LO HACEMOS MEJOR
GOBIERNO DEL CESAR
WWW.LUISALBERTOMONSALVO.COM

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD DE INFORMACIÓN
AÑO 2020

VALLEDUPAR
AÑO 2020

Contenido

INTRODUCCIÓN 4

1. OBJETIVO GENERAL 5

2. ALCANCE 5

3. CONCEPTOS BASICOS RELACIONADOS CON EL RIESGO DE SEGURIDAD DE INFORMACIÓN 6

4. CONOCIMIENTO DE LA ENTIDAD 11

5. OBJETIVOS ESTRATEGICOS. 13

5.1. EJE ESTRATEGICO I: CALIDAD DE VIDA PARA EL DESARROLLO HUANO 13

5.2. EJE ESTRATEGICO II: LA APUESTA DEL DESARROLLO SOCIAL Y LA PROSPERIDAD 13

5.3. EJE ESTRATEGICO III. REVOLUCIÓN PRODUCTIVA, CRECIMIENTO Y EMPLEO 14

5.4. EJE ESTRATEGICO IV. SOSTENIBILIDAD AMBIENTAL Y ADAPTABLIDAD, LA RUTA DEL FUTURO 15

5.5. EJE ESTRATEGICO V. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA 16

6. PLANEACION INSTITUCIONAL 17

7. MODELO DE OPERACIÓN POR PROCESO. 18

8. CARACTERIZACION DE LOS PROCESOS 19

9. PLANES, PROGRAMAS O PROYECTOS ASOCIADOS QUE INCORPORAN COMPONENTES DE TI EN EL PLAN DE DESARROLLO DEPARTAMENTAL 27

10. POLITICA DE ADMINISTRACIÓN DEL RIESGO 28

11. IDENTIFICACION DE RIESGOS 28

12. VALORACIÓN DE RIESGOS 39

14. COMUNICACIÓN Y CONSULTA 47

15. MAPA DE RIESGOS DE SEGURIDAD DIGITAL VER (ANEXO) 48

INTRODUCCIÓN

El Gobierno nacional, a través del documento CONPES 3854 del 11 de abril de 2016 estableció la política nacional de seguridad digital que busca “fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el País”.

La seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la Información –MSPI.

1. OBJETIVO GENERAL

Establecer las acciones necesarias que permitan mitigar los riesgos de seguridad de la información, a través de la implementación de controles como resultado de la valoración del riesgo de seguridad de información.

1.1. Objetivos Específicos

- Identificar los activos de información de la entidad
- Proteger el valor de los activos de información de la entidad, implementando controles y acciones de mitigación frente al riesgo.
- Generar una cultura enfocada a la identificación de los riesgos de seguridad de la información y su mitigación, para evitar que se produzca un determinado impacto en la información.
- Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad de la información.

2. ALCANCE

El proceso parte de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información desde la identificación de los riesgos, su análisis, valoración y formulación de acciones, seguimiento, monitoreo y evaluación, para garantizar una adecuada gestión de riesgos de seguridad de la información dentro de la entidad.

3. CONCEPTOS BASICOS RELACIONADOS CON EL RIESGO DE SEGURIDAD DE INFORMACIÓN

Amenaza: (inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización. (ISO 2700:2016).

Acceso a la información pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56).

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

Contexto estratégico: Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

Causas (factores internos o externos): Son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

CCOC: Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

Cert: Computer Emergency Response Team (Equipo de respuesta a emergencias cibernéticas). (Universidad Carnegie-Mellón).

Cibercrímen (delito cibernético): Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).

Csirt: Por su sigla en inglés: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad cibernética). (http:// www.first.org).

Consecuencia: Resultado o impacto de un evento que afecta a los objetivos. (NTC ISO 31000:2011).

Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Contexto interno: Ambiente interno en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Control: Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Cooperación: Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

Criterios del riesgo: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo. (NTC ISO 31000:2011).

Descripción: Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

Entorno digital abierto: En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo. (NTC ISO 31000:2011).

Evaluación del control: Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).

Evaluación del riesgo: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).

Evento de seguridad de la información: Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).

Evitar el riesgo: Decisión de no involucrarse o de retirarse de una situación de riesgo. (NTC ISO 31000:2011).

Evento: Presencia o cambio de un conjunto particular de circunstancias. (NTC ISO 31000:2011).

Fuente de riesgo: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (NTC ISO 31000:2011).

Frecuencia: Medición del número de ocurrencias por unidad de tiempo. (NTC ISO 31000:2011).

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011).

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).

Incidente digital: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

Incidente de seguridad de la información: Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

Inventario de activos: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org).

Marco de referencia para la gestión del riesgo: Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo, a través

Parte involucrada: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad. (NTC ISO 31000:2011).

Peligro: Una fuente de daño potencial. (NTC ISO 31000:2011).

Pérdida: Cualquier consecuencia negativa o efecto adverso, financiero u otro. (NTC ISO 31000:2011).

Perfil del riesgo: Descripción de cualquier conjunto de riesgos. (NTC ISO 31000:2011).

Política: Intenciones y dirección de una organización como las expresa formalmente su alta dirección. (ISO/IEC 27000:2016).

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Posibilidad: Se utiliza como descripción general de la probabilidad o la frecuencia. (NTC ISO 31000:2011).

Plan para la gestión del riesgo: Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo. (NTC ISO 31000:2011).

Probabilidad: Oportunidad de que algo suceda. (NTC ISO 31000:2011).

Proceso para la gestión del riesgo: Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo. (NTC ISO 31000:2011).

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (ISO GUIA 73:2009).

Riesgo: (inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: Riesgo que permanece después del tratamiento de riesgos

Riesgo estratégico: Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgos financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Revisión: Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos. (NTC ISO 31000:2011).

Reducción del riesgo: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).

Retención del riesgo: Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

SGC: Sistema de gestión de calidad.

SGSI: Sistema de gestión de seguridad de la información.

Sistema para la gestión del riesgo: Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo. (NTC ISO 31000:2011).

Telecomunicaciones: Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos. (Resolución Min TIC 202 de 2010).

TI: Tecnologías de la información.

TO: Tecnología de operación

TIC (Tecnologías de la información y las comunicaciones): Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC).

Tratamiento del riesgo: Proceso para modificar el riesgo. (ISO/IEC Guía 73:2009).

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

4. CONOCIMIENTO DE LA ENTIDAD

4.1. Misión

En el 2032 el Departamento del Cesar, se habrá consolidado como el corredor de desarrollo logístico, agroindustrial y minero más importante de la Región Caribe, caracterizado por ser un territorio de Paz que brinda seguridad a sus ciudadanos para el desarrollo de sus actividades productivas, los cuales están al logro de competitividad territorial, potenciando sus ventajas comparativas a través del uso y desarrollo de nuevas tecnologías y mecanismo de desarrollo limpio, donde su riqueza natural y folclor vallenato lo han posicionado como uno de los destinos turísticos más atractivo del país. Todo eso gracias al fortalecimiento y aumento de su talento humano, capaz de jalonar su propio desarrollo, respetando su riqueza natural y

biodiversidad, en armonía con los pueblos indígenas y los afrocesarenses, bajo los principios del desarrollo humano y sobre la base de la seguridad democrática.

4.2. Visión

Planificar, dirigir y promover el desarrollo económico y social del Departamento del Cesar, a través de una gestión pública responsable, orientada con criterios de prioridad, racionalidad, equidad, solidaridad, desarrollo sostenible, de trasparencia administrativa y de buen gobierno, para el mejoramiento de la calidad de vida y el bienestar general se sus habitantes.

5. OBJETIVOS ESTRATEGICOS.

5.1. EJE ESTRATEGICO I: CALIDAD DE VIDA PARA EL DESARROLLO HUANO

Programa I. estrategia social para vida digna e incluyente

Objetivo Estratégico: Ejecutar acciones que superen con éxito el gran desafío de acortar las brechas y generar desarrollo social con énfasis en la conquista de condiciones para que el acceso pleno a la salud, la educación, la nutrición, agua potable y saneamiento básico y la vivienda, consoliden la equidad, la igualdad y en general eleven el nivel de vida de los y las cesarenses, de manera especial: primera infancia, niñez, adolescencia, juventud, adulto mayor, discapacidad, mujeres, afrocesarenses, indígenas, población víctima y población sexualmente diversa.

Programa II. Acuerdo de lucha contra el hambre

Objetivo estratégico: Desarrollar acciones integrales en coordinación colaborativa entre las sectoriales de la Gobernación, instancias privadas e interinstitucionales, para mejorar y/o recuperar el estado nutricional de la población en alto riesgo nutricional, especialmente de los niños y niñas y de las mujeres lactantes, gestantes y adulto mayor, impulsando la producción sostenible de alimentos, en los subsectores agropecuario y pesquero, para el autoabastecimiento y el acceso y consumo de alimentos del Departamento. . (Fuente: PDDC).

5.2. EJE ESTRATEGICO II: LA APUESTA DEL DESARROLLO SOCIAL Y LA PROSPERIDAD

Programa I. Educación incluyente para promover el desarrollo humano

Objetivo estratégico: Desplegar las gestiones enfocadas a asegurar que todas y todos los cesarenses en edad escolar o de formación, tengan la garantía de acceso y permanencia a este servicio sin restricciones y en condiciones de equidad e igualmente, que haya oportunidades de acceso a la formación superior de calidad y que ésta responda a los requerimientos de la dinámica económica del territorio.

Programa II. Mejor salud

Objetivo estratégico: Fortalecer las acciones encaminadas al mejoramiento de los servicios de salud, a través de iniciativas proyectos y programas, que buscan intensificar la promoción y prevención, así como mejorar los componentes sociales que apuntan al elevamiento de los estándares de atención, adecuación

de infraestructura hospitalaria, dotación y prestación de servicios en todas las áreas del sistema departamental de salud.

Programa III. Deporte, recreación y actividad física: un nuevo horizonte
Objetivo estratégico: Impulsar acciones que incidan en el mejoramiento de la infraestructura y estructuras organizativas y operativas de la actividad deportiva, la promoción y la capacitación del talento humano para el fortalecimiento institucional, que impacte, positivamente la competitividad del sector y que se conviertan en herramientas fundamentales de convivencia y de prevención al consumo de sustancias psicoactivas entre jóvenes y adultos. .

Programa IV. Un salto a la era digital y nuevas tecnologías.
Objetivo estratégico: Diseñar y poner en marcha una estrategia digital que incorpore formación, competencias y habilidades, infraestructura, conectividad y contenidos, y que se extienda a los sectores público, productivo y en hogares tanto del área urbana como rural, el Cesar se destacará en el Caribe por un audaz avance de los Indicadores de Competitividad en este campo. . (Fuente: PDDC).

5.3. EJE ESTRATEGICO III. REVOLUCIÓN PRODUCTIVA, CRECIMIENTO Y EMPLEO

Programa I. Transformación del campo
Objetivo estratégico: Fortalecer el sector agroindustrial, para brindar los instrumentos necesarios que conduzcan a una transformación integral del campo, dirigidos a la provisión de bienes públicos de infraestructura que permitan superar los retos y dificultades para seguir consolidando el aparato productivo, promoviendo la asociatividad y alianzas público-privadas, para el apoyo a los productores, en la adaptación de tecnologías para la tecnificación y la agregación de valor a sus procesos, apostándole a la transformación productiva para el aprovechamiento de las ventajas comparativas y así, mejorar los indicadores de competitividad de este renglón económico.

Programa II. Emprender para crecer
Objetivo estratégico: Desarrollar las acciones conducentes a la modernización del aparato productivo agropecuario, pesquero y de pequeña minería, el comercio y servicios, apostando a una cultura empresarial innovadora, sostenible y tecnológicamente adaptada y con agregación de valor a la cadena productiva,

para la modernización sectorial, produciendo con orientación a la demanda de cara a mercados locales, regionales e internacionales.

Programa III. Minería y energía sostenible para un mejor futuro
Objetivo estratégico: Convertir al Departamento del Cesar en líder regional de la minería y producción sostenible e innovadora de energía, principalmente limpia y renovable, a través del apoyo en la ejecución de programas, proyectos y estrategias para hacer de este sector el más competitivo para el crecimiento social del territorio.

Programa IV. Mejor infraestructura, más desarrollo
Objetivo estratégico: Mejorar la oferta de infraestructura pública para el crecimiento social y económico sostenido del Departamento del Cesar.

Programa V. El cesar, cultura y turismo de calidad
Objetivo estratégico: Fortalecer la institucionalidad del sector turismo, cultura, arte y patrimonio, con el apoyo firme e innovador a los actores departamentales, tanto de la industria turística como creativa, para construir la estrategia de desarrollo turístico, bajo la misión de promoción interna y externa, que consolide un turismo, que aporte al crecimiento social y económico, la productividad y competitividad del Cesar.

Programa VI. Idecesar: la fuerza del desarrollo social y económico regional
Objetivo estratégico: Promover una economía competitiva, inteligente e integradora que potencie el desarrollo territorial y empresarial orientando el apoyo de emprendimientos en aquellos sectores con mayor potencial de desarrollo económico y social que privilegien la innovación, proporcionando el acompañamiento para la creación y el crecimiento sostenido, inclusivo de nuevas empresas y de las existentes, orientando esfuerzos hacia la industrialización, mediante la atracción de capitales y de grandes empresas, que contribuyan a la mejora del empleo regional. . (Fuente: PDDC).

5.4. EJE ESTRATEGICO IV. SOSTENIBILIDAD AMBIENTAL Y ADAPTABLIDAD, LA RUTA DEL FUTURO

Programa II. Gestión del riesgo de desastres.
Objetivo estratégico: Generar las intervenciones necesarias para la gestión de riesgo de desastres fortaleciendo las capacidades institucionales para aumentar

la resiliencia ante las amenazas y los riesgos de emergencias que afectan a las comunidades vulnerables del territorio del Departamento del Cesar. . (Fuente: PDDC).

5.5. EJE ESTRATEGICO V. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA

Programa I. Seguros y en armonía

Objetivos estratégicos: Estructurar y poner en marcha una estrategia que empuje a la consolidación de la seguridad y la tranquilidad para los cesarenses, en la que se implementarán programas de educación ciudadana encaminados a fortalecer comportamientos colectivos de apego a la ley, convivencia, valores y resolución pacífica de las diferencias y conflictos en la población (PISCC), a la protección de la vida, la integridad y el patrimonio, honra y bienes, que a la vez sea posible y efectiva la prevención, persecución y castigo de las conductas delictivas, para bienestar de los ,habitantes de este territorio.

Programa II. Generación de valor público para la gente

Objetivos estratégicos: A través de un ejercicio eficiente, eficaz y transparente de la gestión pública departamental, se producirán trascendentes niveles de confianza, credibilidad e interacción de parte de los ciudadanos que se destacarán por altos niveles de participación y satisfacción de la sociedad civil, como elevados niveles de sentido de pertenencia y colaboración por los integrantes del equipo de gobierno.

Programa III. Construcción de paz, equidad para las víctimas y postconflicto

Objetivos estratégicos:

Programa IV. Movilidad segura

Objetivos estratégicos: Poner en marcha un conjunto de acciones en el marco de las estrategias de movilidad regional, orientadas fundamentalmente al mejoramiento de la calidad de vida en diferentes localidades del Departamento del Cesar, a la reducción de siniestros viales y al mejoramiento de los indicadores de eficiencia operativa en los diferentes modos de transporte, atendiendo la protección e incorporación de comportamientos adecuados en las vías y promoviendo el uso de tecnologías y modos sostenibles. (Fuente: PDDC)

6. PLANEACION INSTITUCIONAL

En la estructuración del Plan de Desarrollo del Departamento del Cesar 2020-2023, agregan valor los lineamientos de los Objetivos de Desarrollo Sostenible, el Plan Nacional de Desarrollo, documentos Conpes, los Planes de Vida de las Comunidades Indígenas, Planes de Autodesarrollo de Comunidades Afrocolombianas y los diferentes planes sectoriales que son políticas públicas. Así mismo, nuestro aporte se centra en factores enmarcados en las cuatro dimensiones argumentadas en el informe de estos grandes pensadores; son estas, la educación y el componente de Ciencia, Tecnología e Innovación en industrias culturales y creativas, energía sostenible, biotecnología, medio ambiente y bioeconomía, ciencias sociales y desarrollo humano con equidad, ciencias de la vida y la salud, por supuesto ajustados a la vocación del territorio.

Presupuestos plurianuales de inversión

Este es el componente operativo del Plan de Desarrollo Departamental 2020-2023 y se encuentra estructurado por 5 ejes programáticos, 20 programas y 41 subprogramas, donde se contemplan proyectos estratégicos estructurales del desarrollo social, económico y político del Departamento del Cesar. En esta herramienta de la planeación confluyen los recursos disponibles para inversión; y programas, subprogramas y proyectos de inversión, conjugándose en una distribución priorizada de conformidad con las exigencias del desarrollo en el Departamento del Cesar. Por lo expresado, el Plan Plurianual de Inversiones, en los procesos anuales de Planeación del Desarrollo y Financiero, se convierte en un referente obligado en la construcción del Plan Operativo anual de Inversiones y del Presupuesto Anual, como única forma de que las ejecuciones presupuestales anuales de la inversión se orienten a la consecución de las metas y objetivos del Plan de Desarrollo.

Escenario Piso

El Plan Plurianual de Inversiones contiene los costos y fuentes de financiación de los programas, subprogramas y proyectos de inversión pública en el cuatrienio 2020 – 2023, donde los recursos se distribuyeron con base en la destinación específica de las rentas y en las exigencias prioritarias de la inversión sectorial, hasta alcanzar apropiaciones totales por un monto de $3.560.258.894.713, monto que equivale a los recursos financieros disponibles sin considerar fuentes alternas de recursos, cuadro Escenario Piso del Presupuesto Plurianual de Inversión, que cuenta con recursos que tienen un alto

grado de probabilidad de ingresos al fisco departamental, provenientes de todos los ingresos tributarios de destinación específica y de libre destinación; los no tributarios tales como tasas, derechos, multas y sanciones, sistema general de participaciones, sobretasa al ACPM y Sistema General de Regalías; y recursos del crédito.

Escenario Techo

Este escenario se constituye en una opción ideal de acción, posible en la medida en que la capacidad de construir alianzas para el desarrollo se convierta en un propósito real del equipo de gobierno y se presente como un referente para guiar la gestión de recursos. Tiene como base el escenario piso, al cual se le adiciona la fuente alterna de recursos denominada Gestión por un valor de $722.467.129.789, para un escenario techo con un total de $4.282.726.024.501. (Fuente: PDDC – Pagina 218).

7. MODELO DE OPERACIÓN POR PROCESO.

7.1. Mapa de procesos del departamento del cesar

Tabla No. 1 Mapa de Procesos Departamento del Cesar

MISIONALES	ESTRATEGICOS	DE APOYO	GESTION DE EVALUACION INDPENDIENTE
Gestión del Desarrollo	Planeación de Desarrollo	Administración de los Recursos Físicos	Gestión de la Evaluación Independiente.
Gestión Educativa		Gestión del Talento Humano	
Gestión en Salud y Promoción Social		Contratación e Interventoría	
Apoyo a la Gestión Territorial		Gestión Jurídica	
Atención Ciudadana	Mejoramiento Institucional	Gestión Financiera	
Gestión de Tramites		Gestión Documental	
Inspección Vigilancia y Control		Gestión de las TIC	
Seguimiento y Evaluación a la Gestión Municipal			

8. CARACTERIZACION DE LOS PROCESOS

Tabla N° 2 Caracterización de los Procesos		
PROCESO:	**Planeación del Desarrollo**	
OBJETIVO:	Organizar las necesidades y requerimientos de los diferentes grupos de interés de la comunidad, en el corto, mediano y largo plazo mediante la formulación, seguimiento y evaluación de los planes estratégicos, basados en la normatividad vigente.	
RESPONSABLES:	**DIRIGE:**	Gobernador
	EJECUTA:	Oficina Asesora de Planeación Departamental
	CONTROLA:	Jefe de Oficina Asesora de Planeación

Tabla N° 3		
PROCESO:	**Mejoramiento Institucional**	
OBJETIVO:	Garantizar el cumplimiento de objetivos y el fortalecimiento institucional a través de una planeación y retroalimentación permanente que permita potencializar las oportunidades de mejora y aumentar la efectividad de los procesos de la entidad	
RESPONSABLES:	**DIRIGE:**	Gobernador
	EJECUTA:	Oficina Asesora de Planeación Departamental, Equipo MECI-CALIDAD, Coordinación de Gestión Humana
	CONTROLA:	Representante de la Dirección y Equipo de MECI-CALIDAD.

Tabla N° 4	
PROCESO:	**Comunicación Estratégica**
OBJETIVO:	Fortalecer la identidad institucional de la Gobernación del Cesar y la disposición organizacional para la apertura, la interlocución, la visibilidad en sus relaciones y los flujos de información con los

	clientes internos y externos, que contribuyan con la efectividad y transparencia de su gestión.	
RESPONSABLES:	**DIRIGE:**	Gobernador
	EJECUTA:	Asesor de Prensa, Oficina de Asuntos Internos
	CONTROLA:	Despacho, Comité MECI-CALIDAD

Tabla N° 5

PROCESO:	**Gestión del Desarrollo**	
OBJETIVO:	Generar condiciones y estrategias que permitan el desarrollo económico, social, de infraestructura y servicios públicos, y la participación ciudadana en el ejercicio de los derechos políticos, con el fin de lograr el bienestar de la comunidad cesarense.	
RESPONSABLES:	**DIRIGE:**	Gobernador
	EJECUTA:	Secretarios de Agricultura, Minas, Infraestructura, Gobierno, Educación y Cultura, Salud, Recreación y Deportes; Oficinas Asesoras de Política Social, Paz.
	CONTROLA:	Oficina Asesora de Planeación, Representante de la Dirección y equipo MECI-CALIDAD.
PROCESO:	**Inspección, Vigilancia y Control**	
OBJETIVO:	Ejercer inspección, vigilancia y control de las actividades y/o servicios realizados directamente por las entidades estatales o particulares en el Departamento del Cesar, para garantizar el cumplimiento de las normas establecidas, sean de competencia del Departamento o por delegación de funciones.	
RESPONSABLES:	**DIRIGE:**	Oficina Asesora de Planeación
	EJECUTA:	Secretaria de Salud, Educación y Cultura, Minas e Infraestructura.
	CONTROLA:	Oficina de Control Interno.

Tabla N° 6		
PROCESO:	**Apoyo a la Gestión Territorial**	
OBJETIVO:	Prestar asistencia técnica y/o asesoría a los Municipios del Departamento del Cesar, con el fin de fomentar el desarrollo integral de los mismos.	
RESPONSABLES:	**DIRIGE:**	Gobernador
	EJECUTA:	Secretarias Misionales y de Apoyo
	CONTROLA:	Oficina Asesora de Planeación, Representante de la Dirección y Equipo MECI-CALIDAD

Tabla N° 7		
PROCESO:	**Gestión de Trámites**	
OBJETIVO:	Atender oportunamente las solicitudes de los diferentes trámites que por ley que le corresponda adelantar a la entidad.	
RESPONSABLES:	**DIRIGE:**	Asuntos Internos
	EJECUTA:	Secretarías que gestionan trámites
	CONTROLA:	Asuntos Internos

Tabla N°8		
PROCESO:	**Administración de los recursos físicos**	
OBJETIVO:	Dotar con herramientas necesarias a las diferentes sectoriales de la Gobernación del Cesar, mantener la infraestructura y los archivos y liderar la transformación tecnológica e informática, gestionando y desarrollando estrategias que garanticen la permanente disponibilidad de la plataforma existente de la entidad, para lograr su óptima operación.	
RESPONSABLES:	**DIRIGE:**	Secretaría General
	EJECUTA:	Coordinación de Recursos Físicos y Tecnológicos
	CONTROLA:	Representante de la Dirección y equipo MECI-CALIDAD.

Tabla N°9		
PROCESO:	**Gestión del talento humano**	
OBJETIVO:	Contribuir al desarrollo de las potencialidades, destrezas y habilidades del talento humano de la Gobernación del Cesar, y evaluar su conducta de tal manera que se favorezca el desarrollo integral de los funcionarios, con el fin de optimizar la prestación del servicio público y lograr que se desempeñen como dinamizadores de la gestión administrativa departamental	
RESPONSABLES:	**DIRIGE:**	Gobernador
	EJECUTA:	Coordinador de la Gestión Humana
	CONTROLA:	Secretaria General

Tabla N° 10		
PROCESO:	**Contratación e Interventoría**	
OBJETIVO:	Asegurar que la adquisición y ejecución de bienes y servicios demandados por la Administración Departamental, cumplan con los requisitos legales vigentes y con los establecidos por la Entidad para dar lograr darle cumplimiento a sus metas.	
RESPONSABLES:	**DIRIGE:**	Gobernador
	EJECUTA:	Todas las sectoriales
	CONTROLA:	Oficina de Asuntos Jurídicos, Secretaria de Hacienda.

Tabla N° 11		
PROCESO:	**Gestión Jurídica**	
OBJETIVO:	Asesorar y representar efectivamente a la gobernación del Cesar en los asuntos jurídicos de interés de la entidad para garantizar que los mismos se encuentren dentro de los parámetros legales y constitucionales vigentes.	
RESPONSABLES:	**DIRIGE:**	Asesor Jurídico
	EJECUTA:	Funcionarios de la oficina Asesora Jurídica y Abogados Externos
	CONTROLA:	Asesor Jurídico.

Tabla N° 12		
PROCESO:	**Gestión Financiera**	
OBJETIVO:	Administrar con efectividad los recursos económicos del Departamento del Cesar con el propósito de distribuirlos con equidad, legalidad y progresividad en los planes, programas y proyectos establecidos por la administración.	
RESPONSABLES:	**DIRIGE:**	Gobernador
	EJECUTA:	Coordinadores de Secretaría de hacienda y Tesorería
	CONTROLA:	Secretario de Hacienda

Tabla N°13		
PROCESO:	**Gestión de Evaluación Independiente**	
OBJETIVO:	Verificar y evaluar el esquema de la organización y el conjunto de planes, programas, normas, procedimientos con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previos.	
RESPONSABLES:	**DIRIGE:**	Asesor de Control Interno
	EJECUTA:	Funcionarios Oficina Asesora de Control Interno
	CONTROLA:	Asesor de Control Interno

Tabla N° 14		
PROCESO:	**Atención Ciudadana**	
OBJETIVO:	Garantizar calidad en la atención, oportunidad y capacidad de respuesta a la ciudadanía, mediante la implementación de políticas de servicio y protocolos de atención, a través de los canales telefónico, virtual y presencial, con calidad, oportunidad y en cumplimiento de la normatividad vigente.	
RESPONSABLES:	**DIRIGE:**	Asesor de Asuntos Internos
	EJECUTA:	Todas las dependencias
	CONTROLA:	Jefe Oficina Asesora de Control Interno

Tabla N° 15		
PROCESO:	**Seguimiento y Evaluación de la Gestión Municipal**	
OBJETIVO:	Verificar que los entes municipales cumplan con la información para la evaluación de la planificación financiera y desempeño integral.	
RESPONSABLES:	**DIRIGE:**	Jefe Oficina Asesora de Planeación Departamental
	EJECUTA:	Profesional de Planeación Departamental
	CONTROLA:	Jefe Oficina Asesora de Planeación Departamental

Tabla N° 16		
PROCESO:	**Gestión de la TIC**	
OBJETIVO:	Asegurar la disponibilidad, actualización y optimización de las tecnologías de la información y las comunicaciones, de forma oportuna y eficaz.	
RESPONSABLES:	**DIRIGE:**	Asesor de la TIC
	EJECUTA:	Profesional Especializado de Sistemas
	CONTROLA:	Secretario(a) de Planeación

Tabla N° 17		
PROCESO:	**Gestión Documental**	
OBJETIVO:	Gestionar el manejo de la información recibida y producida por la entidad, mediante la planeación, gestión, organización y conservación de acuerdo con los lineamientos archivísticos de ley e independiente del soporte o medio de registro en el que se encuentre o produzca toda la información.	
RESPONSABLES:	**DIRIGE:**	Secretario General
	EJECUTA:	Todas las dependencias
	CONTROLA:	Grupo de Gestión Documental y Oficina Asesora de Control Interno.
PROCESO:	**Gestión de Salud y Promoción Social**	
OBJETIVO:	Acciones que sobre una población específica, con individuos identificables y caracterizables deben realizar las entidades	

	públicas o privadas para disminuir la probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo. De igual manera se debe atender determinantes particulares que conllevan a la inequidad social y sanitaria por ciclo de vida, etnia, género, víctimas y personas con discapacidad.	
RESPONSABLES:	**DIRIGE:**	Ministerio de Salud y Protección Social
	EJECUTA:	Entidades territoriales, EPS, IPS, otros sectores y la comunidad
	CONTROLA:	Secretario de Salud Departamental, Secretarios de Salud Municipales, Ministerio de Salud, Supersalud, veedurías, asociaciones de usuarios, comités de discapacidad, mesa de víctimas, procuraduría, contraloría.

Tabla N° 18		
PROCESO:	**Gestión Educativa**	
OBJETIVO:	Definir y desarrollar la organización y la prestación de la educación formal, educación para el trabajo y desarrollo humano en los establecimientos educativos oficiales de los 24 municipios no certificados del Departamento del Cesar.	
RESPONSABLES:	**DIRIGE:**	Secretario de Educación
	EJECUTA:	Todas las dependencias de la Secretaría de Educación
	CONTROLA:	Jefe de la Oficina Asesora de Control Interno.

Tabla N° 19	
PROCESO:	**Gestión de Trámites**
OBJETIVO:	Garantizar la prestación de servicios oportunos, transparentes y confiables, con el fin de contribuir al acercamiento entre el ciudadano y el estado a través de los diferentes canales de atención acorde a la normatividad legal aplicable aumentado la satisfacción de los ciudadanos, lo anterior para dar cumplimiento

	a las políticas y estrategias de eficiencia administrativa y racionalización de trámites.	
RESPONSABLES:	**DIRIGE:**	Jefe Oficina Asesora de Planeación Departamental
	EJECUTA:	Secretaria de Salud, Secretaria de Educación, Secretaría de Hacienda, Secretaría de Recreación y Deportes, Secretaría de Gobierno.
	CONTROLA:	Oficina Asesora de Asuntos Internos.

9. PLANES, PROGRAMAS O PROYECTOS ASOCIADOS QUE INCORPORAN COMPONENTES DE TI EN EL PLAN DE DESARROLLO DEPARTAMENTAL

PROYECTOS QUE INCORPORAN COMPONENTES TECNOLOGICOS EN EL PLAN DE DESARROLLO DEPARTAMENTAL DEL CESAR 220 2023 "LO HACEMOS MEJOR" -PDDC				
	EJE ESTRATEGICO	PROGRAMA	Subprograma	producto
2	**EJE ESTRÁTEGICO I. DESARROLLO HUMANO** CALIDAD DE VIDA PARA EL DESARROLLO HUMANO	**PROGRAMA I**. ESTRATEGIA SOCIAL PARA VIDA DIGNA E INCLUYENTE	Subprograma II. Los jóvenes: una fuerza positiva de transformación.	Construcción de plataforma de información para la población joven, que le permita acceder a programas, proyectos, actividades, servicios, convocatorias y rutas de atención, que entidades públicas, privadas, mixtas y comunitarias tengan disponibles para esta población.
13	**EJE ESTRATÉGICO II**. LA APUESTA DEL DESARROLLO SOCIAL Y LA PROSPERIDAD.	**PROGRAMA II**. SALUD, DE BIEN A MEJOR PARA TODOS LOS CESARENSES	**Subprograma IV.** Sistema de Emergencias Médicas	Desarrollar e implementar el sistema integrado de información y telecomunicaciones que articule el CRUE con los municipios del departamento en tiempo real para fortalecer referencia y contra referencia, emergencias y desastres, donación de órganos, misión médica, centro de reserva, ambulancias, red pública y privada
20	**EJE ESTRATÉGICO II**. LA APUESTA DEL DESARROLLO SOCIAL Y LA PROSPERIDAD.	**PROGRAMA IV.** UN SALTO A LA ERA DIGITAL Y NUEVAS TECNOLOGÍAS.	**Subprograma I**. Servicios digitales competitivos sin fronteras	Promover programas de formación orientados a promover competencias y habilidades de los cesarenses y avanzar hacia la consolidación de ciudadanos digitales.
21	**EJE ESTRATÉGICO II**. LA APUESTA DEL DESARROLLO SOCIAL Y LA PROSPERIDAD.	**PROGRAMA IV.** UN SALTO A LA ERA DIGITAL Y NUEVAS TECNOLOGÍAS.	**Subprograma I**. Servicios digitales competitivos sin fronteras	Estructurar un diagnóstico de requerimientos de infraestructura tecnológica, conectividad, uso y apropiación.
22	**EJE ESTRATÉGICO II**. LA APUESTA DEL DESARROLLO SOCIAL Y LA PROSPERIDAD.	**PROGRAMA IV.** UN SALTO A LA ERA DIGITAL Y NUEVAS TECNOLOGÍAS.	**Subprograma I**. Servicios digitales competitivos sin fronteras	Promover la estructuración de una plataforma que per mita divulgar los productos y servicios de los sectoresproductivos del departamento
23	**EJE ESTRATÉGICO II**. LA APUESTA DEL DESARROLLO SOCIAL Y LA PROSPERIDAD.	**PROGRAMA IV.** UN SALTO A LA ERA DIGITAL Y NUEVAS TECNOLOGÍAS.	**Subprograma I**. Servicios digitales competitivos sin fronteras	Promover el aumento de cobertura en TICS a través de alianzas público – privadas en sectores urbanos y rurales del departamento.
24	**EJE ESTRÁTEGICO III.** REVOLUCIÓN PRODUCTIVA, CRECIMIENTO Y EMPLEO	**PROGRAMA I.** TRANSFORMACIÓN DEL CAMPO	**Subprograma I.** Salto a la Agroindustria	Impulsar el uso de plataformas digitales para posicionar al Departamento del Cesar como el epicentro del desarrollo Agro-industrial.
32	**EJE ESTRÁTEGICO III.** REVOLUCIÓN PRODUCTIVA, CRECIMIENTO Y EMPLEO	**PROGRAMA V**. EL CESAR CULTURAL Y TURISMO DE CALIDAD	**Subprograma I.** Turismo competitivo	Fortalecimiento y actualización del Sistema de InformaciónTurística del Departamento del Cesar (SITUR, Cesar).
33	**EJE ESTRÁTEGICO III.** REVOLUCIÓN PRODUCTIVA, CRECIMIENTO Y EMPLEO	**PROGRAMA V**. EL CESAR CULTURAL Y TURISMO DE CALIDAD	**Subprograma I.** Turismo competitivo	Impulsar plataforma Web que permita la promoción de la oferta turística del territorio.
37	**EJE ESTRATÉGICO IV.** SOSTENIBILIDAD AMBIENTAL Y ADAPTABILIDAD: LA RUTA DEL FUTURO	**PROGRAMA II.** GESTIÓN DEL RIESGO Y DESASTRES	**Subprograma I.** Resiliencia, conocimiento, reducción y manejo del riesgo de desastres.	Fortalecimiento de la Central de Información y Telecomunicaciones (CITEL).
38	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA I.** SEGUROS Y EN ARMONÍA	**Subprograma I**. Convivencia y seguridad ciudadana	Implementar sistemas de información de violencia y delincuencia que manejan las instituciones armadas y de justicia, para hacer seguimientos a las estadísticas.
39	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA I.** SEGUROS Y EN ARMONÍA	**Subprograma I**. Convivencia y seguridad ciudadana	Implantar programas de dotación de nuevas cámaras de vigilancia CCTV, drones y equipos de radio de comunicación como mecanismo para brindar apoyo a las autoridades de policía y militares para la seguridad del territorio.
43	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma I.** Gestión para el buen desempeño	Generar espacios de interconectividad eficaces del gobierno departamental con entes de control del orden nacional y departamental.
44	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma I.** Gestión para el buen desempeño	Desarrollar acción que consolide la unificación total de trámites y servicios a través de la ventanilla única, mejorando la interoperabilidad interinstitucional público privada.
45	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma I.** Gestión para el buen desempeño	Implementar un modelo de gestión de documentos electrónicos, la optimización de la información, interoperabilidad entre los sistemas de información, automatización de procesos de atención y servicios para avanzar hacia la estrategia del CERO PAPEL.
46	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma II.** Fortalecimiento institucional	Adquirir y mantener hardware y software que optimicen la operatividad de la Gobernación del Cesar.
47	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma II.** Fortalecimiento institucional	Desarrollar la política de Gobierno Digital de acuerdo a la normatividad vigente
48	**EJE ESTRATÉGICO V. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA**	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma II.** Fortalecimiento institucional	Implementar un Sistema de Información Geográfica que permita consolidar y procesar información para la planificación territorial
49	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma II.** Fortalecimiento institucional	Implementar un Sistema de Información Geográfica que permita consolidar y procesar bases de datos estadísticas para el reconocimiento del territorio y la focalización de la inversión.
50	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma III.** Buengobierno, el camino a laTransparencia	Realizar campañas para fortalecer los canales de divulgación de la información pública generada a través de diferentes medios.
51	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA II.** GENERACIÓN DE VALOR PÚBLICO PARA LA GENTE	**Subprograma III.** Buengobierno, el camino a laTransparencia	Optimizar el Sistema de Gestión de Documentos electrónicos de archivos como herramienta institucional en la simplificación de procesos, acceso a la información y atención apropiada a PQRSD.
	EJE ESTRATÉGICO V. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA III.** CONSTRUCCIÓN DE PAZ, EQUIDAD PARA LAS VÍCTIMAS Y POSTCONFLICTO	**Subprograma I**. Apoyar la implementación del Acuerdo de Paz	Implementar y puesta en marcha de la segunda fase del sistema de información de atención y asistencia a la población víctima.
53	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA IV.** MOVILIDAD SEGURA	**Subprograma I.** La movilidad como herramienta de desarrollo integral	Implementar un sistema tecnológico que permita apoyar el control operativo y reducir la ocurrencia de comportamientos inadecuados en las vías.
54	**EJE ESTRATÉGICO V**. SEGURIDAD, ORDEN Y TRANSPARENCIA PARA LA CONVIVENCIA	**PROGRAMA IV.** MOVILIDAD SEGURA	**Subprograma I.** La movilidad como herramienta de desarrollo integral	Implementar tecnologías de información (página web, app, etc) que permitan y faciliten la interacción con usuarios para la realización de trámites, servicios, proveer información de transporte y gestionar la operación del transporte en el departamento.

10. POLITICA DE ADMINISTRACIÓN DEL RIESGO

10.1. Lineamientos de la política

La gobernación del cesar a través de la resolución N° 001433 del 10 de mayo de 2016 adopta la política de administración del riesgo. En los casos de los riesgos de la seguridad digital, la Gobernación del Cesar los gestiona a través de los criterios establecidos en el Modelo de Seguridad y Privacidad de la información mediante la Resolución 0001534-2010 Politicas_seguridad_informatica, ver anexo 1: "resolución N° 001433 del 10 de mayo de 2016" y anexo 2 "Resolución 0001534-2010 Politicas_seguridad_informatica"

11. IDENTIFICACION DE RIESGOS

11.1. Establecimiento del contexto

11.1.1. Contexto Interno que pueden generar diferentes tipos de riesgos

	Tabla N° 20 Establecimiento del contexto	
	FACTORES INTERNOS	**TTPOS RIESGOS**
1	**Infraestructura:** 1. Disponibilidad de los Activos. 2. Capacidad de los Activos	Riesgo Operativo.
2	**Personal:** 1. Competencias laborales 2. Salud Ocupacional 3. Seguridad	Riesgo Operativo. Riesgo Estratégico
3	**Procesos:** 1. Capacidad, Diseño y Ejecución. 2. Proveedores. 3. Entradas y Salidas. 4. Conocimiento	Riesgo Operativo.
4	**Tecnología:** 1. Integridad de datos. 2. disponibilidad de datos y sistemas. 3. Desarrollo, producción y mantenimiento de sistemas de información	Riesgo de Tecnología
5	**Económicos y financiero :**	Riesgo Operativo

	1. Falta de Ejecución Presupuestal. 2. Falta de Inversión 3. Falta de infraestructura 4. Desviación der Recursos 5. Capacidad Instalada	
	Comunicación Interna: 1. Canales utilizados y su efectividad. 2. flujo de la información necesaria para el desarrollo de las operaciones.	Riesgo Operativo

11.1.2. Contexto Externo que pueden generar diferentes tipos de riesgos

Tabla N° 21 Contexto Externo que pueden generar diferentes tipos de riesgos

	FACTORES EXTERNOS	TTPOS RIESGOS
1	**Económicos:** 1. Embargo a la Gobernación	Riesgo financiero
2	**Medioambientales:** 1. Catástrofe Natural 2. Falta o Falla de Energía	Riesgo Operativo Riesgo Financiero Riesgo Cumplimiento. Riesgo Estratégico
3	**Políticos:** 1. Cambio de Gobierno 2. Voluntad Política	Riesgo Estratégico
4	**Sociales:** 1. Terrorismo 2. situaciones que afecten el orden Público. 3. Responsabilidad Social	Riesgo Operativo.
	Tecnológicos: 1. interrupciones.	Riesgo Cumplimiento. Riesgo de Tecnología

11.1.3. Contexto del Proceso

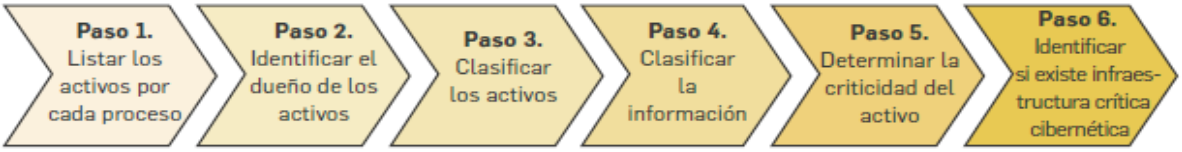
Tabla N° 22 CONTEXTO DEL PROCESO		
PROCESO:	Administración de los recursos físicos	
OBJETIVO:	Dotar con herramientas necesarias a las diferentes sectoriales de la Gobernación del Cesar, mantener la infraestructura y los archivos y liderar la transformación tecnológica e informática, gestionando y desarrollando estrategias que garanticen la permanente disponibilidad de la plataforma existente de la entidad, para lograr su óptima operación.	
ALCANCE:		
RESPONSABLES DEL PROCESO:	**DIRIGE:**	Secretaría General
	EJECUTA:	Coordinación de Recursos Físicos y Tecnológicos
	CONTROLA:	Representante de la Dirección y equipo MECI-CALIDAD.
INTERACION CON OTROS PROCESOS:	1. Procesos de Apoyo. 2. Procesos misionales. 3. Procesos Estratégicos 4. Proceso de Gestión de evaluación independiente	
TRANSVERSALIDAD:	1. Procesos de Apoyo. 2. Procesos misionales. 3. Procesos Estratégicos 4. Proceso de Gestión de evaluación independiente	
PROCEDIMIENTOS ASOCIADOS:	1. gc-ppa-022 administración de la plataforma informática 2. gc-ppm-023 desarrollo del programa para el procesamiento de datos 3. gc-ppa-092 administrador de servidores base de datos y redes 4. gc – ppa – 097 procedimiento adquisición – desarrollo y mantenimiento de software 5. gc-ppa-098 procedimiento apoyo a la gestión de proyectos que incorporen ti 6. gc-ppa-099 procedimiento copia de seguridad o backup 7. gc-ppa-102 procedimiento gestión de incidentes 8. gc-ppa-103 procedimiento protección de activos	

	9. gc-ppa-104 procedimiento separación de ambientes 10. gc-ppa-105 procedimiento gestión de proveedores 11. gc-ppa-106 procedimiento gestión de la capacidad 12. gc-ppa-107 procedimiento gestión de usuarios y contraseñas 13. gc-ppa-108 procedimiento retiro de activos de información 14. gc-ppa-109 procedimiento magnetización
ACTIVOS DE SEGURIDAD DIGITAL	1. Información Física o Digital 2. Servicios Web 3. Medios de almacenamientos magnéticos 4. Medios de almacenamiento Ópticos 5. Medios de almacenamientos Extraíbles 6. Redes 7. Hardware 8. Software

11.1.4. Identificación de activo de seguridad de información

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos los elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación –TO.

11.1.4.1. Como identificar los activos de seguridad de información



11.1.4.2. Paso 1. Listar los activos de cada proceso: los activos de seguridad digital de la entidad, se identifican dentro del inventario de activos de información emitido por la oficina de archivo aprobado a través de la resolución no. 0003350 de 17/08/2019 v1-2019; modificado v2-2020 10/12/2020.

11.1.4.3. **Paso 2. Identificar el dueño de los activos**: la identificación de los dueños de los activos de seguridad digital de la entidad se identifican dentro del inventario de activos de información emitido por la oficina de archivo aprobado a través de la resolución no. 0003350 de 17/08/2019 v1-2019; modificado v2-2020 10/12/2020.

11.1.4.4. **Paso 3. Clasificación de activos:** La Gobernación adopta la clasificación de activos establecida por la guía "articles-5482_G5_Gestion_Clasificacion" del ministerio de tecnología de la información y las comunicaciones.

Tabla N°23 Tipología de Activo

Tipo de Activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)

Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente (*.* Ministerio de tecnología de información y las comunicaciones)

11.1.4.5. Paso 4. Clasificación de la información: la clasificación de la información de la entidad se realizó conforme lo establece la Ley 712 de 2014 y Ley 1581 de 2012

Ley 712 de 2014

Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

Información pública reservada. Es aquella información" que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada 1, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

Concordancias: Constitución Política de Colombia, ART. 20. Ley 1712 de 2014, ART. 5. Ámbito de aplicación. Ley 1712 de 2014, ART. 18. Información exceptuada por

daño de derechos a personas naturales o jurídicas. Ley 1712 de 2014, ART. 19. Información exceptuada por daño a los intereses públicos. Ley 1712 de 2014, ART. 6. Literales c) y d) 6. Definiciones.

Ley 1581 de 2012

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Los activos de seguridad de información se deben identificar en cada proceso, y está en responsabilidad de cada líder de proceso. "***Ver Anexo 1. Activos de Seguridad de información – 2020***" Identificación de Activo de Seguridad de Información.

11.1.4.6. Paso 5. Criticidad de activos: La gobernación del cesar adopta y aplica los niveles de clasificación o niveles de criticidad de los activos, establecidos en la guía "articles-5482_G5_Gestion_Clasificacion".

Tabla N° 24 Niveles de Clasificación de Activos	
ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

11.1.4.7. Paso 6. Identificación de infraestructura critica cibernética:

La gobernación del cesar considera que no cuenta con una infraestructura crítica cibernética, porque sus activos no generan un impacto o afectación que podrían superar alguno de los tres (3) criterios establecidos en el "Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018 como son:

1. **Impacto social:** (0,5%) de Población Nacional, es decir que en el momento de materializarse un riesgo de unos de los activos de información de la entidad generaría un impacto social que afectaría aproximadamente 250.000 personas.

2. **Impacto económico:** PIB de un Día o 0,123% del PIB Anual, es decir que en el momento de materializarse un riesgo de unos de los activos de información de la entidad generaría un impacto económico que afectaría a la entidad en unos $464.619.736

3. **Impacto ambiental:** es decir que en el momento de materializarse un riesgo de unos de los activos de información de la entidad generaría un impacto ambiental que afectaría el ecosistema y duraría 3 años en su recuperación.

11.2. Identificación de Riesgos – Técnica para la identificación de riesgos de gestión y corrupción.

11.2.1. Técnicas para la redacción del Riesgo. La técnica para la identificación de riesgo de la entidad se adopta de la guía "Guía para la administración del - Riesgos de gestión, corrupción y seguridad digital - V4 Octubre de 2018", teniendo en cuenta que para la identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos.

Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo. A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos. Las preguntas claves para la identificación del riesgo permiten determinar:

¿**Qué puede suceder**? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
¿**Cómo puede suceder**? Establecer las causas a partir de los factores determinados en el contexto.
¿**Cuándo puede suceder**? Determinar de acuerdo con el desarrollo del proceso.
¿Qué consecuencias tendría su materialización? Determinar los posibles efectos por la materialización del riesgo.

Para la identificación de los riesgos de seguridad digita, se podrán identificar los siguientes tres (3) riesgos inherentes:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

11.2.2. Tipología de Riesgos

Tabla N° 25 Tipología de riesgos

Riesgos estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.	**Riesgos gerenciales**: posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.	**Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.	**Riesgos financieros:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
Riesgos tecnológicos: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.	**Riesgos de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.	**Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.	**Riesgos de cumplimiento:** posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
Riesgos de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.	**Riesgos de seguridad digital:** posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de	**Riesgo seguridad física:** Se conoce como seguridad física al conjunto de elementos que conforman un plan de seguridad, para proteger un espacio	**Riesgo ambiental:** En ciencias ambientales se denomina riesgo ambiental a la posibilidad de que se produzca un daño o catástrofe en el medio ambiente debido a un fenómeno natural o a una acción humana. El

	objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.	determinado con el fin de evitar daños y minimizar amenazas. Para prestar un buen servicio de seguridad es necesario identificar los posibles riesgos y amenazas que hay en el lugar y buscar los elementos físicos que se requieran para suministrar una excelente protección. Las amenazas que se pueden bloquear con los elementos de la seguridad física, son los incendios, robos, secuestros, homicidios, suplantación y robo de información, que se analizan y designan según la probabilidad de amenaza (altamente probable, probable, poco probable y probabilidad desconocida).	riesgo ambiental representa un campo particular dentro del más amplio de los riesgos, que pueden ser evaluados y prevenidos.

Fuente (*.*)Guía para la administración del - Riesgos de gestión, corrupción y seguridad digital - V4 Octubre de 2018 – Internet

12. VALORACIÓN DE RIESGOS

12.1. Análisis de Riesgos: en materia de seguridad digital se identifican los siguientes tres (3) riesgos inherentes: Pérdida de la confidencialidad, Pérdida de la integridad y Pérdida de la disponibilidad.

12.1.1. Análisis de Causas: Los objetivos estratégicos y de proceso se desarrollan a través de actividades, pero no todas tienen la misma importancia, por tanto, se debe establecer cuáles de ellas contribuyen mayormente al logro de los objetivos y estas son las actividades críticas o factores claves de éxito; estos factores se deben tener en cuenta al identificar las causas**.** Para los riesgos de seguridad digital, no es necesario realizar DOFA a nivel de activos, se toma la realizada para el proceso.

Fuente: Anexo 5 Análisis y Priorización de Causas - Guía riesgos 2018

12.1.2. Calculo de la Probabilidad: Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de **frecuencia,** es decir número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

NIVEL	Tabla N° 26 Criterios para calificar la probabilidad de ocurrencia		
	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi Seguro**	Se espera que el evento ocurra en la mayoría de circunstancias.	Más de (1) una vez al año

4	**Probable**	Se espera que el evento ocurra en la mayoría de circunstancias	Al menos (1) una vez en el último año
3	**Posible**	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos (1) una vez en los últimos 2 años
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos (1) una vez en los últimos 5 años
1	**Raro**	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años

12.1.3. Análisis de Impacto

Nivel de Impacto	Valor del Impacto	Tabla N° 27 - Criterios de Impacto para Riesgos de seguridad digital	
		Impacto (consecuencias - Cuantitativas	**Impacto (consecuencias - Cualitativas**
INSIGNIFICANTE	**1**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	**2**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.

MODERADO	**3**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	**4**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	**5**	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Fuente – Ministerio de tecnología de la información y las comunicaciones

Tabla N°28 Matriz de priorización de probabilidad de ocurrencia						
Probabilidad de ocurrencia	**Casi seguro**	B	B	M	A	A
	Probable	B	B	M	A	E
	Posible	B	M	A	E	E
	Improbable	M	A	A	E	E
	Rara Vez	A	A	E	E	E
		Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
		IMPACTO				

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo. En la matriz de priorización de probabilidad de ocurrencia como ejemplo el impacto fue identificado como **mayor** por cuanto puede generar interrupción de las operaciones por más de dos días. **En el mapa de color** se toma la calificación de probabilidad resultante de la tabla "Matriz de priorización de probabilidad", para este ejemplo se tomará la probabilidad de ocurrencia en **"probable"** y la calificación de impacto en **"mayor"**, nos ubicamos en la calificación de probabilidad en la fila y la de impacto en las columnas correspondientes, se establece el punto de intersección de las dos y este punto corresponderá al nivel de riesgo, que para el ejemplo es nivel **extremo – color rojo** (**R1**), así se podrá determinar el riesgo inherente.

Tabla N° 29 ZONA DE RIESGO		
B	Zona de Riesgo Baja	Asumir el Riesgo
M	Zona de Riesgo Moderada	Asumir el riesgo, Reducir el riesgo
A	Zona de Riesgo Alta	Reducir el Riesgo, Evitar, Compartir o Transferir
E	Zona de Riesgo Extrema	Reducir el Riesgo, Evitar, Compartir o Transferir

12.2. Evaluación del Riesgo.

12.2.1. Análisis Preliminar (Riesgo Inherente).

12.2.1.1. Riesgos Antes del Control: Una vez identificadas la vulnerabilidades y las amenazas, realizamos el análisis para identificar los posibles riesgos, recordemos que en materia de seguridad digital existen tres (3) riesgos inherentes como son: Pérdida de la confidencialidad, Pérdida de la

integridad y Pérdida de la disponibilidad, son riesgos que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso.

12.2.2. Valoración de controles (diseño de controles).

Para una buena valoración de los controles primero se debe tener en cuenta los seis (6) pasos que se deben realizar para el diseño de un buen control, teniendo en cuenta que en materia de seguridad digital la mayoría de los controles se encuentran establecidos en el anexo A de la ISO 270001, tal como lo establece la guía "*articles-5482_G8_Controles_Seguridad*".

Paso 1: Debe tener definido el responsable de llevar a cabo la actividad de control.
Paso 2: Debe tener una periodicidad definida para su ejecución.
Paso 3: Debe indicar cuál es el propósito del control.
Paso 4: Debe establecer el cómo se realiza la actividad de control.
Paso 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
Paso 5: Debe dejar evidencia de la ejecución del control.

En la valoración de los controles para la mitigación de los riesgos se debe asegurar que el control este bien diseñado y que permita mitigar el riesgo, recordemos que no solamente es necesario tener un buen control sino que el control se ejecute oportunamente, porque un control que se ejecute que este mal diseñado no mitiga ningún riesgo.

12.2.3. Niveles de Riesgos (riesgo residual). Se ha evidenciado que ningún riesgo con una medida de tratamiento se puede evitar o eliminar, la entidad debe buscar el desplazamiento de los riesgos inherente que se encuentren en zona de riesgo Alta o Extrema a una zona de riesgo Moderada o Baja de tal forma que la probabilidad o de ocurrencia o impacto disminuya.

13. Monitoreo y Revisión:

La entidad pública a través de las Tres Líneas de defensa definidas en el MIPG en la Dimensión 7 Control Interno, Componente Actividades de control, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y Finalización de los planes de acción.

- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.

- Realizar monitoreo de los riesgos y controles tecnológicos.

- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.

- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.

- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Es muy importante que la entidad monitoree y revise la gestión del riesgo con el fin de lograr los objetivos estratégicos y misionales que permitan alcanzar las metas establecidas en cada vigencia, para eso es necesario establecer los roles y responsabilidades de todos los actores del riesgo y control de la entidad.

De acuerdo a lo anteriormente expuesto surge el siguiente interrogante ¿Quiénes son los responsables para monitorear y revisar la gestión de riesgos de seguridad digital y cuáles son sus roles?

Según la "*Guía para la administración del - Riesgos de gestión, corrupción y seguridad digital - V4 Octubre de 2018*", existen tres (3) líneas de defensas para monitorear y revisar la gestión del riesgo de la entidad.

Para los riesgos de la entidad, le corresponde a la primera línea de defensa desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

13.1. ROLES Y RESPONSABLES. Primera línea de defensa

Responsable: líderes de los procesos, programas y proyectos de la entidad.

Rol principal: Ejecutar, diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la entidad, encargados de

realizar la identificación de riesgos de seguridad de digital, sobre los procesos que tiene a su cargo, con el acompañamiento del Profesional Especializado del Grupo de Recursos Físicos y Tecnológicos.

Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

13.2. ROLES Y RESPONSABLES. Segunda línea de defensa.

Responsable: Servidores públicos que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.

Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

13.3. ROLES Y RESPONSABLES. Tercera línea de defensa.

Responsable: la oficina de control interno, auditoría interna o quien haga sus veces.

Rol principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I.

(Fuente *.* "*Guía para la administración del - Riesgos de gestión, corrupción y seguridad digital - V4 Octubre de 2018*")

13.4. REGISTRO Y REPORTE DE INCIDENTES DE SEGURIDAD DIGITAL

Es importante que la entidad cuente con el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar. El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

13.5. Tratamiento de los riesgos de seguridad de la información

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos mencionados anteriormente.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

Tabla No.30. Tratamiento de Riesgos

COSTO-BENEFICIO	OPCIÓN DE TRATAMIENTO	EJEMPLOS
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios.	**Evitar el riesgo**, su propósito es no proceder con la actividad o la acción que da origen al riesgo.	• Tomar otra alternativa. • Eliminar una actividad, un procedimiento o un proceso que puede ser la causa del incidente.
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo.	**Transferir o compartir el riesgo**, entregando la gestión del riesgo a un tercero.	• Contratar servicios en la Nube para salvaguardar la información. • Contratar o Subcontratar el servicio.
El costo y el tiempo del tratamiento son adecuados a los beneficios.	**Reducir o Mitigar el riesgo**, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto	• Establecer controles que permitan reducir el riesgo.

La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Asumir el riesgo**, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa.	• Elaboración de controles de tipo preventivo y/o correctivo.

Fuente: Elaboración propia

13.6. Seguimiento de los riesgos de seguridad digital

De acuerdo al mapa de riesgo de seguridad digital, los controles se deben ejecutar en cada periodo, es muy importante realizarle seguimiento a las nuevas amenazas y vulnerabilidades que se puedan presentar y que pongan en riesgo la integridad, la disponibilidad y confidencialidad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrá cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: nuevos activos o modificaciones en el valor de los activos, nuevas amenazas, cambios o aparición de nuevas vulnerabilidades, aumento de las consecuencias o impactos, incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición que permitan contextualizar una toma de decisiones de manera oportuna.

14. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes interesadas tanto internas como externas se debe realizar durante todas las etapas de la metodología para la administración de los riesgos de seguridad y privacidad de la información.

Se debe tener en cuenta que la producción y modificación de información es constante, por lo que se sugiere que la actualización del Registro de Activos de Información y sus

respectivos riesgos, se realice cada vez que se presente alguna modificación de la categoría o serie de información.

El Grupo de Recursos Físicos y Tecnológicos, estará acompañando a los procesos en la identificación de los riesgos de seguridad y privacidad de la información, con el acompañamiento de la Oficina Asesora de Planeación Departamental.

15. MAPA DE RIESGOS DE SEGURIDAD DIGITAL VER (ANEXO)

Control de Cambios

Tabla N° 30. Tabla de Control de Cambio

FECHA	VERSION	CAMBIOS
18/01/2019	VER- 1.0	
31/12/2020	VER 1.1	Aplicación de la nueva metodología

Elaboró	Revisó	Aprobó
ALEX GOMEZ Profesional Especializado Grupo Recursos Físicos y Tecnológicos	**ALGONSO GARCÍA PAYARES** Profesional Especializado Grupo Recursos Físicos y Tecnológicos	**COMIÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO**