Contraloría General del Departamento del Cesar

Compromiso con la verdad

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022 - 2025

Elaboró	Revisó	Aprobó
Patricia Alvarez Ortega Profesional Universitario G1	Helene Gomez Monsalve Contralora Auxiliar	Juan Francisco Villazon Tafur Contralor General del Departamento del Cesar
Fecha: Enero 26 2022	Fecha: Enero 26 2022	Fecha: Enero 26 2022

TABLA DE CONTENIDO

INTRODUCCIÓN

La Contraloría General del Departamento del Cesar, tiene la misión de vigilar de manera oportuna, eficiente, eficaz y transparente con la participación de la ciudadanía, la gestión fiscal de la administración departamental, sus entidades descentralizadas, municipios y de los particulares que manejen o administren fondos o bienes públicos en el orden departamental, garantizando que los sujetos de control cumplan con el fin y la función social para los cuales fueron creados, bajo la observancia de los fines esenciales del estado.

Para lo anterior, se ha provisto de los medios humanos y técnicos a fin de optimizar sus actuaciones mediante la modernización e integración sus procesos, usando las tecnologías de la información y la comunicación. Dicha interacción, crea una interdependencia expuesta a riesgos previsibles y manejables, que pueden afectar en diferente proporción aquellas funciones apoyados en TI.

El siguiente plan estructura un conjunto políticas y procedimientos a fin de Anticipar el impacto que tendría, en la cadena de valor y el desarrollo de su objeto misional, la materialización del riesgo asociación a la arquitectura de servicios tecnológicos.

1. OBJETIVOS

OBJETIVO GENERAL

Definir los lineamientos y/o procedimientos para analizar, valorar y tratar los riesgos de seguridad de la información.

OBJETIVOS ESPECÍFICOS

- ✓ Identificar las aplicaciones y plataformas TI consideradas críticas para la operación de la Contraloria General del Departamento del Cesar.
- ✓ Identificar las amenazas que afectan a los activos informáticos y por ende la continuidad de los procesos misionales y funcionales.
- ✓ Establecer las acciones y/o procedimientos a seguir en caso de ocurrencia de un siniestro que restrinja el acceso a los sistemas informáticos.

2. ALCANCE DEL DOCUMENTO

El Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información, será aplicado y cumplido por parte de todos los funcionarios de la Contraloría General del Departamento del Cesar, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad.

3. MARCO NORMATIVO

- **Ley 1437 de 2011**, Capítulo IV, “utilización de medios electrónicos en el procedimiento administrativo”. “Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.”

- **Ley 1581 de 2012**, g) Principio de seguridad: “La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.”

- **Ley 1581 de 2012**, Artículo 17, ítem d: “Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- **Ley 1712 de 2014**, “principio de transparencia”: “Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.”

- **Ley 1712 de 2014**, artículo 7: “Disponibilidad de la información” “En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.”

- **Ley 1712 de 2014** -Título III “Excepciones acceso a la información” “Información exceptuada por daño de derechos a personas naturales o

jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito."

4. DEFINICIONES

- **Acceso a la información Pública:** Derecho fundamental consistente en la facultad que tiene todas las personas de conocer sobre la existencia y acceder a la información pública de posesión o bajo control de sujetos obligados.
- **Amenaza:** es un ente o escenario interno o externo que pues hacer uso de una vulnerabilidad y generar un mal funcionamiento de una organización tanto en su parte tecnológica como humana.
- **Datos:** Los datos son hechos y/o valores que por sí solos carecen de un sentido completo, pero que al ser procesados o agrupados conforman información.
- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Control o medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **CGDC:** Contraloria General del Departamento del Cesar.

5. ANÁLISIS DE IMPACTO DENTRO LA CADENA DE VALOR DE LA CGDC

5.1. IDENTIFICACIÓN DE FUNCIONES Y PROCESOS

La Contraloría General del Departamento del Cesar, adoptó el enfoque basado en procesos, donde las actividades desarrolladas por cada unidad funcional están interrelacionadas e interactúan entre sí transformando los elementos de entrada en resultados, para ello es esencial la asignación de recursos, dicho enfoque permite entre otros:

- Lograr los resultados deseados previstos mediante la integración y alineación de los procesos.
- Ayudar a focalizar los esfuerzos en la eficacia y eficiencia de los procesos.
- Aportar confianza a los usuarios y demás partes interesadas en cuanto al desempeño de la CGDC.
- Ofrecer transparencia en las operaciones de la organización.
- Proporcionar mejores resultados, más coherentes y predecibles.
- Facilitar oportunidades para priorizar las iniciativas de mejora, lo que consigue estimular la participación del personal y la clarificación de sus responsabilidades.

En la siguiente imagen se ilustra la cadena de valor de la CGDC, muestra los procesos estratégicos, evaluadores, misionales y de apoyo.

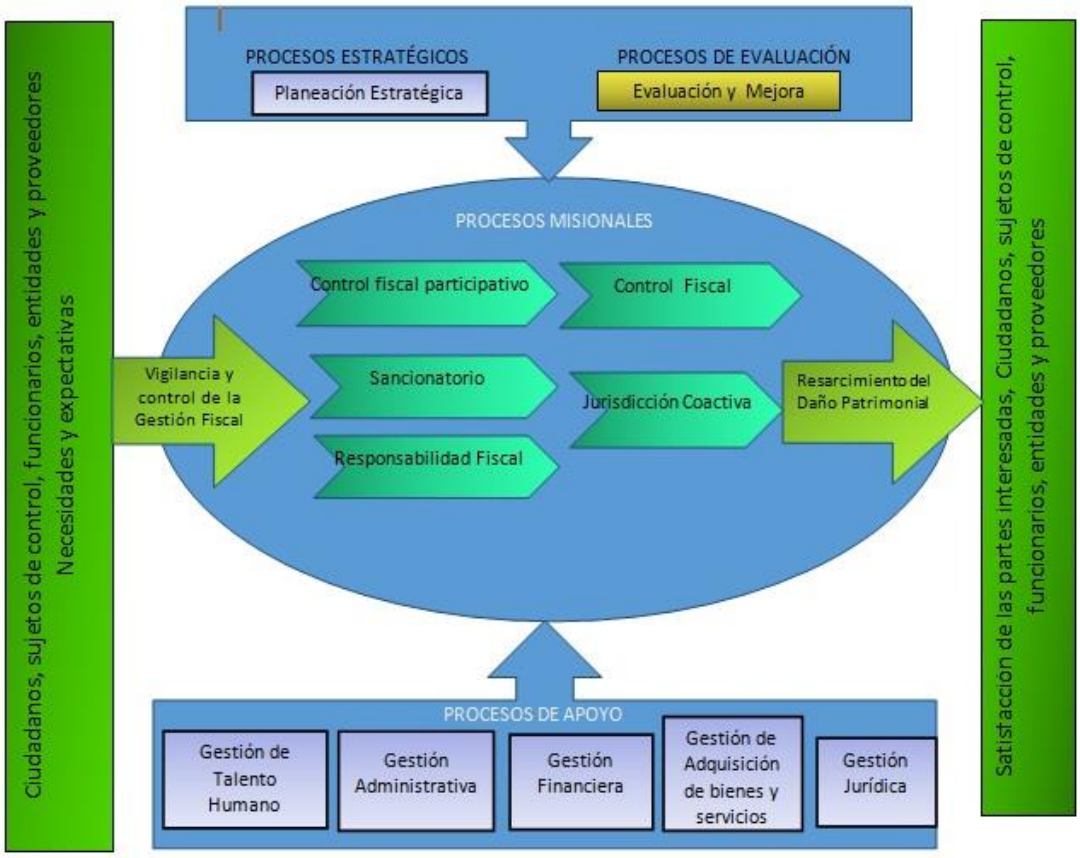

Imagen 1. Mapa de Procesos CGDC

Los procesos misionales son desarrollados por las áreas operativas que adelantan actividades de: Control Fiscal, Control Fiscal Participativo, Sancionatorios, Responsabilidad Fiscal y Jurisdicción Coactiva.

Los procesos de apoyo están conformados por las unidades de que desarrollan labores administrativas tales como: Gestión de Talento Humano, Gestión Financiera, Gestión de Adquisición Bienes y Servicios, Gestión Jurídica.

Finalmente, los procesos de evaluación desarrollan actividades y funciones inherentes al control interno.

Los procesos, antes mencionados, están caracterizaciones de tal manera que permita identificar sus interacciones (entradas, salidas, responsables, proveedor y cliente interno), los criterios (objetivos, indicadores y metas), los métodos (procedimientos y registros), los recursos y la planificación de las actividades de seguimiento y medición (plan de seguimiento de los indicadores).

5.2. DETERMINACIÓN DE PROCESOS Y SISTEMAS CRÍTICOS.

5.2.1. Identificación De Procesos Críticos

La contingencia, es modular en función de la continuidad, por ello el propósito del análisis del impacto sobre las actividades misionales de la CGDC, es identificar y priorizar aquellos procesos que se apoyan en componentes de la arquitectura de servicios tecnológica correlacionado con el nivel de soporte que reciben y caracterizando el efecto sobre la organización en un escenario de no disponibilidad.

En el sentido de lo anteriormente mencionado, Los procesos descritos con anterioridad se apoyan en menor o mayor medida en TI para sostener en niveles tolerables los productos y servicios críticos para el desarrollo misional de la CGDC.

Mediante la estructuración de procedimientos, tecnología e información se generan productos que son desarrollados, compilados y mantenidos a fin de proteger los intereses de las partes interesadas, la reputación, las finanzas, los activos críticos y otros aspectos generadores de valor.

El impacto sobre procesos y su relación con los sistemas permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones de la CGDC; el impacto se medirá utilizando el siguiente esquema de valoración, para lo cual se han definido los siguientes niveles: A, B o C.

Nivel A: La operación es crítica para la CGDC cuando al no contar con ésta, las funciones asociadas a un proceso no pueden realizarse.
Nivel B: La operación es una parte integral en un proceso de la CGDC, al fallar la entidad no se puede operar normalmente, pero la función no es crítica.
Nivel C: La operación no es una parte integral de un proceso de la CGDC.

Al analizar la cadena de valor podemos encontrar los siguientes procesos, los cuales desarrollan funciones que proveen insumos para otras actividades.

PROCESO	DESCRIPCIÓN
Planeación estratégica	Diseñar, implementar ejecutar y hacer seguimiento a la Planificación Estratégica de la entidad para cumplir con la misión institucional, inicia con la formulación de las directrices y lineamientos de direccionamiento de la entidad hasta el seguimiento de la implementación y /o ejecución de los planes y programas para el desarrollo de la misión de la Contraloría Departamental.
Evaluación y Mejora	Verificar el grado de cumplimiento y desarrollo del sistema de control interno, adoptado por la Contraloría, para contribuir al mejoramiento continuo del Sistema y al logro de los objetivos y la misión institucional.
Control Fiscal	Vigilar la gestión fiscal de la administración y de los particulares o entidades que manejen fondos o bienes del estado, promoviendo la eficacia, eficiencia y efectividad del manejo de los recursos públicos.
Responsabilidad Fiscal	Lograr el resarcimiento de los daños ocasionados al patrimonio público cuando en el ejercicio de la gestión fiscal los servidores públicos y particulares, causen por acción u omisión y en forma dolosa o culposa daño al patrimonio del Estado. Además, desarrollar la actividad ejecutiva para cobrar las deudas fiscales claras derivadas de los procesos sancionatorios y de responsabilidad Fiscal, expresas y actualmente exigibles, que consten en documentos que presten merito ejecutivo.
Participación Ciudadana	Responder a los requerimientos de los ciudadanos de manera oportuna y efectiva y generar mecanismos de

PROCESO	DESCRIPCIÓN
	capacitación y promoción que fortalezcan el ejercicio del control fiscal participativo por parte de la ciudadanía.
Gestión Financiera	Administrar de manera eficiente y eficaz los recursos financieros para el cumplimiento de la gestión institucional, proveer información financiera para la toma de decisiones y realizar seguimiento y control de los recursos financieros.

Los siguientes procesos representan dentro del funcionamiento de la entidad aquellos de mayor impacto, para este se describen los subprocesos que determinan la afectación en sus resultados.

Proceso	***Subprocesos***
Control fiscal	Elaborar y comunicar el Plan de Vigilancia y Control fiscal territorial (PVCFT)
	Revisión de cuenta e informes
	Realizar auditorias
	Planes de mejoramiento
	Traslado de Hallazgo
Responsabilidad fiscal	Evaluar la información para dar inicio a la Indagación Preliminar o proferir el Auto de Apertura.
	Prácticas de Pruebas.
	Recepcionar los argumentos de defensa y pruebas.
Participación ciudadana	Recepcionar, Peticiones, Quejas, Reclamos y Sugerencias (PQRS)
	Radicación y Diligenciamiento de Formato
	Evaluación de Denuncias, Quejas y/o petición por la coordinación de participación ciudadana

	Gestión y tramites de la petición, quejas, denuncias y/o remisión al proceso de responsabilidad fiscal o al de control fiscal Micro y Macro
	Remisión o traslado de las denuncias que no son competencia de la Contraloría Municipal
Gestión financiera	Ejecutar y controlar los recursos financieros.
	Realizar la legalización de los avances para viáticos y gastos de viaje

5.2.2. Identificación De Sistemas Críticos

Una vez identificados los procesos y subprocesos críticos es necesario establecer aquellos componentes de la arquitectura de servicios tecnológicos sobre los cuales se apoyan, si bien no existe una fuerte dependencia para el desarrollo de la función principal en cada proceso, ya que para cada elementos existen procedimiento de tipo manual que permiten soportar el servicio de manera alterna, por lo anterior, la valoración de estos componentes se da en función de la celeridad que aportan cuando son ejecutados en un contexto de tecnologías.

Los procesos de apoyo, dentro de la cadena de valor de la CGDC, revelan una mayor dependencia de la arquitectura TI. Las funciones de liquidar nomina, el control de ingresos mediante los sistemas de identificación biométrica, la contabilidad y las actividades de tipo financiero, suponen el uso de software especializado para cada tarea, conformado así el grupo que presenta una mayor sensibilidad a la disponibilidad y exige la implementación de mecanismos de protección de los datos y terminales de usuario.

Sobre el entendido que cada actividad requiere recursos de hardware, software y comunicaciones se han agrupado en las siguientes categorías de disponibilidad y definido el nivel y el tiempo estimado de tolerancia a fallos.

Disponibilidad de Función dentro de la CGDC	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
Aplicaciones	Sistema de Control de flujo de documentos, ventanilla única	B	3	Contenedor de aplicaciones
Web	Sitio web Entidad	A	1	Capa de presentación
Base de Datos	Nomina, financiero, contabilidad y control biométrico	B	1	Contenedor de aplicaciones en MYSQL
Comunicaciones	Acceso Local a Internet	B	2	Comunicación de Internet del usuario local
Proveedores de Aplicaciones y/o comunicaciones	Interno/externo, ventanilla única, software de rendición cuenta	A	2	Desarrollo Interno o contratado por externos. Canales de comunicaciones provisto por terceros (SIA, SECOP, etc.)
Terminales de usuario	Terminales de usuario en puesto de trabajo y auditorías externas	B	2	Capa de procesamiento de datos y disponibilidad de usuarios.

5.2.3. Establecimiento De Tiempos De Recuperación

Debido al impacto que supone sobre los procesos la disponibilidad de los recursos de TI, se han definido los siguientes tiempos de recuperación para cada componente considerados como fundamental, dicho tiempo se define como el mínimo lapso que debe trascurrir para recuperar, el componente o sistemas, de una alteración o falla de los servicios. Para su valoración se utilizará la siguiente escala.

Tiempo de Recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Como se mencionó previamente, algunos procesos utilizan elementos de la arquitectura tecnología sin embargo pueden funcionar con procedimiento manuales alternos los cual disminuye el impacto operacional aumentando la tolerancia del MTD, es decir, el tiempo máximo de inactividad que puede tolerar la entidad antes de evidenciar en los resultados y productos la carencia del servicio.

Función de los procesos misionales o de apoyo	Proceso Crítico (Servicios)	MTD (en días)	Prioridad de Recuperación
Aplicaciones	Sistema de Control de flujo de documentos, ventanilla única	4	4
Aplicaciones	Sistema de Nómina	0.5	1
Aplicaciones	Sistemas Biométrico	2	2
Aplicaciones	Página Web	0.3	1
Comunicaciones	Correo Electrónico	0.3	1
Comunicaciones	Servicio Wifi, red local	1	2
Soporte Informático	Equipo PC de usuario	3	2
Soporte Informático	Servidores de datos	1	2

5.3. GESTIÓN DEL RIESGO

El riesgo es la probabilidad de ocurrencia de eventos negativos que perjudiquen los equipos informáticos y periféricos. El análisis supone obtener una evaluación del impacto de dichos sucesos negativos. El valor calculado se utiliza para contrastar el costo de la protección de la información con el costo de una nueva producción.

Ante la posible materialización de algún evento que ponga en riesgo la operatividad de la CGDC y con el fin de establecer prioridades para la mitigación de los riesgos, se hace necesario disponer de metodologías para su evaluación., la cual hace perentoria establecer un conjunto de causas que pueden generar dificultades, entre las que encontramos:

Riesgos Tecnológicos:

- Fallas en el Fluido Eléctrico.
- Sabotaje Informático.

Fallas en los servidores de datos.

- Problemas Técnicos.
- Fallas en equipos tanto de procesamiento, telecomunicaciones como eléctricos.
- Servicios de Soporte a Sistemas de Producción y/o Servicios.

Riesgos Humanos:

- Robos.
- Acto Hostil.
- Marchas, mítines.
- Artefactos explosivos.
- Problemas organizacionales.
- Problemas de terceros involucrados en la producción o soporte a un servicio.
- Problemas con los proveedores de insumos o subproductos.

Desastres Naturales:

- Sismos
- Tormentas Eléctricas
- Incendios
- Inundaciones

5.3.1. Clasificación De Escenarios De Riesgo

A fin de conocer con precisión los riesgos potenciales en la prestación de servicios de tecnologías de la información en las CGDC, se clasifican los posibles escenarios de riesgos y describe su nivel de impacto por cada proceso crítico. La siguiente tabla expone esta clasificación en la cadena de valor de la CGDC.

Categorías	Escenarios	Descripción Impacto
Red Eléctrica	Fallas en el fluido eléctrico red normal (no regulada)	Fallas del servicio eléctrico de la entidad que afecta equipos eléctricos normales.
	Fallas en el Fluido Eléctrico red regulada	Fallas en los servicios de Tecnología de Información.
Red Datos, Internet y Seguridad	Problemas dispositivos Red: Falla Parcial	Falla temporal de los servicios de TI de todo un componente por limitación en la comunicación.
	Problemas dispositivos Red: Falla Total	Falla general de los servicios de TI de todos los componentes por ausencia en las comunicaciones
	Problemas en los Dispositivos Seguridad: Falla Parcial	Falla parcial de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware Software) y ausencia de políticas y controles de TI.
	Problemas en los Dispositivos Seguridad: Falla Total	Falla general de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware, Software) y ausencia de políticas y controles de TI.
	Ausencia servicio del canal de Internet: Total	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de internet por ausencia en la comunicación. No acceso a internet; impacto directo con el proveedor del servicio.
	Perdida conectividad hacia el NAP Colombia: Parcial	Falla parcial de los servicios de TI por ausencia en la conexión hacia el NAP Colombia. Acceso parcial a la red de internet por parte del proveedor del servicio.
Hardware distribuido – soporte de infraestructura para ventanilla	Problema de Hardware de Servidores: Falla Total	Falla total de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problema HW Servidores: Falla Parcial	Degradación de la calidad (lentitud) de los servicios de los sistemas de información que usan la plataforma de servidores.

Categorías	Escenarios	Descripción Impacto
Única – Pagina web y aplicativos Locales	Problemas en sistema Almacenamiento	Falla de los servicios de los sistemas de Información que usan la plataforma de almacenamiento de información.
	Problemas Hardware de Servidores	Falla de los servicios de los sistemas de información que usan la plataforma de servidores.
Aplicaciones Infraestructura Distribuida – Ventanilla Única – Pagina web	Problemas Capa de Aplicaciones	Falla o degradación del servicio prestado en el sistema de información afectado por problemas en las aplicaciones.
	Problemas Capa Media	Falla o degradación de la aplicación soportada por las herramientas de software y el sistema de almacenamiento masivo de datos - SAN, por tanto, se puede presentar degradación o ausencia del servicio prestado por sistema de información afectado por problemas de la capa media.
	Problemas Capa de Bases de Datos	Falla o degradación de las aplicaciones soportadas por las herramientas y motores de Base de Datos, por tanto, se puede presentar degradación o ausencia del servicio prestado por los sistemas de información afectados por problemas de la capa de base de datos.
Recurso Humano	Ausencia de funcionarios, incapacidades y rotación	Disminución de capacidad de atención a los usuarios y funcionarios, lentitud en la atención a requerimientos e incidentes, como también el retraso en la puesta en marcha de nuevos servicios.

Categorías	Escenarios	Descripción Impacto
	Errores humanos en operación	Contempla desde la degradación de un servicio hasta la pérdida del mismo, como también la ejecución de procedimientos de manera errada que de cómo resultado la pérdida del servicio de uno o todos los sistemas de información de la CGDC.

5.3.2. Metodología Del Riesgo

Un aspecto fundamental en los procesos de contingencia reactiva es la identificación de los riesgos a los que están enfrentada la infraestructura de TI de la CDGC, si bien, sus procesos misionales consumen información mediante aplicaciones provistas por terceros, los ciclos operativos de las funciones de apoyo utilizan aplicaciones locales que agilizan el desarrollo de ciertas actividades. A pesar de lo anterior es perentoria y relevante la identificación tanto de amenazas como de vulnerabilidades que pueden afectar las operaciones de la entidad.

Identificación de amenazas

Se consideran amenazas como aquellos factores que pueden generar daños dentro de la organización y que requieren ser identificados, por lo tanto, las amenazas pueden ocasionar riesgos al aprovechar las vulnerabilidades y permitir la afectación de los activos de información.

La identificación de amenazas que pueden afectar un activo de información puede clasificarse de la siguiente manera:

- Amenazas a las instalaciones: Caídas de energía, daños de agua, fallas mecánicas, pérdidas de acceso.
- Amenazas tecnológicas: Fallas en las comunicaciones, fallas en el software, fallas en el hardware, virus, spam, hacking, pérdida de datos, entre otros.

- Amenazas naturales: Inundaciones, sismos, huracanes, tormentas, incendios, entre otros.
- Amenazas sociales: Protestas, sabotajes, motines, asonadas, terrorismos, vandalismos, entre otros.
- Amenazas humanas: Problemas de transporte, huelgas, epidemias, pérdida de personal clave.

Identificación de vulnerabilidades

Se entienden Las vulnerabilidades como aquellas debilidades de seguridad de Información asociadas a los activos de información y se hacen efectivas cuando una amenaza la materializa en los sistemas de información de las CGDC.

Las vulnerabilidades no son causas de daño necesariamente, sino que son condiciones que pueden hacer que una amenaza afecte a un activo de información en particular. Luego de analizar las amenazas identificadas previamente se realizar un catálogo de riesgo para identificar las vulnerabilidades.

La siguiente tabla muestra las amenazas y vulnerabilidades por cada Activo de Información.

Sistema TI	Activo de Información	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia	Impacto
Servicio Web de la Entidad	Página Web Entidad	Defacement (desfiguración página web)	Mal diseño del sitio web	Medio	Alto
Servicio de correo electrónico	Correo electrónico	Virus, listas negras	Carencia de parches de seguridad	Alto	Alto
Sistema de Base de datos	Bases de datos interna	Usuario no autorizado	Mala configuración	Bajo	Alto

Servicio Red de comunicaciones	Equipos Switches de la Entidad	Falla de comunicaciones	Bloqueo de puertos	Medio	Alto
Terminales de usuarios	Informes preliminares de auditoria.	Robo de información.	Falta de antivirus. Poca capacitación a usuario sobre técnicas de suplantación y otros ataques informáticos.	Medio	Alto
Terminales de usuario	Documentos de procesos de auditoría en soporte digital	Destrucción o pérdida de datos por acción de virus o intrusión u otro mecanismo.	Ausencia de control centralizado de seguridad perimetral de red. Ausencia de antivirus.	Alto	Alto

5.3.3. Esquema General De Procedimientos

A continuación, se indican los procedimientos y actividades generales que se deben tener en cuenta para la correcta ejecución del plan de contingencia que aplica para cualquier sistema de información en la CGDC.

Equipos de Cómputo

La Oficina de Sistemas encargada de ejecutar el plan de continuidad debe llevar el inventario actualizado de los equipos de manejo de información (computadores, lectoras biométricas, impresoras, escáneres, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y una bitácora de mantenimiento que permita establecer, el ultimo personal externo que accedió al sistema con todos los privilegios.

Plan de respaldo

A fin de dar cumplimiento a los aspectos de reanudación de servicios y comportamiento contingente expuesto previamente, se hace necesario observar los siguientes componentes.

N°	ACTIVIDAD	ELEMENTOS	RESULTADO
1	Implementar un sistema de Copias de seguridad centralizada para toda la información y documentos residentes en los discos duros de los computadores de las áreas de la CGDC.	Documentos en formatos Word, Excel, PDF, artes, imágenes, audio y correos electrónicos	Una copia de seguridad en sistemas de almacenamiento externo de manera opcional, una Copia de seguridad anual obligatoria de todos los activos de información. **Responsable**: Oficina Sistemas.
2	Copias de seguridad de los sistemas de información y Bases de Datos de la CGDC.	Aplicaciones WEB. Aplicaciones y Bases de Datos de los procesos y archivos.	Copia de seguridad semanal del sistema de información activos de la Entidad. Realizar copia de seguridad de la pagina web alojada en servicio Hosting Contratados con tercero. **Responsable**: Oficina Sistemas.

3	Contar mínimo con un kit de instalación para restaurar los archivos del sistema operativo y aplicaciones de un computador o servidor en caso de falla o virus.	Sistema operativo. Bases de datos Drivers y utilitarios de impresoras, redes, computadores, etc.	Una copia u original del instalador en custodia de sistemas. **Responsable**: *Oficina de Sistemas*
5	Mantener pólizas de seguros vigentes, asegurando por el valor real, contra todo riesgo los equipos y bienes.	Equipos eléctricos y/o electrónicos, móviles, portátiles, software y equipos de comunicación.	Póliza vigente contra todo riesgo de daño y/o pérdida física por cualquier causa. **Responsable**: *Secretaria General*
6	Formular y desarrollar el plan de Mantenimiento preventivo y correctivo para equipos de computación y comunicación.	Equipos de computación y comunicación periféricos, sistemas eléctricos UPS, Aire acondicionado.	Contratos anuales de mantenimiento, garantías vigentes y control del mantenimiento de los equipos. **Responsable**: *Oficina de Sistemas.*
7	Actualizar las claves o contraseña de acceso a las aplicaciones y bases de datos.	Base de Datos, y sistemas de información de la CGDC y la provista por terceros.	Realizar cambio y o actualización semestral o cuando se requiera por el usuario o por reemplazos del cargo. Responsable: Todos los funcionarios de la Entidad que manejen sistemas de información.

8	Implementar mecanismos eficientes para garantizar la actualización de los sistemas operativos, antivirus y aplicaciones.	Sistemas operativos de equipos de cómputo, antivirus y aplicaciones.	Asegurar que los sistemas operativos o software de productividad cuenten con las últimas actualizaciones de seguridad. **Responsable:** Oficina de Sistemas.
10	Mantener como respaldo un inventario adicional con equipos de cómputo, repuestos, consumibles, para su reemplazo inmediato en caso de falla.	Equipos de computación y comunicación de la Entidad.	Reducción del tiempo de respuesta a fallas de hardware y sistemas de información. **Responsable:** Ingeniero de sistemas.
11	Disponibilidad de redundancia de recursos para evitar la interrupción de la prestación del servicio en los sistemas de información de la Entidad.	Concepto n+1: UPS, Planta eléctrica, almacenamiento, conexiones, líneas, equipos de cómputo adicional.	Evitar la suspensión del servicio a los usuarios teniendo una alternativa adicional, contratando servicio que garanticen la disponibilidad. Responsable: Oficina de Sistemas

5.3.4. Adopción del Protocolo IPV6

Se desarrollará en la CGDC el análisis y planeación para la implementación del Protocolo IPV6 en la entidad.

REFERENCIAS

Modelo de Seguridad y Privacidad de la información. Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Guia para realizar el Análisis de Impacto de Negocios BIA, Recuperado https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

Guía de Gestión de riesgos. Recuperado https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf