



LO HACEMOS MEJOR
GOBIERNO DEL CESAR
WWW.LUISALBERTOMONSALVO.COM

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACION SGSI – GOBERNACION DEL CESAR 2022

Nombre de Documento	Plan de tratamiento de riesgos de seguridad digital y seguridad de la Información
Versión del Documento	1.2
Fecha	10/12/2021
Detalle	El presente documento establece las medidas de seguridad identificadas para desarrollar e implementar al 31 de diciembre del 2022 el plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información en la Gobernación del Departamento del Cesar.

Control de Cambios

Fecha	Versión	Descripción
18/01/2019	1.0	
31/12/2020	1.1	Aplicación de la nueva metodología
10/12/2021	1.2	Seguimiento

Control de Aprobación

Variables	Fecha	Nombre	Cargo o Perfil
Elaboró	10/12/2021	Alex Gómez Garzón	Ing. Sistemas
Revisó	10/12/2021	Alfonso García. P	Ing. Sistemas
Aprobó	30/12/2021	Comité Institucional de Gestión y Desempeño	

Tabla de Contenido

1. GENERALIDADES – CONOCIMIENTO DE LA ENTIDAD

- 1.1 Introducción
- 1.2 Objetivo general
 - 1.2.1 Objetivo específicos
 - 1.2.2 Propósitos
- 1.3 Alcance
- 1.4 Misión
- 1.5 Visión
- 1.6 Objetivos estratégicos
- 1.7 Conceptos básicos relacionados con el riesgo de seguridad de la información
- 1.8 Marco normativo

2. MODELO DE OPERACIÓN POR PROCESO

- 2.1 Caracterización de los procesos

3. GESTION DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

- 3.1 Fase 1. Planificación de la gestión de riesgo de seguridad digital y seguridad de la información.
 - 3.1.1 Contexto interno y externo de la entidad publica
 - 3.1.1.2 Establecimiento del contexto externo
 - 3.1.2 Establecimiento del contexto interno
 - 3.1.3 Política de gestión de riesgo de seguridad digital y seguridad de la información
 - 3.1.4 Definición de roles y responsabilidades
 - 3.1.4.1 Roles y responsabilidades – Primera línea de defensa
 - 3.1.4.2 Roles y responsabilidades – Segunda línea de defensa
 - 3.1.4.3 Roles y responsabilidades – Tercera línea de defensa
 - 3.1.5 Definición de los recursos para la gestión de riesgos de seguridad digital y seguridad de la información.
 - 3.1.6 Identificación de activos de seguridad digital y seguridad de la información.
 - 3.1.6.1 Como identificar los activos de seguridad digital y seguridad de la información
 - 3.1.7 Identificar los riesgos inherentes de seguridad digital y seguridad de la información
 - 3.1.8 Tipología de riesgos
 - 3.1.9 Valoración de riesgos
 - 3.1.9.1 Análisis de riesgos
 - 3.1.9.2 Análisis de las causas
 - 3.1.9.3 Calculo de la Probabilidad
 - 3.1.9.4 Análisis de impacto
 - 3.1.10 Valoración de los controles existentes
 - 3.1.11 Valoración de los controles (diseño de controles)
 - 3.1.12 Niveles de riesgos (riesgo residual)
 - 3.1.13 Tratamiento de los riesgos de seguridad digital y seguridad de la información

3.2 Fase 2. Ejecución

3.3 Fase 3. Monitoreo y revisión

3.3.1 Registro y reporte de incidentes de seguridad digital y seguridad de la información

3.3.2 Reporte de la gestión de riesgos de seguridad digital y seguridad de la información al interior de la entidad

3.3.2.1 Reporte

3.3.2.2 Periódicidad

3.3.3 Reporte de gestión de riesgo de seguridad digital y seguridad de la información a autoridades o entidades especiales

3.3.4 Medición del desempeño

3.4 Fase 4. MEJORAMIENTO CONTINUO DE LA GESTION DE RIESGOS DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

4. CONTROLES DE REFERENCIA PARA LA MITIGACION DE RIESGOS DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

5. PUBLICACIÓN

6. MEDIOS DE DIFUSIÓN

1 GENERALIDADES – CONOCIMIENTO DE LA ENTIDAD

1.1 Introducción

La Gobernación del Departamento del Cesar en cumplimiento a lo establecido por el Gobierno Nacional a través del documento CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y en virtud del decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP

De acuerdo a lo anterior, la entidad busca fortalecer las capacidades institucionales realizando acciones que permitan 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.

1.2 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 identificación, valoración y análisis del riesgo de seguridad de información.

1.2.1 Objetivos específicos

- Identificar los activos de información de la entidad
- Proteger los activos de información, implementando controles que permitan mitigar el riesgo de seguridad de información.

1.2.2 Propósitos

- Preservar la disponibilidad, integridad y confidencialidad de la información.
- Implementar controles que permitan reducir, mitigar o trasladar el riesgo de seguridad de información

1.3 Alcance

Inicia con la identificación de los activos de información en cada uno de los procesos de la entidad y finaliza con la implementación, seguimiento y evaluación de los controles, incluye la implementación de las mejores prácticas y métodos que permitan garantizar la disponibilidad, integridad y confidencialidad de la información de la entidad. Aplica para todos los procesos de la entidad y solo para los activos de información que se encuentren en un nivel de clasificación ALTA. No aplica para los activos de información que se encuentren por fuera de la entidad.

1.4 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.

1.5 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 transparencia administrativa y de buen gobierno, para el mejoramiento de la calidad de vida y el bienestar general de sus habitantes.

1.6 Objetivos estratégicos

Los objetivos estratégicos de la entidad están establecidos en cada uno de los programas de los cinco ejes estratégicos que conforman la estructura del Plan de Desarrollo del Departamento del Cesar. PDDC. 2020-2023. “Lo Hacemos Mejor”. Lo puedes consultar en el siguiente link:

<https://cesar.gov.co/d/index.php/es/menvertpolpla/menvertplandes/232-artmenplandes>

1.7 Conceptos básicos relacionados con el riesgo de seguridad de información

Tabla N°1. Conceptos Básicos	
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 INTERNAS O EXTERNAS (FACTORES):	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 ABIERTO:	DIGITAL 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
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 CUMPLIMIENTO:	DE 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 RIESGO	DEL Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).
RETENCIÓN RIESGO:	DEL 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).

1.8 Marco normativo

La Documentación del plan de tratamiento de riesgo de seguridad de la información de la entidad se hace en base al siguiente marco normativo.

Tabla No. 2. Marco Normativo	
Marco Normativo	Descripción
Decreto 1151 de 2008	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones

Tabla No. 2. Marco Normativo

Marco Normativo	Descripción
Ley 1955 del 2019	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC)
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Ley 1341 de 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 962 de 2005	El artículo 14 lo siguiente “Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá al usuario. Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. El envío de la información por fax o por cualquier otro medio de transmisión electrónica, proveniente de una entidad pública, prestará mérito suficiente y servirá de prueba en la actuación de que se trate, siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite”.

Tabla No. 2. Marco Normativo

Marco Normativo	Descripción
Decreto 1413 de 2017	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Decreto 4485 de 2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Decreto 728 2016	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional

Tabla No. 2. Marco Normativo

Marco Normativo	Descripción
	del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 2106 del 2109	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Resolución 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Resolución 3564 2015	Reglamenta algunos artículos y párrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.
CONPES 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.

Tabla No. 2. Marco Normativo

Marco Normativo	Descripción
Conpes 3920 de Big Data, del 17 de abril de 2018	La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
Conpes 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016	El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
Conpes 3975	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Directiva 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

2. MODELO DE OPERACIÓN POR PROCESOS.

Tabla No.3. Mapa de Procesos Departamento del Cesar			
MISIONALES	ESTRATEGICOS	DE APOYO	GESTION DE EVALUACION INDEPENDIENTE
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			

2.1 Caracterización de los procesos

Tabla N° 4. 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° 5	
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° 6		
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° 7		
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.

Tabla N° 8		
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:	Secretaría de Salud, Educación y Cultura, Minas e Infraestructura.
	CONTROLA:	Oficina de Control Interno.

Tabla N° 9		
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:	Secretarías Misionales y de Apoyo
	CONTROLA:	Oficina Asesora de Planeación, Representante de la Dirección y Equipo MECI-CALIDAD

Tabla N° 10		
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°11		
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°12		
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° 13		
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 logro darle cumplimiento a sus metas.	
RESPONSABLES:	DIRIGE:	Gobernador
	EJECUTA:	Todas las sectoriales
	CONTROLA:	Oficina de Asuntos Jurídicos, Secretaria de Hacienda.

Tabla N° 14		
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° 15	
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°16		
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° 17		
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° 18		
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° 19		
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° 20		
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.

Tabla N° 21		
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° 22		
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° 23		
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.

3. GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El documento CONPES 3854, pág. 24 define la Gestión de Riesgo de Seguridad Digital como 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.

La Gobernación del Departamento del Cesar adoptó la estructura del Anexo N°4 DEL MODELO DE GESTION RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS “LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PUBLICAS”.

3.1 Fase 1. Planificación de la GRSD y Seguridad de la Información

La fase de planificación establece los primeros tres (3) pasos de la Guía para la Administración de los Riesgo de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida por la Función Pública, es decir:

1. Política de administración de riesgos.
2. Identificación de riesgos
3. Valoración de riesgos

Para el caso de la gestión de riesgo de seguridad digital y seguridad de información se debería utilizar una técnica de recolección de datos primarios que puede ser un cuestionario de preguntas o encuesta, esta herramienta de recolección de datos va dirigida al responsable del riesgo es decir al dueño del proceso, con el fin de identificar de cada proceso y activo de seguridad digital y seguridad de información posibles controles existentes, vulnerabilidades, amenazas, riesgo etc.

3.1.1 Contexto interno y externo de la entidad pública

La Gobernación del Departamento del Cesar realizó la identificación del contexto interno y externo de la entidad, alineado con el riesgo de seguridad de la información que se puede presentar al interior de la entidad. A continuación se presentan unas directrices que permiten identificar con mayor claridad el contexto interno y externo de la entidad.

3.1.1.2 Establecimiento del contexto externo

Para establecer el contexto externo, se debe tener en cuenta los siguientes factores relacionados con la Gestión de Riesgo de seguridad de Información

Tabla N° 24. 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

3.1.2 Establecimiento del contexto interno

El contexto interno, puede generar unos factores de riesgo de seguridad de la información que afectan de forma directa a la entidad tales como

Tabla N° 25. 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 4. Toda la estructura organizacional	Riesgo Operativo. Riesgo Estratégico
3	Procesos: 1. Capacidad, Diseño y Ejecución. 2. Proveedores. 3. Entradas y Salidas.	Riesgo Operativo.

	<ol style="list-style-type: none"> 4. Conocimiento 5. Roles y responsabilidades 	
4	<p>Tecnología:</p> <ol style="list-style-type: none"> 1. Integridad de datos. 2. disponibilidad de datos y sistemas. 3. Desarrollo, producción y mantenimiento de sistemas de información. 4. Sistemas de información o servicios. 5. Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) 	Riesgo de Tecnología
5	<p>Económicos y financiero :</p> <ol style="list-style-type: none"> 1. Falta de Ejecución Presupuestal. 2. Falta de Inversión 3. Falta de infraestructura 4. Desviación der Recursos 5. Capacidad Instalada 	Riesgo Operativo
	<p>Comunicación Interna:</p> <ol style="list-style-type: none"> 1. Canales utilizados y su efectividad. 2. flujo de la información necesaria para el desarrollo de las operaciones. 	Riesgo Operativo

3.1.3 Política de gestión de riesgo de seguridad de información

La Gobernación del Cesar a través de la resolución N° 001433 del 10 de mayo de 2016 adopta la política de administración del riesgo.

Teniendo en cuenta que el Departamento Administrativo de la Función Pública -DAFP, a través de la “**Guía para la administración del riesgo y el diseño de controles en entidades públicas**”, establece tres (3) tipos de riesgos que se pueden presentar al interior de una entidad pública como son: Riesgo de Gestión, Corrupción y Seguridad Digital.

De acuerdo a lo anteriormente expuesto es preciso anotar que la resolución 001433 del 10 de mayo de 2016 “**por la cual se adopta la política de administración de riesgo de la Gobernación del Cesar**”, no tiene incluido de forma clara y precisa las políticas de administración de riesgo de seguridad digital, por tal razón estas serán incluidas en la (resolucion_003471_03__2019 Política de seguridad y privacidad de la información), teniendo en cuenta que el Modelo de Seguridad y Privacidad de la información hace

parte de uno de los tres habilitadores del marco de referencia de arquitectura empresarial.

3.1.4 Definición de roles y responsabilidades

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.

3.1.4.1 Roles y responsabilidades – 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.

3.1.4.2 Roles y responsabilidades – 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.

3.1.4.3 Roles y responsabilidades – 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***)

3.1.5 Definición de los recursos para la gestión de riesgo de seguridad de la información.

Los líderes de proceso, los cuales son los propietarios de los riesgos, y los responsables de implementar los controles de seguridad de información, deben informar sobre los recursos necesarios que necesitan para el desarrollo de la gestión de riesgos de seguridad de información, (capital, tiempo, personal, procesos, sistemas y tecnologías), teniendo en cuenta que la entidad debe tener un responsable de la coordinación, seguimiento, reporte de los avances, logros e inconvenientes relacionados con la gestión de los riesgos de seguridad digital y seguridad de la información.

En anexo N° 4 de la guía de Gestión de Riesgo de seguridad digital recomienda que la alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad digital.
- Recursos económicos para la implementación de controles de mitigación de riesgos (Con base al análisis de riesgo realizado).
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

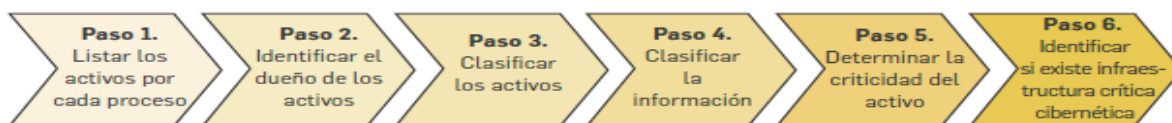
Para ver cada una de las fases, actividades y tareas a desarrollar en el plan de tratamiento de riesgo de seguridad digital y seguridad de la información de la Gobernación del Departamento consulta el ANEXO N° 1. ACTIVIDADES - SGRSD-2022

3.1.6 Identificación de activo de seguridad digital y 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.

Nota: La identificación de los activos de seguridad de información que se encuentren en un nivel de clasificación **ALTA**, será tomado del Plan Institucional de Archivo publicado en la página web de la entidad, con el fin de elaborar el mapa o matriz de riesgo de seguridad de información.

3.1.6.1 Como identificar los activos de seguridad de información y seguridad digital



Paso 1. Listar los activos de cada proceso

Los activos de seguridad de información, 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.

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.

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°26 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 godd 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)	

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.

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° 27. 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.

Paso 6. Identificación de infraestructura crítica 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.

3.1.7 Identificar los riesgos inherentes de seguridad digital y Seguridad de la información.

Para la identificación de los riesgos de seguridad digital y seguridad de la información, 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.

3.1.8 Tipología de Riesgos

Tabla N° 28. Tipología de riesgos		
Riesgos estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública.	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 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.

<p>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</p>	<p>Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales.</p>	<p>Riesgo seguridad física: Se conoce como seguridad física al conjunto de elementos que conforman un plan de seguridad, para proteger un espacio determinado con el fin de evitar daños y minimizar amenazas.</p>
<p>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.</p>	<p>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.</p>	<p>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.</p>
<p>Fuente (*.*)Guía para la administración del - Riesgos de gestión, corrupción y seguridad digital - V4 Octubre de 2018 – Internet</p>		

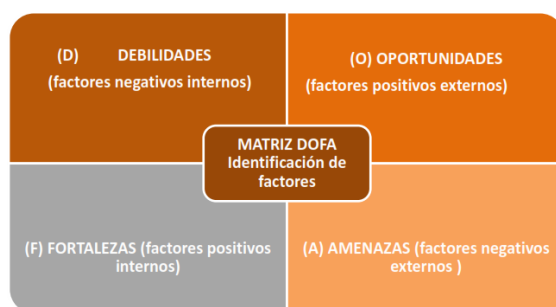
3.1.9 Valoración de riesgos

3.1.9.1 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.

3.1.9.2 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

3.1.9.3 Cálculo 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.

Tabla N° 29. Criterios para calificar la probabilidad de ocurrencia			
NIVEL	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


3.1.9.4 Análisis de Impacto

Tabla N° 30. Criterios de Impacto para Riesgos de seguridad digital			
Nivel de Impacto	Valor del Impacto	Impacto (consecuencias - Cuantitativas)	Impacto (consecuencias - Cualitativas)

INSIGNIFICANTE	1	<p>Afectación $\geq X\%$ de la población. Afectación $\geq X\%$ del presupuesto anual de la entidad. No hay afectación medioambiental.</p>	<p>Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.</p>
MENOR	2	<p>Afectación $\geq X\%$ de la población. Afectación $\geq X\%$ del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de $\geq X$ días de recuperación.</p>	<p>Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.</p>
MODERADO	3	<p>Afectación $\geq X\%$ de la población. Afectación $\geq X\%$ del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de $\geq X$ semanas de recuperación.</p>	<p>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.</p>
MAYOR	4	<p>Afectación $\geq X\%$ de la población. Afectación $\geq X\%$ del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de $\geq X$ meses de recuperación.</p>	<p>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.</p>

CATASTRÓFICO	5	<p>Afectación $\geq X\%$ de la población. Afectación $\geq X\%$ del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de $\geq X$ años de recuperación.</p>	<p>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.</p>

Fuente – Ministerio de tecnología de la información y las comunicaciones

Tabla N°31. 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° 32. 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

3.1.10 Valoración de Controles Existentes

La Gobernación del Departamento del Cesar una vez identifique, establezca y valore los riesgos inherentes deberá identificar y evaluar los controles existentes, teniendo en cuenta que en algunos casos los controles establecidos podrán estar documentados pero no implementados o en su defecto mal implementados

3.1.11 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.

3.1.12 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.

3.1.13 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.33. Tratamiento de Riesgos	
OPCIÓN DE TRATAMIENTO	EJEMPLOS
Evitar el riesgo , su propósito es no proceder con la actividad o la acción que da origen al riesgo.	<ul style="list-style-type: none"> • Tomar otra alternativa. • Eliminar una actividad, un procedimiento o un proceso que puede ser la causa del incidente.
Transferir o compartir el riesgo , entregando la gestión del riesgo a un tercero.	<ul style="list-style-type: none"> • Contratar servicios en la Nube para salvaguardar la información. • Contratar o Subcontratar el servicio.
Reducir o Mitigar el riesgo , seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto	<ul style="list-style-type: none"> • Establecer controles que permitan reducir el riesgo.
Asumir el riesgo , no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa.	<ul style="list-style-type: none"> • Elaboración de controles de tipo preventivo y/o correctivo.

3.2 Fase 2. Ejecución

La Gobernación del Departamento del Cesar en la fase de ejecución debe implementar y ejecutar cada una de las actividades contempladas en la fase 1.

La entidad a través de la línea Estratégica debe disponer los recursos que permitan la implementación y ejecución de la Gestión de Riesgo de Seguridad Digital y Seguridad de la Información.

La primera línea de defensa en articulación con la oficina de sistemas debe supervisar y acompañar la ejecución de las tareas en los tiempos establecidos.

3.3 Fase 3. 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.

3.3.1 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.

3.3.2 Reporte de la gestión del riesgo de seguridad digital y seguridad de la información al interior de la entidad

3.3.2.1 Reporte.

El responsable de seguridad digital y seguridad de la información debe reportar periódicamente a la Línea Estratégica (Alta dirección, comité de gestión y desempeño, Coordinación de Control Interno de gestión) y a las partes interesadas la siguiente información:

- Matriz de los riesgos identificados de seguridad digital.
- Listado de Activo críticos
- Reporte de criticidad/impacto de la entidad
- Plan de tratamiento de riesgo de seguridad digital y seguridad de la información
- Impacto económico que podría presentarse frente a la materialización de los riesgos.

3.3.2.2 Periodicidad.

- Cuando ocurra un cambio en la organización o en los Procesos que genere un impacto en la operación de la entidad.
- Cuando de incluya un nuevo proceso dentro del alcance de gestión de riesgo de la seguridad digital de la entidad.
- Cuando se reporte un incidente de seguridad de información que genere un impacto económico, de imagen o reputación

3.3.3 Reporte de la gestión del riesgo de seguridad digital a autoridades o entidades especiales

La entidad pública debe reportar los incidentes de seguridad digital a las autoridades o entidades especiales, cuando el incidente de seguridad digital genere un impacto económico y de imagen

3.3.4 Medición del Desempeño

La Gobernación del Departamento del Cesar, debe realizar las medidas de desempeño (indicadores) para la gestión de los riesgos de seguridad digital, con en el fin de medir la implementación del Plan.

3.4 Fase 4. MEJORAMIENTO CONTINUO DE LA GESTION DE RIESGO DE SEGURIDAD DIGITAL.

La Gobernación del Departamento del Cesar, debe realizar acciones que permitan garantizar el mejoramiento continuo de la gestión de riesgos de seguridad digital, en ese sentido deben existir políticas claras que establezcan las actividades a realizar, de tal forma que cuando se evidencien hallazgos, falencias o incidentes de seguridad digital, se tomen medidas para controlarlos y prevenirlos

Algunas acciones recomendadas por la guía de administración del riesgo de seguridad digital son las siguientes:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizados.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Empezar acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

4 CONTROLES DE REFERENCIA PARA LA MITIGACION DE RIESGOS DE SEGURIDAD DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

La entidad debería aplicar los controles establecidos en el Anexo A del estándar ISO/IEC 27001:2013 con el fin de mitigar y tratar los riesgos de seguridad digital.

5 PUBLICACIÓN

Su publicación se realizará a través de la página web, y en caso de modificación o actualización al “Plan de tratamiento de riesgo de seguridad de la información”, se realizará una nueva publicación por los medios dispuestos.

6 MEDIOS DE DIFUSIÓN

Los canales que se emplearán para la socialización del “Plan de tratamiento de riesgo de seguridad de la información” a nivel interno y externo se describen a continuación:

Tabla N° 34. DIFUSIÓN			
CANAL/MEDIO	ACTIVIDAD	PERIODICIDAD	RESPONSABLE
PÁGINA WEB http://cesar.gov.co/d/index.php/es/	Realizar la presentación del Plan de tratamiento de riesgo de seguridad de la información en el botón de	Anual	Profesional Especializado grupo de recursos físicos

	“Transparencia y acceso a la información pública”.		y tecnológicos/ Asesor TIC.
INTRANET ORION	Publicación del Documento: “Plan de tratamiento de riesgo de seguridad de la información” en la Sesión de “ Documentos ”	Anual	Profesional Especializado grupo de recursos físicos y tecnológicos/ Asesor TIC.
SISTEMA DE INFORMACIÓN DE GESTIÓN DOCUMENTAL CONTROL DOC	Circular de tipo de informativa explicando brevemente el “Plan de tratamiento de riesgo de seguridad de la información”, sus objetivos, y alcance.	Anual	Profesional Especializado grupo de recursos físicos y tecnológicos/ Asesor TIC.