno en Línea de la Republica de Colombia, cuyo propósito es contribuir a la construcción de un estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC, y que uno de los componentes es el Modelo de Seguridad de la Información, el cual debe definir unas políticas que permitan proteger la información de la Entidad, datos personales y sus activos de la información.
2. Que la Gobernación del Departamento del Choco, debe garantizar un manejo adecuado de sus activos de información, salvaguardando su integridad, confidencialidad y disponibilidad.
3. Que la Gobernación del Departamento del Chocó define políticas de seguridad de la Información, con el fin de establecer responsabilidades y establecer criterios mínimos en el manejo de los activos y la aplicación de buenas prácticas.
4. Que mediante acta Nº 05 del 03 de julio de 2013, el comité de gobierno en línea aprobó la política de seguridad de la Información.

REPUBLICA DE COLOMBIA
DEPARTAMENTO DEL CHOCO
NIT 891.680.010-3
DESPACHO DEL GOBERNADOR DEL CHOCO

Con fundamento en los anteriores considerandos el Gobernador del Departamento del Chocó.

RESUELVE

ARTICULO PRIMERO: Adoptar la Política de Seguridad de la información el cual fue aprobada por el Comité de Gobierno en Línea Territorial GEL, mediante acta de reunión Nº 05 del 03 de julio de 2013 donde señalo lo siguiente.

El Departamento del Chocó protegerá la Información generada, procesada o resguardada por los procesos estratégicos, misionales y de apoyo de la Entidad, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej. : proveedores o clientes), o como resultado de un servicio interno en outsourcing.

El Departamento del Chocó protegerá la Información creada, procesada o resguardada por sus procesos de negocios con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta, para es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

El Departamento del Chocó protegerá su información de las amenazas originadas por parte del personal.

El Departamento del Chocó protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

Anexo B. Portafolio de servicios y manual de procesos y procedimientos para las responsabilidades en la Gestión TIC de la GDC. Tomado de *(Gobernación_Del_Chocó 2017)*

SECRETARÍA DE PLANEACIÓN Y DESARROLLO ÉTNICO TERRITORIAL – TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
II. PROPÓSITO PRINCIPAL
Participar en la formulación, desarrollo e implementación de políticas, estrategias, planes programas, proyectos, estudios y demás estrategias que involucren las tecnologías de información y comunicaciones del Departamento del Chocó dentro del marco constitucional y legal, mediante la proyección de estudios, informes y otros documentos que tiendas a conseguir los propósitos de la dependencia, así como de participar activamente en los programas, planes o campañas que organice la misma.
III. DESCRIPCIÓN DE FUNCIONES ESENCIALES
6. Participar en la preparación y formulación mediante la proyección de estudios, informes y otros documentos del Plan Estratégico de Tecnologías de la Información, las Comunicaciones y Gestión del Conocimiento de la Gobernación, así como en la ejecución del mismo siguiendo las pautas y lineamientos establecidos. 7. Proyectar estudios y documentos que busquen determinar las necesidades que en materia de Tecnologías de la Información, las Comunicaciones y Gestión del Conocimiento requiera la Gobernación. 8. Apoyar la administración de los procesos de operación, mantenimiento y actualización del hardware y software adquirido e implantado para las diferentes dependencias. 9. Participar en el asesoramiento y apoyo a las diferentes dependencias de la Gobernación sobre el uso de los equipos de cómputo, procesamiento de datos, programas y aplicaciones y demás aspectos básicos para la correcta utilización de los sistemas y recursos informáticos, mediante la proyección de estudios, informes y otros documentos. 10. Desarrollar las aplicaciones que requieren las dependencias de la Gobernación para mejorar la efectividad del servicio. 11. Ejecutar el Plan de Capacitación para fortalecer la cultura informática de los servidores de la Gobernación mediante la proyección de estudios, informes y otros documentos.

12. Las demás que se le asignen conforme a la naturaleza del cargo.
IV. CRITERIOS DE DESEMPEÑO
1. El asesoramiento y el apoyo que el grupo le hace a todas las dependencias de la Gobernación y los municipios del Departamento en la formulación, desarrollo e implementación de las políticas, estrategias, planes, programas y proyectos relacionados con los sistemas de tecnologías de informática y comunicaciones debe hacerse en cumplimiento de los estándares nacionales en materia de TICs y de información pública así como en coordinación con la Jefatura de Gabinete. 2. Las necesidades que en materia de Tecnologías de la Información, las Comunicaciones y Gestión del Conocimiento requiera la entidad y el desarrollo de las mismas se debe estructurar de manera transversal en la Gobernación incluyendo todas sus entidades. 3. Los estudios y documentos que busquen determinar las necesidades que en materia de Tecnologías de la Información, las Comunicaciones y Gestión del Conocimiento requiera la entidad, se proyectan con regularidad y se actualizan constantemente 4. El asesoramiento y el apoyo a las diferentes dependencias de la Gobernación sobre el uso de los equipos de cómputo, procesamiento de datos, programas y aplicaciones y demás aspectos básicos para la correcta utilización de los sistemas y recursos informáticos debe hacerse de manera global y organizada incluyendo a todos los funcionarios de la Gobernación. 5. Las aplicaciones que requieren las dependencias de la Gobernación para mejorar la efectividad del servicio, se desarrollan de manera oportuna. 6. El Plan de Capacitación para fortalecer la cultura informática de los servidores de la Gobernación mediante la proyección de estudios, informes y otros documentos, se ejecuta de acuerdo a lo programado.
V. RANGO DE APLICACIÓN
▪ Tipo de Entidad: Entidades, organismos del nivel departamental y municipal. ▪ Información: Verbal, Telefónica, Virtual (Chat, e-mail, teleconferencia, Foro Virtual). ▪ Comunicaciones Utilizadas: Escrita, Digital, Verbal y Presencial de modo o variación: Clientes internos y externos.
VI. CONOCIMIENTOS BÁSICOS O ESENCIALES
▪ Lenguajes de programación. ▪ Administración de recursos. ▪ Canales de información, medios de comunicación y sistemas. ▪ Recursos multimedia, informáticos y virtuales.

Anexo C. Relaciones de los resultados del gobierno de seguridad con las responsabilidades gerenciales, tomado de (isaca 2013). Tomado de *(isaca 2013)***.**

Niveles de Gestión	Alineación estratégica	Gestión de riesgos	Entrega de valor	Medición del desempeño	Gestión de recurso	Aseguramiento del proceso
Concejo de Dirección	Requiere de una alineación comprobable	-Establece tolerancia al riesgo. -Supervisa una política de riesgo. -Supervisa el cumplimiento de las normas reguladoras.	Requiere reportar los costos de las actividades relacionadas con la seguridad.	Requiere reportar la eficacia de la seguridad.	Supervisa política de gestión del conocimiento y utilización de recursos.	Supervisa políticas para la integración de proceso de aseguramiento.
Dirección ejecutiva	Instituye procesos para integrar a la seguridad en los objetivos de negocio.	-Verifica que los roles y responsabilidades incluyan la gestión del riesgo en todas sus actividades. -Supervisa el cumplimiento de las normas reguladoras.	Requiere estudios de business case (caso de negocio) de las iniciativas de penalidad.	Requiere monitoreo y métricas para las actividades de seguridad.	Garantiza la ejecución los procesos para captar conocimiento y métricas de eficiencia.	Supervisa todas las funciones de aseguramiento y planes de integración.
Comité directivo	-Revisa y presta asistencia en la estrategia de seguridad e integración. -Garantiza que la integración cuente con el apoyo de los dueños del negocio.	Identifica los riesgos emergentes, promueve las prácticas de la seguridad de la unidad de negocio.	Revisa y asesora sobre la suficiencia de las iniciativas de seguridad para ayudar a las funciones de negocio	Revisa e informa que las iniciativas de seguridad cumplan con los objetivos del negocio.	Revisa los procesos para captar y difundir conocimientos.	-Identifica procesos de negocio críticos y proveedores de aseguramiento. -Dirige los esfuerzos de la integración del aseguramiento.
Director de seguridad	Desarrolla la estrategia	-Garantiza que se realicen las	Monitorea la utilización	Desarrolla e	Desarrolla tanto métodos	-Se comunicada con otros

de información	de seguridad; vigila el programa y las iniciativas de seguridad, y se coordina con los dueños de proceso de negocio para una alineación constante.	evaluaciones de riesgo e impacto al negocio. -Desarrolla estrategias de mitigación de riesgos. Hace cumplir las regulaciones y las políticas.	y la eficiencia de los recursos de seguridad.	implementa enfoques de monitoreo y métricas y dirige y monitorea las actividades de seguridad.	para captar y difundir el conocimiento, como métricas para determinar la eficacia y la eficiencia.	proveedores de aseguramiento. -Garantizan que se identifiquen y resuelvan las brechas y los vacíos y superposiciones.
Ejecutivo de auditoria	Evaluar y reportar el grado de alineación	Evaluar e informar sobre los riesgos corporativos prácticas de gestión y resultados.	Evaluar y reportar sobre la eficiencia.	Evaluar e informar sobre la eficiencia o de recursos.	Evaluar y reportar sobre la eficiencia o la gestión de recursos.	Evaluar y reportar sobre eficacia sobre los procesos de aseguramiento realizado por las diferentes áreas de la gerencia.

Anexo D. Oferta del mantenimiento a distancia del Sistema de Información PCT ENTERPRISE. Tomado de la *(Gobernación_Del_Chocó 2017)***.**

Oferta de Mantenimiento a distancia Sistema de Información PCT ENTERPRISE - 2018

PA019-2018

Bogotá, 11 de enero de 2018

Señores
GOBERNACION DE CHOCO
Quibdó

Referencia: Actualización y Soporte Técnico a Distancia del Sistema PCT ENTERPRISE

Cordial saludo,

Dejo a su disposición la propuesta para mantenimiento a distancia del sistema de Información PCT Enterprise – 2018, teniendo en cuenta nuestro actual convenio y el trabajo que hemos venido haciendo durante este tiempo.

Es de su conocimiento nuestra experiencia en el Sector Público y nuestras fortalezas para brindar a ustedes la confianza y tranquilidad al momento de relacionarse con nuestro sistema.

PCT LTDA continúa afianzando el reconocimiento y credibilidad con el cumplimiento de requisitos legales y jurídicos necesarios para la contratación estatal, y a través de nuestras entidades clientes que como Ustedes, han entregado su confianza en nuestra compañía para darnos la oportunidad de ofrecer un excelente servicio, garantizando así un alto nivel de calidad y competencia en nuestro campo.

En esta propuesta encontrará el valor del mantenimiento a distanciay garantías correspondientes.

Estaremos atentos a sus observaciones para el mejoramiento del servicio y atención a nuestros clientes.

Atentamente,

GERMAN ALBERTO LINARES ROMERO
Presidente

CUADRO No. 7 OBLIGACIONES DE LA ENTIDAD CONTRATANTE *Compromisos adquiridos por la entidad contratante al momento de recibir mantenimiento a distancia por parte de* ***PCT LTDA.***
1. La entidad debe suministrar al personal de PCT LTDA el tiempo de computador y las herramientas necesarias tales como: personal, DBA (Ingeniero administrador de base de datos) e ingenieros desarrolladores para migraciones, papelería, discos magnéticos, y las instalaciones para la realización de las visitas contempladas.
2. La entidad asume todos los procesos relacionados con la administración de bases de datos, licenciamiento, instalación, configuración, afinamiento, migración, conexión de equipos clientes (si se requiere), copias de seguridad, planes de contingencia y demás relacionados.
3. La entidad se responsabiliza de mantener los motores de base de datos con versión actualizada y el servicio respectivo a la versión instalada de base de datos.
4. La entidad debe atender a las indicaciones y planes de trabajo que asigne el (los) Ingeniero(s) de PCT LTDA de acuerdo con el diagnóstico que se deje escrito en el reporte de la visita.
5. La entidad es responsable de aplicar en la base de datos las instrucciones de mantenimiento a distancia que PCT requiera para la operación de los aplicativos.
6. La entidad debe mantener como mínimo una copia de seguridad diaria, semanal y mensual de los archivos de datos en medios magnéticos de almacenamiento externo. PCT LTDA no se hace responsable del NO CUMPLIMIENTO de las copias mencionadas anteriormente.
7. La entidad debe cancelar en el plazo el valor estipulado.

CUADRO No. 9 ANULACIÓN DE LA GARANTÍA DEL SISTEMA PCT ENTERPRISE
Razones por las cuales la garantía queda totalmente inhabilitada
La garantía se pierde en el momento que se compruebe que ha existido intervención de los funcionarios de la entidad o de terceras personas en la configuración externa de los programas y/o manipulación de la base de datos.
Aclaración
La manipulaciónde los objetos, procedimientos, datos de la base de datos oprocesos ejecutadossin autorización puede generar información no coherente,loque deja a PCT LTDA fuera de toda responsabilidad.

CUADRO No. 10 VALOR CONVENIO MANTENIMIENTO A DISTANCIA DEL SISTEMA PCT – ENTERPRISE

El siguiente cuadro evidencia el costo de la inversión del producto adquirido por parte de la entidad contratante teniendo en cuenta que el precio variara dependiendo de la necesidad de cada entidad.

DESCRIPCIÓN	VALOR UNITARIO
Actualización del Sistema PCT Enterprise	$31.325.000
Soporte Técnico a Distancia del Sistema Gráfico Sistema PCT Enterprise	$46.988.000
SUBTOTAL COSTOS DE INVERSION	**$78.313.000**
IVA 19% (Exento de IVA, reforma tributaria Ley 1819 de 2016 Art 187 Numeral 24)	$0
TOTAL COSTOS DE INVERSION	**$78.313.000**

SON: SETENTA Y OCHO MILLONES TRECIENTOS TRECE MIL PESOS M/CTE.

15 Módulos y Submódulos Licenciados

CUADRO No. 15 MODULOS Y SUBMODULOS LICENCIADOS SISTEMA PCT ENTERPRISE

En el siguiente cuadro encontrara la relación de módulos / sub módulos para el mantenimiento a distancia teniendo en cuenta que los mismos cambiaran dependiendo de la necesidad de cada entidad.

SISTEMA FINANCIERO	
MÓDULO PRESUPUESTO	módulo de apropiación
	Submódulo de solicitudes de CDP
	Submódulo Presupuesto de Ingresos
	Submódulo Presupuesto de Gastos
	Submódulo Plan anual de caja P.A.C.
MÓDULO CONTABILIDAD	Submódulo de contabilidad
	Submódulo Causación
	Submódulo Información Exógena (Informes DIAN).
	Submódulo de Integración
MÓDULO CENTRAL DE CUENTAS	Submódulo de Central de cuentas
	Submódulo de legalizaciones
MÓDULO TESORERÍA	Submódulo de Egresos
	Submódulo de Ingresos
	Submódulo de Conciliaciones Bancarias
	Submódulo de Entrega de Cheques
SISTEMA RECURSO FÍSICO	
	Submódulo de almacén
	Submódulo de órdenes de suministro
	Submódulo de solicitudes
SISTEMA DE BIENES INMUEBLES	
	Submódulo Bienes Inmuebles
SISTEMA MODULO DE CONTRATACION	
	Submódulo Contratación
SISTEMA DE RENTAS DEPARTAMENTALES	
	Submódulo de Rentas Departamentales
	Submódulo de Cartera
MÓDULOS TRANSPARENCIA WEB	
MODULO DE CONSULTAS WEB	
MODULO ADMINISTRACION DEL TRIBUTO	
MODULOS COMPLEMENTARIOS	
	Submódulo de Seguridad
	Submódulo de Herramientas
	Submódulo de Consultas
	Submódulo de Transparencia
	Submódulo SIG
OTROS MODULOS DE USO OPCIONAL	
Submódulo de Informes Entes de Control CGR y FUT	
Submódulo de INFOSIA	

Anexo E. Objetivo de mantenimiento a distancia del Software de Nomina de empleados y Pensionados (por contrato). Tomado de la *(Gobernación_Del_Chocó 2017)*.

Bogotá, 23 de Enero del 2018

Señores:
GOBERNACIÓN DEL CHOCÓ
Colombia

Estimados Señores:

Tenemos el agrado de dirigirnos a ustedes con la finalidad de saludarlos y, a su vez, remitirles adjunto a la presente, la propuesta prestación del servicio de mantenimiento a distancia del programa de Nomina de Empleados y Pensionados ("SIAN") instalado en la Gobernación.

El mencionado programa implementado y actualmente, se encuentra en operación en la Entidad, apoyando de manera vertical el manejo de su nómina. Asimismo, esta propuesta incluye la integración presupuestal y contable con el software financiero que la Gobernación tiene instalado. De igual forma, la presente remisión se produce en virtud de su invitación para presentar la presente oferta.

Cualquier inquietud con relación a éste documento, por favor, no dude en comunicarse con nosotros, estamos gustosos a resolverla con la mayor brevedad.

Cordialmente,

Atentamente.

Jorge Martínez Mimbela
Representante Legal
Solredes SAS

solredes
desarrollando e innovando tu futuro

solredes s.a.s
secretaria@solredes.bi
www.solredes.co
Tel. (+57 1) 4572609 Cel. (+57) 318649559
Diagonal 61 B No. 26-21 Ofi. 20

1. OBJETO DE LA PROPUESTA.

Brindar el mantenimiento a distancia del programa de Nomina de Empleados y Pensionados, que actualmente tiene nuestra empresa en operación para el pago de los funcionarios de su Gobernación.

A continuación se relacionan el alcance de los aspectos básicos de la propuesta:

1.1 ALCANCE DEL SERVICIO DE MANTENIMIENTO A DISTANCIA DE NOMINA

El servicio de mantenimiento a distancia antes descrito abarcará las siguientes prestaciones:

- ✓ **Mantenimiento evolutivo**: el cual incluye las actualizaciones del programa en alguno de los módulos instalados por nuestra empresa, que incorporarán los cambios a la normativa vigente.
- ✓ **Mantenimiento correctivo:** el cual incluye las correcciones por fallas detectadas en la operación y utilización del programa licenciado a fin de tener la correcta operación del sistema de nómina de empleados y pensionados.
- ✓ Brindar **mantenimiento a distancia y asesoría técnica** a los usuarios en la utilización y administración de la aplicación.
- ✓ Brindar el mantenimiento **preventivo** durante la operación del programa de nómina SIAN: Este mantenimiento a cargo de Solredes será para la totalidad de los componentes licenciados de la Gobernación, así como para la totalidad de procesos que se ejecutan en función de la gestión de pago de las mesadas pertinentes.
- ✓ Consultas por internet mensuales, presentando al Supervisor del Contrato los informes de resultados, las observaciones y recomendaciones a que haya lugar.
- ✓ Asignar el personal calificado necesario para garantizar la oportuna puesta en producción de los cambios normativos o procedimentales que se presenten durante la ejecución del contrato.
- ✓ Parametrizar en el aplicativo, los cambios normativos en materia de Retención en la Fuente, emitidos por el Gobierno Nacional.
- ✓ Presentar los informes, las facturas y otros documentos de control al Supervisor del contrato para la verificación de la ejecución del contrato y proceder al pago respectivo.
- ✓ De igual forma, la integración presupuestal y contable con el software financiero que maneja la Gobernación.
- ✓ Generación de los siguientes reportes:

  - ➢ ARL.
  - ➢ RESUMEN BANCOS
  - ➢ RESUMEN DETALLADO BANCOS
  - ➢ CERTIFICADO DE INGRESOS Y RETENCIONES
  - ➢ DEDUCIDOS FUNCIONARIOS POR CONCEPTO
  - ➢ DEVENGADOS FUNCIONARIOS POR CONCEPTO
  - ➢ PRENOMINA
  - ➢ EMBARGOS POR JUZGADOS

4. PROPUESTA ECONÓMICA

El valor de la propuesta esta discriminado así:

DESCRIPCIÓN DE ITEMS	VALOR
Mantenimiento a distancia del programa de Nomina de Empleados y Pensionados hasta el 31 de Diciembre de 2018.	**$40.280.000**
NO APLICA IVA (19%) – Ver Nota 1-	**$0**
VALOR TOTAL PROPUESTA INCLUIDO IVA (19%)	**$40.280.000**

Nota 1: En la Reforma Tributaria Ley 1819 de 2016, se adicionó el numeral 24 al artículo 476 del Estatuto Tributario, el cual manifiesta que los servicios de "mantenimiento a distancia de programas" quedan excluidos del impuesto sobre las ventas (IVA).

Nota 2: En caso la Gobernación requiera más servicios y/o servicios adicionales, Solredes cobrará el monto indicado en el punto 2.

4.1 Validez de la oferta

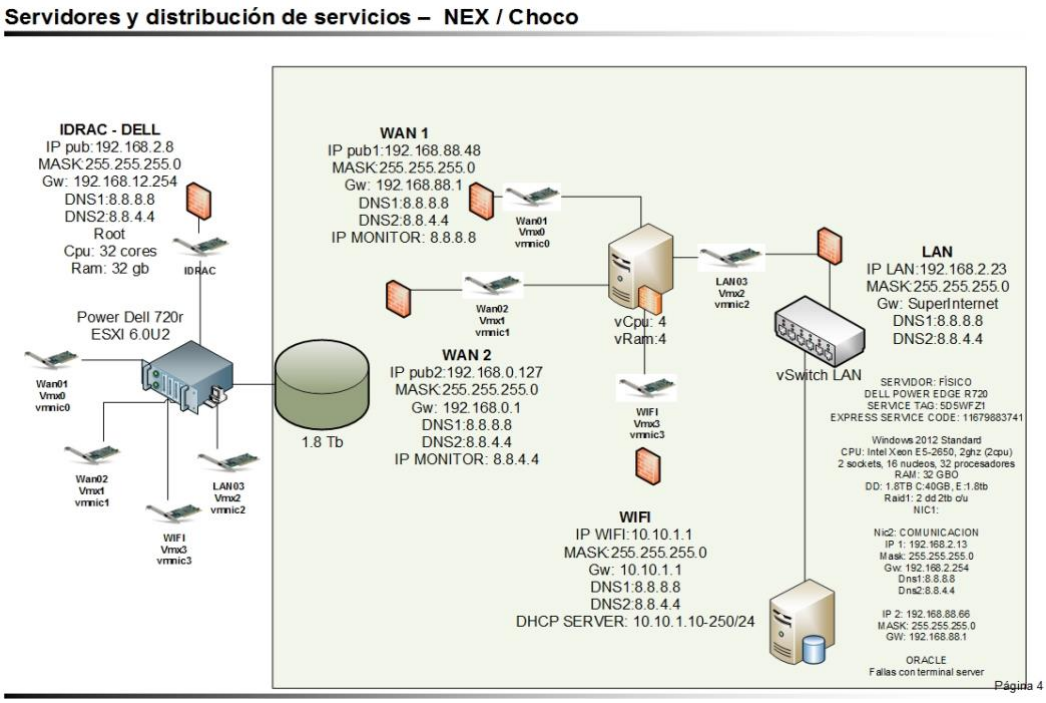
Treinta (30) días calendario.

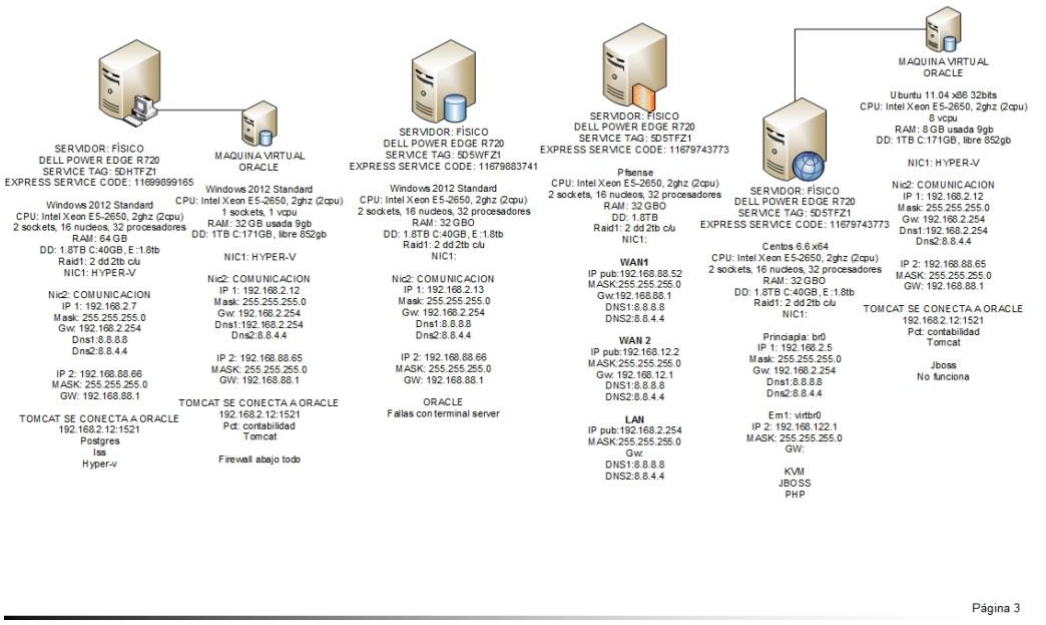
5. FORMA DE PAGO.

La forma de pago del monto total ($40.280.000) es la siguiente:

1. El 40% del monto del contrato contra la firma del mismo, entrega de cronograma (de ser, el caso) y firma de Acta de Inicio.
2. El 30% al quinto mes de la firma del contrato.
3. El 25% al octavo mes de la firma del contrato.
4. El 5% contra la firma del Acta de Liquidación del contrato.

Anexo F. Esquema de Red e infraestructura de la GDC. Servidores y distribución de servicios – NEX / Chocó. Tomado de la *(Gobernación_Del_Chocó 2017)*.





Anexo G. Roles y responsabilidades para la gestión del DRP en la GDC.

Matriz de Asignación de Responsabilidades (RACI)

Roles / Responsabilidades: **R:** Comprometido, **A:** Responsable, **C:** Consultado, **I:** Informado, **S**: Soporte, **Q**: Qualys

Actividad		Roles / Responsabilidades					Roles / Responsal
ID Actividad	Actividad	Coordinador (Harlen Ibarguen)	Lider de Sistemas (Andres Mosquera)	Lider de Infraestructura (Yosimar Palacio)	Practicantes (SENA)	Secretaria de Planeación	Auditor Interno (Revisoria)
1	Selección de Estrategias de respaldos y definición de roles para las actividades del DRP.	**AC**	**R**	**R**	**I**	**C**	**Q**
2	Gestión y clasificación de Activos (Ver ítem 6.1.6) del DRP	**A**	**R**	**R**	**S**	**I**	**Q**
3	Divulgación y creación de politicas generales para la gestión del DRP	**RA**	**R**	**R**	**I**	**C**	**Q**
4	Proceso y gestión de sensibilización de buenas practicas de seguridad	**RA**	**R**	**R**	**S**	**I**	**Q**
5	Mesa de atención de incidentes de seguridad	**RA**	**R**	**R**	**R**	**C**	**Q**
6	Administración y Gestión del Riesgo (Ítem 6.3) del DRP	**RA**	**R**	**R**	**S**	**I**	**Q**
7	Activación del plan en caso de emergencia (ver 6.1.5.1)	**AC**	**R**	**R**	**R**	**I**	**Q**
8	Gestión de Respaldo	**RA**	**R**	**R**	**S**	**I**	**Q**
9	Mejora continua del DRP en la GDC	**RA**	**R**	**R**	**S**	**I**	**Q**