UNIVERSIDAD EXTERNADO DE COLOMBIA

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

MAESTRÍA EN GERENCIA ESTRATÉGICA DE TECNOLOGÍA DE INFORMACIÓN

MODELO DE GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN PARA LA CONTRALORÍA GENERAL DE LA REPÚBLICA DE COLOMBIA

OLGA LUCIA GARCÍA VALENCIA

DIRECTOR DE TRABAJO DE GRADO: MÁSTER, SEGURIDAD DE LA INFORMACIÓN, ANDRÉS RICARDO ALMANZA JUNCO

BOGOTÁ

Julio, 2019

Dedicatoria y/o agradecimientos

Esta tesis de grado la dedicó primero a Dios, quien me fortalece y me guía en todo el proceso de conocimiento que he llevado en el transcurso de mi vida.

A mi hijo David Alejandro Valenzuela García, por su paciencia, apoyo y comprensión en los procesos académicos de su madre, quien siempre está en busca de la Excelencia y de sumergirse en el mar de conocimientos que tiene la disciplina a la que decidió dedicarse con mucho amor.

A mis padres Lelia María Valencia y Evelio García Marín, a mi abuela Ernestina Guañarita, quienes en vida me enseñaron el valor del estudio, la disciplina y quienes con su apoyo, hicieron de mí un gran ser humano, para desarrollar mi intelectualidad y encontrar el gusto de compartir mis conocimientos desde la docencia, con las personas que quieren aprender. Mil gracias.

Índice

Índice de Tablas

Índice de Figuras

Índice de Gráficas

Introducción

Este trabajo aborda la importancia de la seguridad de la información para todas las organizaciones, en especial las del Estado; como, a partir de las nuevas formas de transmisión de información y de las nuevas tendencias que surgen para realizar los trámites en línea los ciudadanos utilizan cada vez más los medios digitales como forma de interactuar con el Estado colombiano.

Así también, la Entidades del Estado buscando llegar a los lugares más lejanos, despliegan a través de los portales web, sistemas de información y aplicaciones nuevos trámites para que el ciudadano pueda acceder a éstos, agilizando los procesos para obtener los servicios que requiere en su interacción con los organismos públicos.

Se observa como el tema de gobierno de seguridad de la información para las entidades, cobra gran relevancia haciendo que se visualice como una sombrilla, que permite organizar la postura de seguridad de una organización y sus diferentes formas de dirigir, comunicar, evaluar y generar controles de seguridad para gobernar los recursos dirigidos hacia la seguridad y alineados con la estrategia de la entidad, con una adecuada administración de riesgos de seguridad de la información para minimizar que ésta pueda ser comprometida por alguna amenaza en su integridad, confidencialidad o disponibilidad.

Capítulo 1

Antecedentes

La información es muy importante, por ende su seguridad, es así como las organizaciones tienen una creciente dependencia de ésta y de los sistemas que la manejan, junto con los riesgos, beneficios y oportunidades que representan dichos recursos, esto ha hecho del gobierno de seguridad de la información un aspecto cada vez más crucial como dice (Tharakan, Devassy Jose, 2016, párr. 1) “la información es un activo vital para el negocio, pero no es siempre reconocida como tal. En el pasado se han desencadenado diversas fugas de información que han terminado por paralizar a muchas organizaciones”, lo que refuerza la importancia y la criticidad de la seguridad de información y su gobierno, que exigen un tratamiento de respaldo por parte de los niveles más altos dentro de la organización.

También sucede con el entorno digital al que se enfrentan las Entidades del Estado, la seguridad y la privacidad de la información tiene un nivel de riesgo, lo que hace importante su aseguramiento porque es transmitida por grandes redes a nivel global; la tendencia de publicar la información de la organización en la nube, hace que se encuentre distribuida en servidores de diferentes países, es por este intercambio de información que surgen nuevos esquemas de aseguramiento y control.

Existen desafíos y múltiples escenarios de riesgos emergentes que afectan las operaciones, la tecnología, la infraestructura y la información, por lo cual se debe tener presente que han surgido

nuevos modelos de negocios; en este sentido los Chief Information Officer (CIO) es decir los Directores de Información por su traducción al español, de la Corporate Executive Board Company (CEB), que es una subsidiaria de Gartner, compañía global de conocimientos y tecnología de mejores prácticas, ofrece productos y servicios a los líderes empresariales en Tecnologías de la información, diseña un estudio, basado en 4 arquetipos o modelos que las organizaciones han ido implementando para desarrollar su función de seguridad de la información.

Si bien la función de seguridad de información se ha convertido en un factor de alto impacto y relevancia para la Contraloría General de la República (CGR); la preocupación no es solo ser productivos, eficientes, eficaces y generar mejores servicios para la ciudadanía y/o el cliente en general, sino también la protección de la información para garantizar la continuidad del negocio en todos sus procesos, máxime en los de misión crítica con el fin de evitar sanciones y pérdida de reputación. (Cano M, 2016)

Ésta entidad pertenece al sector gobierno, su entorno está regido por el cumplimiento de las políticas públicas y aspectos legales, la protección de la privacidad y seguridad de la información es necesaria, por lo que su postura en relación con la seguridad de información está alineándose a un modelo de operaciones, gobierno y aspectos legales en razón a que su entorno de riesgo y cumplimiento es el predominante. (Cano M, 2016)

La Contraloría General de la República (CGR) está expuesta a múltiples riesgos debido a amenazas o ataques, por la incorporación de nuevas tecnologías; así como, al cumplimiento de la

normatividad vigente respecto a la materia de la protección y privacidad de la información, por lo cual es importante contar con un *modelo de gobierno de seguridad de la información,* que facilite la orientación sobre los principios y conceptos para gobernar los componentes que hacen parte de la función de seguridad de la información en la CGR.

Problemática

Para la CGR es importante gobernar la seguridad de la información que trata y maneja en cumplimiento de su función constitucional, la cual se debe administrar y gestionar al interior de la organización en respuesta a la necesidad de un entorno digitalmente confiable que es la seguridad digital que está dada como directriz desde los lineamientos del Gobierno Nacional.

Una necesidad que se requiere cubrir con la propuesta de modelo de gobierno de seguridad de la información que se plantea en este documento, es fortalecer dicha capacidad de seguridad digital en respuesta al CONPES 3854 (Departamento Nacional de planeación, 2016. p.27) que dice:

> Así las cosas, la política nacional de seguridad digital: (i) adoptará la gestión sistemática y cíclica del riesgo; (ii) será liderada desde el alto nivel del gobierno; (iii) asegurará la defensa y seguridad nacional; (iv) estimulará la prosperidad económica y social; (v) adoptará un enfoque multidimensional, es decir, la seguridad digital será abordada tanto desde la dimensión técnica o jurídica, como desde la dimensión económica y social; (vi) tendrá en cuenta a las múltiples partes interesadas; (vii) promoverá la responsabilidad compartida; (viii)

> salvaguardará los derechos humanos; (ix) protegerá los valores nacionales; y (x) concientizará y educará.

En razón a esta política que busca que todas las partes interesadas se involucren, y apliquen en sus entornos internos estos ítems planteados en el párrafo anterior, la Contraloría General de la República (CGR), como Entidad del Gobierno nacional requiere alinearse a esta normatividad y generar elementos que le permitan cumplir, es por esto que el modelo de gobierno de seguridad de la información que se plantea en esta tesis busca definir las dimensiones de seguridad de la información al interior de la CGR, para fortalecer la seguridad digital promoviendo mayor confianza al ciudadano.

Actualmente, la Entidad carece de una visión holística de seguridad de la información, que conlleva a la CGR a no tener una postura de seguridad de la información definida, pese a que viene trabajando en diversos flancos para alinear esta capacidad con los objetivos estratégicos; ha ido asumiendo buenas prácticas como implementar el Gobierno de Tecnologías de la Información liderado por la Oficina de Sistemas e Informática, generar la capacidad de arquitectura empresarial, dar sus primeros pasos para iniciar con un Sistema de Gestión de Seguridad de la Información (SGSI), del cual hasta ahora solo se tiene una base de documentos de políticas; sin embargo, estos esfuerzos están desarticulados y no existe un gobierno de la seguridad de información.

Es necesario definir funciones, roles y responsabilidades sobre la seguridad de la información porque en este momento no se tiene claras, ¿qué hace la Oficina de Sistemas e Informática? y

¿qué hace la Unidad de seguridad y aseguramiento tecnológico e informático?; en varias oportunidades se traslapan o duplican la actividades, no se tiene claridad de quien realiza la función de monitoreo y correlación de eventos, se han definido políticas desde las dos oficinas y no hay claridad de quien gobierna la seguridad de la información; es por esto, que es pertinente establecer cómo se articulan los diferentes componentes que hacen parte del gobierno de seguridad de la información y cómo interactúan con las oficinas involucradas.

En la siguiente tabla se muestran las funciones actuales que tienen las Oficina de sistemas e Informática (OSEI) y la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI) y se relaciona de acuerdo a la percepción que tiene el investigador por ser funcionario de la Contraloría General de la República, el porcentaje % de participación en cada una ellas.

Tabla 1. Participación funciones Seguridad de Información Dependencias con el rol en la CGR

Funciones según Decreto 267 de 2000 para la Oficina de Sistemas e Informática	**Participar USATI %**	**Participar OSEI %**
1. Asistir al Contralor General y por su conducto a la administración de la Contraloría General de la República, en el desarrollo de los sistemas, normas y procedimientos de informática requeridos por las dependencias de la entidad.	70% relacionados con SI	30% en las relacionadas con SI

2. Elaborar los diseños de programas, la codificación y las otras tareas requeridas para la programación de reportes y cómputo de información.	20% apoyo códigos seguros	80%
3. Determinar las tecnologías y técnicas requeridas para la recolección, el procesamiento y la emisión de información.	30% asegurando técnicas	70%
4. Establecer los controles sobre utilización de equipos y verificar la calidad del trabajo que se realice sobre los mismos.	50%	50%
5. Asesorar en el procesamiento de la información que requieran las diferentes dependencias de la Contraloría General de la República.	30% verificación de controles	70%
6. Realizar investigaciones para diseñar y sugerir la utilización óptima de equipos electrónicos, de los sistemas y del software.	40% diseños seguros	60%
7. Realizar estudios que permitan determinar la factibilidad técnica y económica de sistematizar las aplicaciones que requiera la Contraloría General de la República.	50% Aportar en factibilidad de seguridad de aplicaciones	50%
8. Realizar o participar técnicamente en los	50%	50%

procesos de contratación tendientes al análisis, diseño y programación de las aplicaciones que vayan a ser sistematizadas.	Proponer y participar en asegurar el desarrollo de software	
9. Elaborar los diferentes manuales de aplicación ajustados a las normas existentes.	10% verificar que los manuales aborden la seguridad	90%
10. Realizar el mantenimiento adecuado a los programas de computación para satisfacer los cambios en las especificaciones de los sistemas.	10% verificar si los cambios afectan la seguridad	90%
11. Establecer los controles necesarios para llevar el historial de las modificaciones que se efectúen en los programas o aplicaciones.	30% verificación de controles, seguimiento, auditorias a modificación	70%
12. Velar por la seguridad del acceso a las instalaciones donde se encuentren los equipos electrónicos.	70% Supervisar el diseño, implementación y mantenimiento de los dispositivos de acceso a las instalaciones.	30% Velar por cumplimiento controles físicos
13. Definir las prioridades y prestar los servicios de cómputo que se requieran.	30% verificar permisos y autorizaciones a los servicios	70%
14. Dictaminar sobre requerimientos de	30% verificar y auditar que	70%

mantenimiento y conservación de los equipos por las diferentes dependencias y garantizar las reparaciones correspondientes.|	se realicen mantenimientos con seguridad de personal y de que la información del dispositivo no quede expuesta a quien realiza la reparación o mantenimiento	
Funciones Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI) según Ley 1474 2011(Secretaria de Transparencia Presidencia de la República, 2016)	**Participar USATI**	**Participar OSEI**
Prestar apoyo profesional y técnico para la formulación y ejecución de políticas y programas de seguridad sobre personas, bienes e información;	80% Lineamientos de seguridad de Información para la Entidad	20% Procedimientos de seguridad informática y operacional
Llevar el inventario de los equipos de seguridad, así como garantizar su adecuado uso y mantenimiento	70% Llevar inventario y garantizar su seguridad mediante verificación	30% Custodiar el inventario de equipos de seguridad que tenga a su cargo

Promoverá la celebración de convenios con entidades nacionales y extranjeras que garanticen la seguridad de personas, bienes e información.	100%	

Así mismo, existe una metodología de riesgos de la entidad, pero aún no se han incluido los riesgos de seguridad digital, por lo que no existe una metodología que permita establecer y gestionar los riesgos de los activos de información; es importante aclarar que el Ministerio de Tecnologías de la Información y las Comunicaciones definió una guía para gestionar los riesgos de seguridad digital pero aún la entidad no ha incluido estas directrices en su metodología de riesgos.

Existe una problemática en la entidad sobre algunos riesgos que se han ido materializando a través de amenazas a las que se expone la organización, lo cual se muestra en la sección de Anexos como Eventos y amenazas de incidentes de seguridad de la información en la CGR, que fundamenta la necesidad de organizar un gobierno para minimizar estos incidentes.

Preguntas de Investigación

¿Qué modelo de Gobierno de Seguridad de la información es aplicable a la Contraloría General de la República, para fortalecer la seguridad de la información en la entidad, alineada con los objetivos misionales?

¿Qué componentes se debe contemplar o incluir para definir la postura de seguridad de la información en la Entidad?

Objetivos

Diseñar un modelo de gobierno de seguridad de la información para la Contraloría General de la República.

Identificar los componentes y las rutas que hacen parte del diseño del modelo de gobierno de seguridad de la información propuesto.

Alcance y Limitaciones

La propuesta de modelo de gobierno de seguridad de la información para la CGR incluirá y alineará los objetivos estratégicos de la entidad, los componentes del gobierno de Tecnologías de la Información (TI) y de Arquitectura empresarial proponiendo la articulación para ejercer un gobierno de seguridad de la información con el liderazgo de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático.

El nivel investigativo será cualitativo de acuerdo a flick (2009) citado por (Ugalde Binda & Balbastre-Benavent, 2013), este tipo de diseño es idóneo para:

> Estudiar los cambios que tienen lugar en los procesos de carácter social y organizativo. Dada la implicación del investigador cualitativo en el contexto de su estudio, el mismo se encuentra en una posición más favorable para ver las vinculaciones entre los eventos y las actividades, así como para explorar las interpretaciones que las personas hacen de los factores que producen dichas interconexiones.

Esta investigación es pertinente para el trabajo desarrollado por cuanto el investigador está implícito en el entorno y contexto de estudio, es decir, este trabaja en la Organización y en la dependencia orientada a la protección de la seguridad de la información, por lo que se cuenta con la visión de seguridad de la entidad, de sus procesos y de varios insumos necesarios para estructurar un adecuado modelo de gobierno de seguridad de la información.

Limitaciones

Se entregará el diseño del modelo de seguridad de la información para la CGR porque el tiempo dado es corto para realizar la implementación para la cual también se requieren recursos que son difíciles de conseguir rápidamente.

Será un modelo de gobierno de seguridad de la información, no abarcará todas las aristas de la seguridad integral (personas, bienes e información) de la CGR, por cuanto, no cubre la seguridad de personas y bienes, solo del componente de información, esto en razón a que la arista de personas está enfocada en la protección de servidores públicos amenazados en ejecución de sus funciones, y la seguridad de bienes es relacionada con la Gestión que realiza el Área de Recursos físicos y tiene relación con inventario de bienes muebles.

Justificación

Teniendo en cuenta que la Contraloría General de la República es un organismo rector del Control Fiscal, debe estar al día con los avances tecnológicos, alinearse y contribuir con la política digital del Estado Colombiano para estar a la vanguardia y fortalecer los vínculos entre las entidades gubernamentales y realizar un trabajo colaborativo que permita al país obtener un mejor desarrollo económico.

Es así que de acuerdo a los nuevos retos digitales se crea el Estatuto Anticorrupción Ley 1474 de 2011(Secretaria de Transparencia Presidencia de la República, 2016), por la cual se dictan normas y medidas administrativas para la lucha contra la corrupción establece en su artículo 128 el fortalecimiento institucional de la Contraloría General de la República y se crean dentro de su estructura varias dependencias, entre ellas la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI) cuyas funciones son: (i) prestar apoyo profesional y técnico para la formulación y ejecución de políticas y programas de seguridad sobre personas, bienes e información; (ii) llevar el inventario de los equipos de seguridad, así como garantizar su adecuado uso y mantenimiento; y (iii) promoverá la celebración de convenios con entidades nacionales y extranjeras que garanticen la seguridad de personas, bienes e información.

En alineación con los temas regulatorios y normativos, el CONPES 3854 de 2016, (Departamento Nacional de Planeación, 2016), define la Política Nacional de Seguridad Digital basada en el creciente uso de las Tecnologías de la Información y las Comunicaciones en todos los ámbitos socioeconómicos de Colombia, con el uso masivo de servicios en línea la población

se convierte en una *ciudadanía altamente digital*; pero en la misma línea también incrementan nuevas y sofisticadas formas de atentar contra la seguridad de las personas y del mismo Estado Colombiano, estamos hablando del *aumento de los riesgos relacionados con la seguridad digital*, proveniente de las nuevas interacciones del ciudadano con el gobierno.

Por las anteriores razones, la Contraloría General de la República (CGR) afronta el reto de dar cumplimiento a ésta política y afrontar los nuevos desafíos tecnológicos y riesgos asociados estableciendo medidas necesarias para contar con un *modelo de gobierno de seguridad de la información* que le permita alinearse con los objetivos estratégicos de la Organización, así como, armonizar todos los planes, procesos, políticas y demás componentes relacionados para fortalecer la capacidad de seguridad digital que es lo que busca el Gobierno colombiano con la política de Estado CONPES 3854.

Así también, definir una postura de seguridad de la información en la CGR, todo que confluya a propender por la confidencialidad, integridad y disponibilidad de la información de la CGR y el análisis de riesgo de los activos de información de la Entidad para fortalecer su capacidad de seguridad digital en los servicios que la CGR otorga al ciudadano.

El ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) “es consciente de que la misión de las instituciones es servir a los ciudadanos con un Estado abierto y transparente; con servicios y trámites ágiles y efectivos; con información precisa y de alta calidad; y con seguridad de los datos y los procesos públicos” (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018, párr. 3) es por esto que ha creado la estrategia de

Gobierno en Línea, el cual está dividido en cuatro ejes temáticos Tecnologías de la Información y las Comunicaciones para servicios, Tecnologías de la Información y las Comunicaciones para gestión, Tecnologías de la Información y las Comunicaciones para gobierno abierto y seguridad y privacidad de la información como se muestra en la Figura 1

Figura 1. Basada en Ejes de Gobierno en línea.

Fuente:(Ministerio de Tecnologías de la Información y las Comunicaciones, 2018)

Así mismo, la estrategia es soportada por unos componentes de la Arquitectura de Tecnologías de la Información, la cual se muestran en la Figura 2

Figura 2. Componentes de la Arquitectura de Tecnologías de la Información

Fuente: (Ministerio de Tecnologías de información y las comunicaciones, 2018)

De acuerdo a lo anterior, existen unas políticas de Estado que marcan la ruta a las entidades del Estado para aplicar el marco de referencia de Tecnologías de la Información, incorporar mejores prácticas para optimizar los trámites realizados por el ciudadano siendo más eficientes, allí es

donde la seguridad digital toma mayor importancia, porque, se requiere diseñar estrategias al interior de las entidades, que permitan tener un gobierno de seguridad de la información para proteger sus tres pilares, disponibilidad, confidencialidad e integridad, así como velar por la seguridad y privacidad de la información de los ciudadanos.

Dentro de los diferentes componentes la Contraloría bajo el programa de fortalecimiento Institucional (FOCO), da vida al Proyecto de Arquitectura Empresarial, cuyo alcance fue los Macroprocesos Misionales de la entidad, uno de los resultados de este ejercicio es un mapa de ruta a desarrollar al interior de la CGR y un consolidado de proyectos propuestos para poner en marcha la ruta destino propuesta en la Arquitectura empresarial que incluye los proyectos de seguridad de la información.

Es así que para mitigar los impactos a los que conlleva la materialización de los riesgos de seguridad de la información que enfrentan las entidades y en especial la Contraloría General de la República, la Unidad de Seguridad y Aseguramiento Tecnológico e Informático USATI, ve beneficioso para la entidad generar un modelo de gobierno de seguridad de la información que permita marcar la línea a seguir para fortalecer la capacidad de seguridad digital lo que redunda en confianza para el ciudadano en los trámites con la Entidad.

Capítulo 2

Revisión Literaria - Marco Teórico

Importancia de la Estrategia de Seguridad digital en el Estado Colombiano

La Estrategia Tecnologías de la Información está organizada para actuar desde siete campos de acción o iniciativas que fortalecen una gestión más organizada, para satisfacer a esos ciudadanos digitales quienes tienen ahora más capacidades de interacción tecnológica y cercanía al Estado, y una de éstas iniciativas tiene que ver con la Seguridad, que toma mayor importancia porque las amenazas informáticas a los sistemas del Estado son una constante preocupación, estos evolucionan; el Estado está fortaleciendo su capacidad de defensa cibernética a través de una estrategia nacional, con políticas, normatividad de prevención y generación de control. (Mintic, 2018a)

De acuerdo a lo que se describe:

> La sofisticación del uso y estrategia de Tecnología de Información conlleva a la necesidad y obligación de mejorar las herramientas de seguridad. En todo el mundo los ataques cibernéticos se han incrementado con métodos innovadores. En Colombia, las instituciones de seguridad se están vinculando a la Estrategia Tecnologías de la Información para aumentar la capacidad del Estado de enfrentar las amenazas informáticas, pues en el momento presenta grandes debilidades, pese a que existen iniciativas gubernamentales, privadas y de la sociedad civil que

> buscan contrarrestar sus efectos, no hay una coordinación interinstitucional apropiada. (Mintic, 2018b)

Las entidades de gobierno deben incrementar los niveles de madurez en seguridad digital que conlleve a generar confianza en el ciudadano para que él haga uso y apropiación de las Tecnologías de la Información y las Comunicaciones (Tecnologías de la InformaciónC) en su interacción con el Estado; la política del país desde el Gobierno central es generar capacidades, entre éstas la seguridad de la información.

Con toda esta nueva visión del gobierno colombiano se define el CONPES 3854 del 11 de abril de 2016 (Departamento Nacional de Planeación, 2016), por medio del cual se establece la política de Seguridad digital cuyo objetivo general es que los ciudadanos, las entidades del Gobierno y los empresarios conozcan e identifiquen los riesgos a los que están expuestos en el entorno digital y aprendan cómo protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos, y así generar directrices de política de Estado para que todas las entidades públicas tomen los lineamientos de esta política y marquen su ruta de seguridad digital con el fin de proteger y brindar privacidad a la información que maneje cada entidad.

Reseña Normativa

A continuación se relacionan una serie de normas y legislación desarrollada por el Estado colombiano para definir lineamientos y enfocar a las Entidades del Estado a la seguridad digital en todos sus procesos y servicios internos y con el ciudadano.

Es así como según (Ocampo, 2015) es la directiva presidencial No. 02 del 28 de agosto de 2000 la cual inicia a plantear la importancia de las tecnologías de la Información para todas las Entidades del Estado e inicia la obligatoriedad de cumplir con la Estrategia de Gobierno en línea, para integrar a los diversos actores de la economía nacional en el uso de las Tecnologías de la Información y las Comunicaciones (TIC).

> Así también, se encuentra que existe otra normatividad importante para fundamentar el tema de seguridad digital, por cuanto, se promueve las transacciones y los tramites en línea y se fortalece el Gobierno en línea, algunas de éstas normas se relacionan como lo indica (Ocampo, 2015, pp-1-2)
>
> La ley 790 de 2002, en su capítulo III de Gobierno en línea, art.14 promueve las transacciones en línea por parte del Gobierno Nacional.
>
> Ley 692 de 2005, establece disposiciones sobre la racionalización de trámites en las entidades públicas para incentivar el uso de las Tecnologías de la Información y las Comunicaciones (Tecnologías de la InformaciónC).
>
> Decreto 1151 de 2008 de Mintic establece lineamiento de Gobierno en línea, y se elabora el Manual de Gobierno en Línea.
>
> Decreto 2693 de 2012 estrategia de gobierno en línea y plazos que tienen las diferentes entidades del Estado para su cumplimiento.
>
> En el artículo 7 el Decreto 2693 constituye el modelo de gobierno en línea por 6 componentes un de los cuales es implementar un sistema de gestión de seguridad

de la información (SGSI) en las entidades del Estado y establece según el tipo de entidad dar cumplimiento a las acciones para cada componente.

Es importante nombrar la Ley de Habeas Data, es la 1266 de 2008 en esta se dictan “las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”, en esta también se define el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica” (El congreso de la República de Colombia, 2008, Párr.11),

Ley 1581 de 2012 es la ley para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales. (Congreso de la República de Colombia, 2012)

Según el Decreto 1377 del 27 de junio de 2013, tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información. (Presidencia de la República, 2013)

La Ley 1712 de 2014 o de Transparencia y del Derecho de Acceso a la Información Pública Nacional es una norma que regula el ejercicio del derecho fundamental de acceso a la información pública en Colombia, su objetivo es:

> Que la información que tienen posesión, custodia o bajo control de cualquier entidad pública, órgano y organismo del Estado colombiano, persona natural o jurídica de derecho privado que ejerza función pública delegada, reciba o administre recursos de naturaleza u origen público o preste un servicio público, esté a disposición de todos los ciudadanos e interesados de manera oportuna, veraz, completa, reutilizable y procesable y en formatos accesibles. (Secretaria de Transparencia; Presidencia, 2015).

También se encuentra la Ley de Delitos Informáticos que es a 1273 de 2009, "Por medio del 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", es así como esta Ley también tipifica como delitos una serie de conductas relacionadas con el manejo de datos personales, como son: acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso y violación de datos personales. (Congreso de la república de colombia, 2009).

El decreto 1078 de 2015 por medio del cual se expide el decreto único reglamentario del sector de las tecnologías de la información y las comunicaciones expedido por este mismo Ministerio, en la sección 2 artículo 2.2.9.1.2.1 establece los componentes que facilitarán la masificación de la oferta y la demanda de gobierno en línea, y es así como uno de los componentes relacionado en el ítem 4 es el componente de seguridad y privacidad de la información el cual comprende las acciones transversales los demás componentes los cuales son Tecnologías de la Información y las comunicaciones (TIC) para servicios, Tecnologías de la Información y las comunicaciones (TIC) para el gobierno abierto y Tecnologías de la Información y las comunicaciones (TIC) para la Gestión, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada. (Ministerio de las Tecnologías y las Comunicaciones, 2015)

Finalmente, para dar un mayor panorama en el tema normativo de seguridad digital en la sección de anexos de este trabajo bajo el título Anexo Normativa de Seguridad Digital se relacionan la normatividad relacionada por el Consejo Nacional de Política Económica y Social CONPES 3854 en su anexo C sobre este tema.

Familia de normas ISO27000

La familia de normas Internacional Organization for Standardization (ISO) 27000 es un conjunto de normas realizadas por la Organización Internacional de Normalización que facilitan

un marco de gestión de la seguridad de la información se puede aplicar en cualquier tipo de organización o privada o pública, sin importar el tamaño.

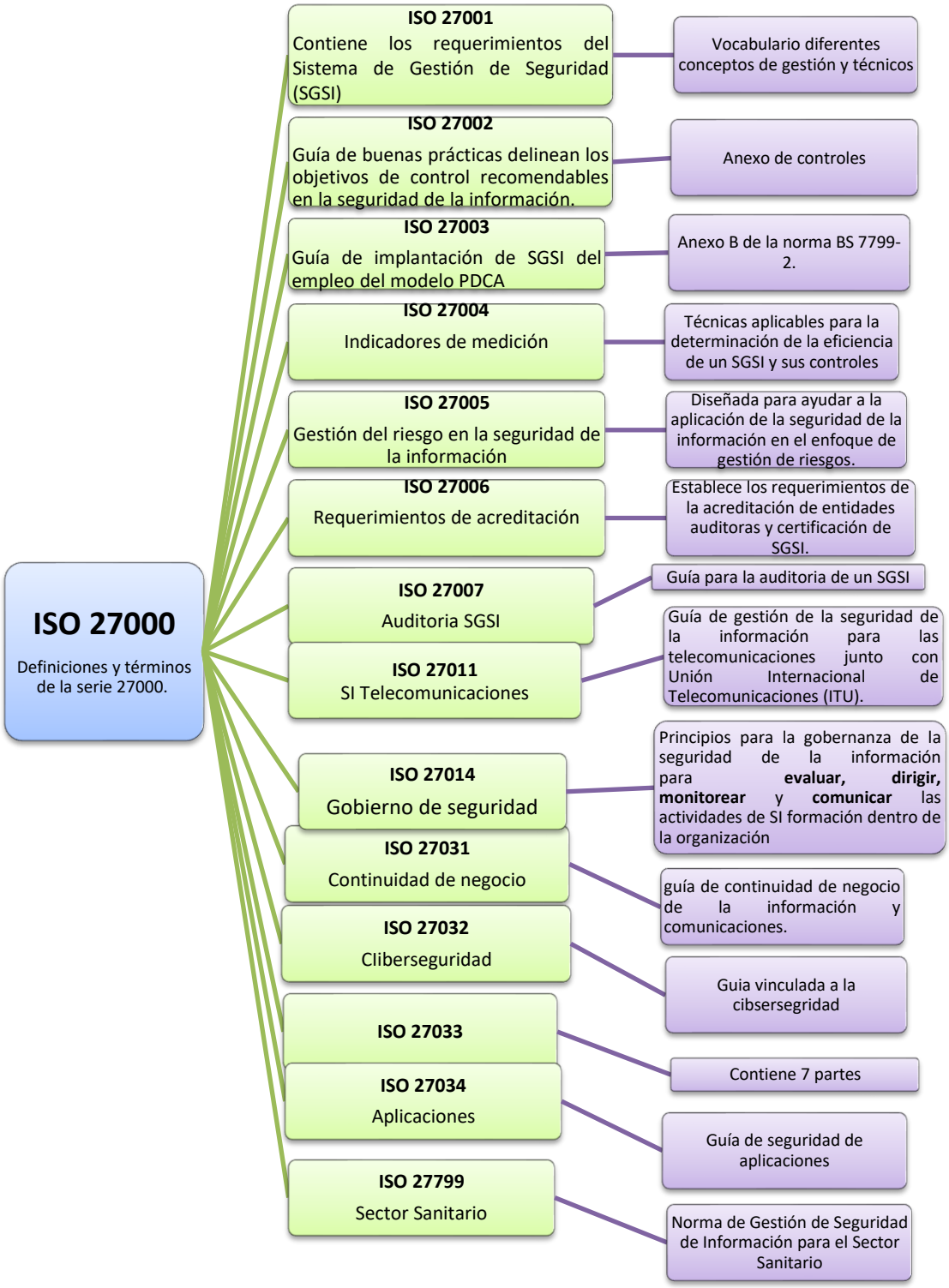
Los beneficios de la norma ISO 27000 según (ISO, 2013) son:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

A continuación se muestra el detalle de normas de la familia ISO 27000 y su aplicación de acuerdo a (ISOtools Excellence, 2014)

Figura 3. Familia de Normas ISO 27000



Fuente: Imagen elaboración propia basada en (ISOtools Excellence, 2014)

Sistema de Gestión de Seguridad de la Información

Según (Lopez, 2012) dice que el Sistema de Gestión de Seguridad de la Información (SGSI) es como "la gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización", el propósito es propender que los riesgos de la seguridad de la información sean gestionados, de manera que traten en forma adecuada, asumiéndolos, minimizándolos o trasladando a un tercero, proceso que debe ser repetible y de acuerdo a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En la figura 3 se muestra el ciclo de implementación del Sistema de Gestión de Seguridad de la información, basado en el ciclo de Deming con éste se abordan las actividades para cada fase, las cuales después de ser desarrolladas permiten establecer un proceso sistémico para gestionar los riesgos, asegurar el cumplimiento normativo aplicable y tener una planeación adecuada para abordar la gestión y aseguramiento de la información en cualquier organización.

Es importante resaltar que para la implementación del Sistema de Gestión de Seguridad SGSI en una organización su base está dada por la ISO 27001 que es la que es certificable y establece los requerimientos del SGS (Sistema de Gestión de Seguridad) de la información, los mínimos claves son: compromiso y apoyo de la Dirección de la organización, definición clara del alcance del sistema, concienciación y formación del personal en seguridad de la información (cultura), evaluación de riesgos para la organización, compromiso de mejora continua por la dirección con evidencias, establecimiento de políticas y normas, organización y comunicación,

gestión adecuada de la continuidad de negocio, de los incidentes de seguridad, del cumplimiento legal y de la externalizarían e integración del SGSI en la organización.(ISO, 2013)

Figura 4. Ciclo de vida para la implementación del SGSI

Fuente: Imagen elaboración propia basada en el Ciclo de Deming (ISO27000.es, 2012).

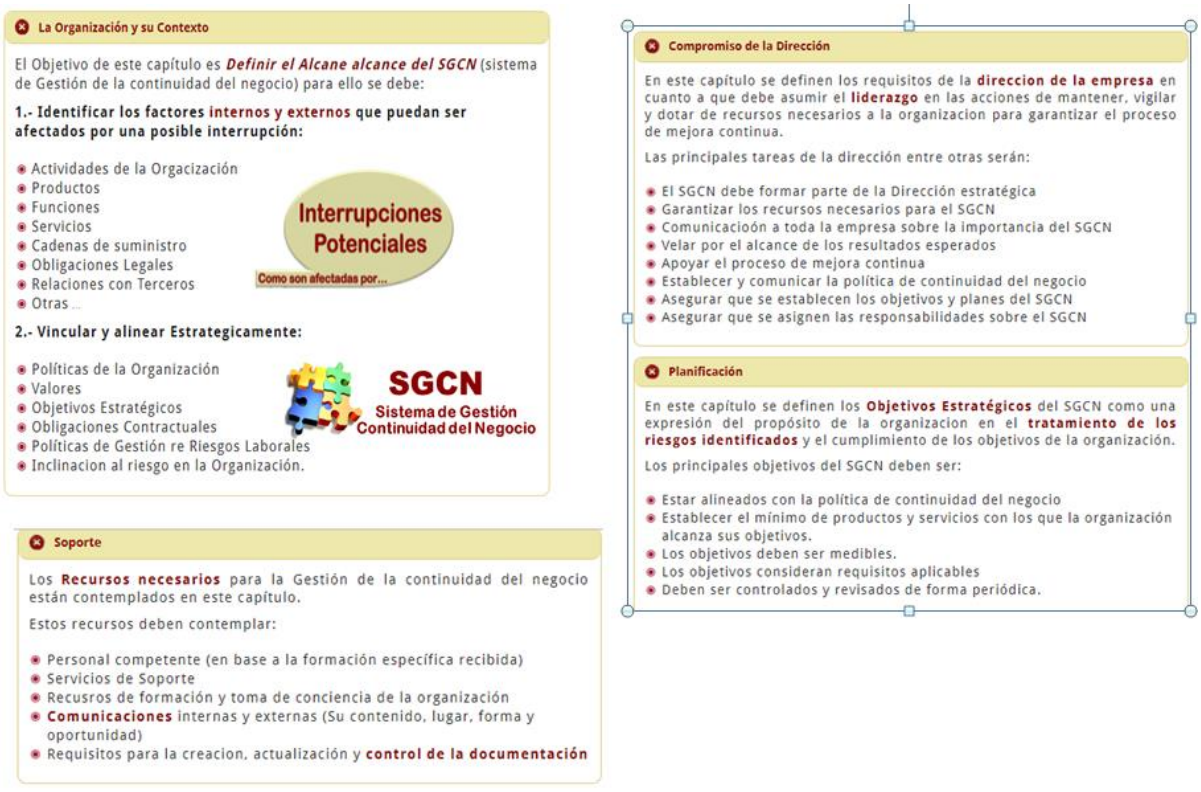
El sistema de gestión de seguridad de la Información (SGSI) es una metodología estructurada que permite a las organizaciones realizar de manera organizada el aseguramiento de la información desde la definición del sistema, los documentos de lineamientos sobre la gestión de la información, la administración y tratamiento de riesgos, hasta los procesos de mejoramiento continúo después de realizar la verificación del cumplimiento del sistema a través de auditorías; esto hace que se gestione y aseguren adecuadamente los activos de información a través de clasificarlos priorizarlos, identificar y gestionar riesgos para asignar controles y poder minimizar que la información sea vulnerable.

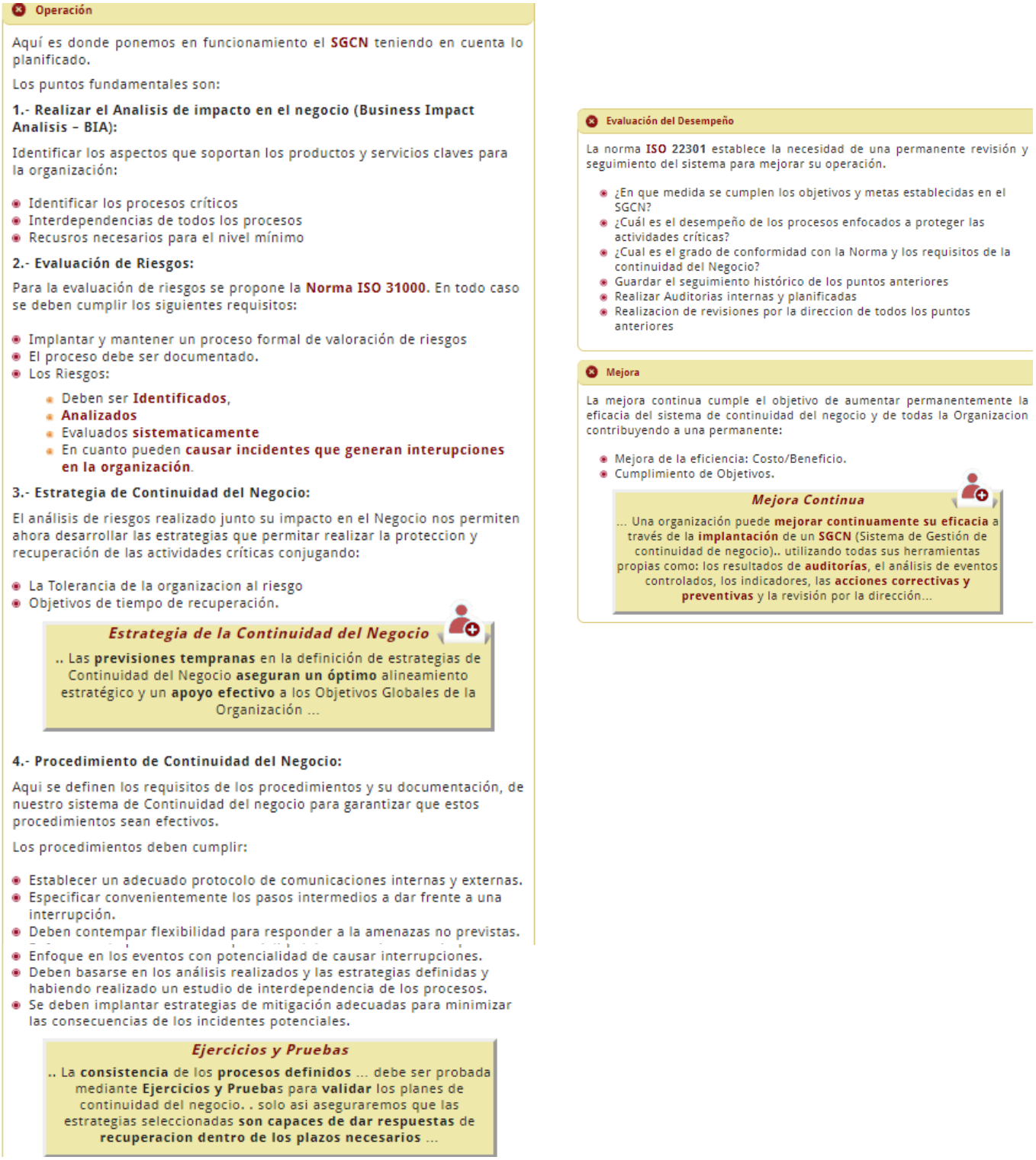
Norma ISO 22301 para Continuidad del Negocio

Un Sistemas de Gestión de la Continuidad del Negocio permite a la organización restablecer su operación después de que surja algún desastre y haya existido interrupción del negocio, con el fin de proteger la reputación, el cumplimiento, la satisfacción del cliente y evitar posibles pérdidas a nivel económico. (ISOTools, 2016)

Esta norma establece los requisitos a seguir para el Sistema de Gestión de la Continuidad de Negocio; sus principales capítulos y actividades a realizar para implementar este sistema se muestran a continuación:

Figura 5. Contenido de la Norma ISO 22301





Operación

Aquí es donde ponemos en funcionamiento el **SGCN** teniendo en cuenta lo planificado.

Los puntos fundamentales son:

1.- Realizar el Analisis de impacto en el negocio (Business Impact Analisis – BIA):

Identificar los aspectos que soportan los productos y servicios claves para la organización:

- Identificar los procesos críticos
- Interdependencias de todos los procesos
- Recusros necesarios para el nivel mínimo

2.- Evaluación de Riesgos:

Para la evaluación de riesgos se propone la **Norma ISO 31000.** En todo caso se deben cumplir los siguientes requisitos:

- Implantar y mantener un proceso formal de valoración de riesgos
- El proceso debe ser documentado.
- Los Riesgos:
  - Deben ser **Identificados**,
  - **Analizados**
  - Evaluados **sistematicamente**
  - En cuanto pueden **causar incidentes que generan interupciones en la organización**.

3.- Estrategia de Continuidad del Negocio:

El análisis de riesgos realizado junto su impacto en el Negocio nos permiten ahora desarrollar las estrategias que permitar realizar la proteccion y recuperación de las actividades críticas conjugando:

- La Tolerancia de la organizacion al riesgo
- Objetivos de tiempo de recuperación.

Estrategia de la Continuidad del Negocio

.. Las **previsiones tempranas** en la definición de estrategias de Continuidad del Negocio **aseguran un óptimo** alineamiento estratégico y un **apoyo efectivo** a los Objetivos Globales de la Organización ...

4.- Procedimiento de Continuidad del Negocio:

Aqui se definen los requisitos de los procedimientos y su documentación, de nuestro sistema de Continuidad del negocio para garantizar que estos procedimientos sean efectivos.

Los procedimientos deben cumplir:

- Establecer un adecuado protocolo de comunicaciones internas y externas.
- Especificar convenientemente los pasos intermedios a dar frente a una interrupción.
- Deben contemplar flexibilidad para responder a la amenazas no previstas.
- Enfoque en los eventos con potencialidad de causar interrupciones.
- Deben basarse en los análisis realizados y las estrategias definidas y habiendo realizado un estudio de interdependencia de los procesos.
- Se deben implantar estrategias de mitigación adecuadas para minimizar las consecuencias de los incidentes potenciales.

Ejercicios y Pruebas

.. La **consistencia** de los **procesos definidos** ... debe ser probada mediante **Ejercicios y Pruebas** para **validar** los planes de continuidad del negocio. . solo asi aseguraremos que las estrategias seleccionadas **son capaces de dar respuestas** de **recuperacion dentro de los plazos necesarios** ...

Evaluación del Desempeño

La norma **ISO 22301** establece la necesidad de una permanente revisión y seguimiento del sistema para mejorar su operación.

- ¿En que medida se cumplen los objetivos y metas establecidas en el SGCN?
- ¿Cuál es el desempeño de los procesos enfocados a proteger las actividades críticas?
- ¿Cual es el grado de conformidad con la Norma y los requisitos de la continuidad del Negocio?
- Guardar el seguimiento histórico de los puntos anteriores
- Realizar Auditorias internas y planificadas
- Realizacion de revisiones por la direccion de todos los puntos anteriores

Mejora

La mejora continua cumple el objetivo de aumentar permanentemente la eficacia del sistema de continuidad del negocio y de todas la Organizacion contribuyendo a una permanente:

- Mejora de la eficiencia: Costo/Beneficio.
- Cumplimiento de Objetivos.

Mejora Continua

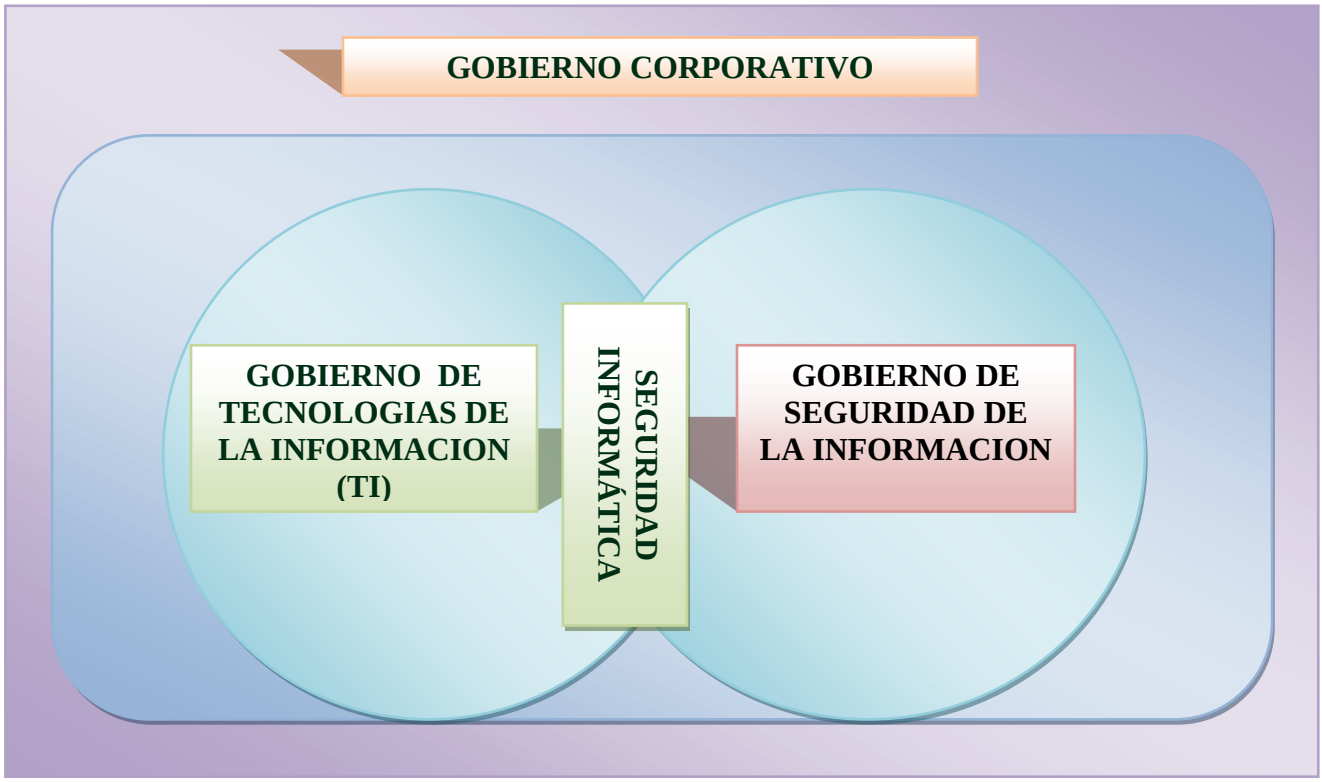
... Una organización puede **mejorar continuamente su eficacia** a través de la **implantación** de un **SGCN** (Sistema de Gestión de continuidad de negocio).. utilizando todas sus herramientas propias como: los resultados de **auditorías**, el análisis de eventos controlados, los indicadores, las **acciones correctivas y preventivas** y la revisión por la dirección...

Fuente: (ISO 22301 Sistema de Gestión y Continuidad del Negocio, 2016)

Integración entre Gobierno Corporativo, Gobierno de Tecnologías de la Información y Gobierno de Seguridad de la Información

El siguiente grafico muestra la integración entre el Gobierno Corporativo, Gobierno de Tecnologías de la Información, Gobierno de Seguridad de la Información y la seguridad informática en las organizaciones.

Figura 6. Integración del Gobierno Corporativo, Gobierno de Tecnologías de la Información y Gobierno de Seguridad de la Información



Fuente. Elaboración propia basa en (Augusto & Focazzio, 2011, p.10)

El Gobierno corporativo es el gran marco donde se realiza a nivel de organización lo siguiente.: ► Proveer dirección estratégica. ► Asegurar el logro de los objetivos.► Establecer que los riesgos se administran adecuadamente.► Verificar que los recursos de la empresa se utilizan responsablemente.

El Gobierno de Tecnologías de la información (TI), hace parte del Gobierno Corporativo y enfatiza la alineación de los objetivos estratégicos de las organizaciones con los del área de Tecnologías de la Información, así las inversiones y acciones que se realicen en tecnología son acordes a lo que necesita la empresa y se alinea a la estrategia; para esto, es fundamental dirigir y monitorear las iniciativas y planes de Tecnologías de la Información, orientando y ejerciendo una dirección para llevar a cabo las estrategias de Tecnologías de la Información acorde con lo que está solicitando el negocio para cumplir su misión.

La seguridad informática es la que implementa las medidas técnicas que preservan las infraestructuras y de comunicación que soportan la operación de una empresa, normalmente es un área que hace parte de la Oficina de Sistemas o de Tecnología.

Y el gobierno de la seguridad de la información hace parte del gobierno corporativo al proporcionar una dirección estratégica a las actividades de la seguridad y garantizar que se alcancen los objetivos, así también hace que los riesgos relacionados con la seguridad de la información se administren y se gestionen adecuadamente y que los recursos de información de la empresa se utilicen con responsabilidad. (Augusto & Focazzio, 2011, p.9)

Para establecer la integración entre el Gobierno Corporativo, el Gobierno de Tecnologías de la Información y el Gobierno de Seguridad de la Información también es pertinente revisar algunos conceptos así:

Según (ISO/IEC Organización Internacional de Normalización, 2013) citado por (Evans, 2011, p.5) es "El gobierno corporativo es la forma como se toman decisiones corporativas después de ajustar los intereses de los interesados, para definir la dirección y para ejecutar las decisiones tomadas."

De acuerdo al (Information Security Forum, 2011) citado por (Evans, 2011, p.6) el gobierno corporativo es "un marco de acción demostrable para operar una organización a niveles aceptables de riesgo, cumpliendo a cabalidad con los requerimientos regulatorios y legales y garantizando la protección de valor de los interesados"

Así también, para todas las organizaciones es importante contar con un Gobierno de Tecnologías de la Información (TI), que establece "los estándares para un buen gobierno de los procesos y decisiones empresariales relacionados con los servicios de información y comunicación que, suelen estar gestionados tanto por especialistas en Tecnologías de la Información y las Comunicaciones (TIC) internos o ubicados en otras unidades de negocio de la organización" (Ballester, 2018), el cual se enmarca en la norma ISO 38500.

El termino de Gobierno de TI se utiliza desde el año 2003, como lo indica (Vargas-Bermúdez, 2017, p. 4), "es una parte integral del gobierno de la organización y consiste en el

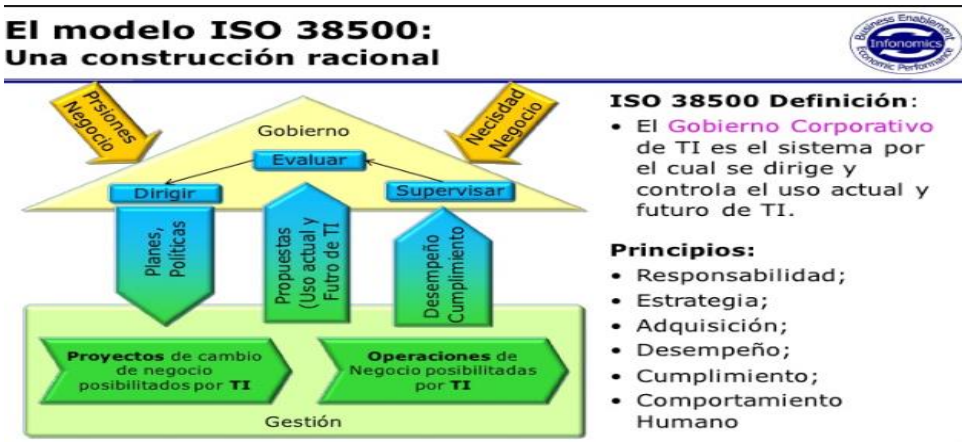
liderazgo de las estructuras y procesos organizativos que aseguran que las Tecnologías de la Información de la organización sostienen y extienden la estrategia y los objetivos de la organización".

El estándar ISO 38500, establece una serie de principios como lo indica (Francavilla, 2014a) *responsabilidad*, permite que todos comprendan y acepten sus responsabilidades en la oferta o demanda de Tecnologías de la Información y la autoridad para su realización, la *estrategia de negocio de la organización*, toma en cuenta las capacidades actuales y futuras de Tecnologías de la Información, define planes estratégicos de Tecnologías de la Información y satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio, *adquisiciones de Tecnologías de la Información* se realizan alineadas a los objetivos estratégicos, con un apropiado análisis y decisiones claras y transparentes, equilibrio entre beneficios, oportunidades, costes y riesgos.

También, es importante el *Desempeño Tecnologías de la Información*, para dar soporte con calidad cubriendo los requerimientos de necesidades de las organizaciones actuales y futuras, *cumplimiento*, la función de Tecnologías de la Información tiene temas de cumplimiento de las normatividad vigente. Las políticas y prácticas estén definidas, implementadas y exigidas con claridad. Y *el comportamiento humano*, las decisiones, políticas, prácticas de Tecnologías de la Información tienen en cuenta necesidades actuales y emergentes de todo el talento humano. (Francavilla, 2014b)

La figura 4 muestra el modelo de gobierno de Tecnologías de la Información y describe los principios que lo fundamentan los cuales fueron explicados anteriormente.

Figura 7. Corporativo de Tecnologías de la Información - ISO 38500



Fuente:(Francavilla, 2014)

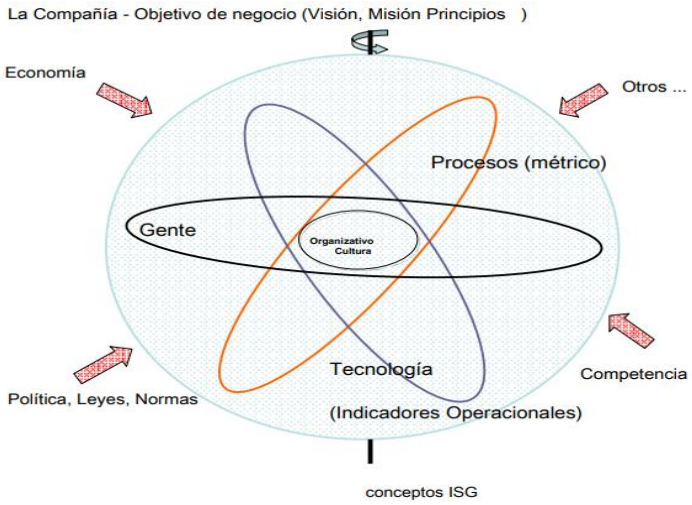
En cuanto a los beneficios de gobierno de Tecnologías de la Información según (Ballester, 2018) facilita el cumplimiento de legislación, estándares, normatividad de todo tipo aplicable a la organización, así como un buen rendimiento de las Tecnologías de la Información y las Comunicaciones (TIC), lo que implica implementación y operación de los activos de información, claridad de la responsabilidades, sostenibilidad del negocio, alineación de las Tecnologías de la Información y las Comunicaciones (TIC) a los objetivos del negocio, asignar recursos en forma eficiente, innovación en servicios y mercados, mejora en relaciones con los interesados, reducción de costes, materialización efectiva de beneficios esperados en cada inversión en Tecnologías de la Información y las Comunicaciones (TIC).

Según (Sylvester, 2011, Párr.3) [Texto traducido del inglés] la ISO 38500 estructura la "gobernanza eficaz de las Tecnologías de la Información para ayudar a los que están en el más alto nivel de las organizaciones a entender y cumplir con sus obligaciones legales, reguladoras y éticas relacionadas con el uso de las Tecnologías de la Información de sus organizaciones"

Es así que para garantizar protección a la Información que es administrada por el Gobierno de TI se requiere contar con un Gobierno de seguridad de la información de acuerdo al texto (De Oliveira Alves, Gustavo Alberto; Da Costa Rust Carmen, Luiz Fernando; Ribeiro de Almeida Dutra, 2006) y como lo muestra la figura 5 es:

> El acto de dirigir y controlar una organización alineada con los objetivos de la estrategia y de negocios, establecer y mantener una cultura de seguridad de la información, la optimización de los procesos relacionados (basados en indicadores y lecciones aprendidas) , y la asignación de actividades a las personas más competentes para llevar a cabo las acciones necesarias. El consejo de administración debe apoyar todas aquellas acciones.

Figura 8. Conceptos de Gobierno de Seguridad de la Información (ISG)



Fuente: (De Oliveira Alves, Gustavo Alberto; Da Costa Rust Carmen, Luiz Fernando; Ribeiro de Almeida Dutra, 2006b. P.72)

El gobierno de seguridad de la información fija los componentes para brindar la dirección y definición de una postura de seguridad de la información en la organización, para utilizar un enfoque estructurado con el fin de implementar un programa de seguridad que permita dirigir y orientar la seguridad de información acorde y alineada a los objetivos estratégicos del negocio.

Un modelo de gobierno de seguridad de la información, se da a partir de la postura de seguridad de la información definida por la entidad, adoptando los lineamientos y buenas prácticas que existen sobre la materia como lo es la norma NTC/ISO 27014:2013 (ISO/IEC Organización Internacional de Normalización, 2013) relacionadas con el gobierno de seguridad de la información, mediante la cual las organizaciones pueden evaluar, dirigir, monitorear y comunicar las actividades relacionadas con la seguridad de la información dentro de la

organización, así como gestionar los riesgos de seguridad de la información, establecer el nivel de apetito del riesgo y protección de activos de información de acuerdo a su clasificación.

La norma ISO / IEC 27014 de acuerdo a al sitio de la norma (ISO / IEC, 2013, párr.3) dice que la adecuada gestión de la seguridad de la información "*garantiza la alineación de la seguridad de la información con las estrategias y los objetivos empresariales , la entrega de valores y la responsabilidad . Apoya el logro de visibilidad, agilidad, eficiencia, efectividad y cumplimiento*".

Importancia de tener una gobierno de seguridad de la Información

En la actualidad la información para todas las empresas se vuelve un activo fundamental sin el cual sería imposible dirigir las organizaciones la cual se transforma en conocimiento para las empresas y se transmite por medios digitales; es así como a partir de ella se fundamentan decisiones y estrategias en el desarrollo de las metas y objetivos de cualquier organización, en razón a esto surge la necesidad y la importancia de contar con un gobierno de seguridad de la información que permita articular todos los componentes necesarios para direccionar en forma eficiente el aseguramiento de la información, permitiendo la protección de sus pilares principales como son integridad, disponibilidad y confidencialidad.

En la figura 6 que se muestra a continuación, se puede observar que la parte del Security Assurance SGSI Sistema de Gestión de Seguridad de la información se refiere al proceso de aseguramiento de la seguridad como un proceso sistemático de seguridad de la información y se

enfatiza en la gestión de riesgos y controles sobre los activos de información, es decir es la parte táctica, lo que tiene que ver con la operación, esto se da a partir de unos lineamientos y procesos definidos para la administración de éstos desde el gobierno de seguridad.

En cambio, el segundo referente a gobierno de seguridad tiene que ver con la alineación de la seguridad con la estrategia del negocio, establecer la metodología de riesgos, el apetito del riesgo, establecer políticas y dirigir las acciones requeridas para proveer los recursos y lineamientos necesarios para dar una dirección a la seguridad de la información en una organización.

Comparación entre la Gestión de la Seguridad o Security Assurance (SGSI) y el Gobierno de Seguridad

Figura 9. Diferencia entre la Gestión de la Seguridad Security Assurance (SGSI) y Gobierno de seguridad

Security Assurance (SGSI)	Gobierno de Seguridad
Desarrollo e implementación de políticas de seguridad	Alineación de la seguridad con la estrategia de negocio
Ejecución de programas de sensibilización en seguridad	Relacionar el gobierno de seguridad con los requerimientos del gobierno corporativo
Creación de los esquemas de clasificación de información y garantizar que se implementa en toda la organización	Establecer la política
Ejecución de los análisis de riesgos de información	Proveer los recursos apropiados (tanto dinero como personas)
Validar el estado de la seguridad	Determinar el apetito de riesgo
Gestionar el proceso de respuesta ante incidentes	Establecer tablas de impacto
Proveer consejo y guía	Comunicarse con los interesados en el gobierno (ej. la junta, inversores, clientes, reguladores)

Fuente: (Evans, 2011)

Para mayor ilustración se observa en la figura 6 las diferencias entre asegurar la información y gobernarla, allí podemos ver como el aseguramiento está vinculado con el desarrollar e implementar las políticas de seguridad de la información, establecer los controles, mecanismos y procesos que permitan como su nombre lo indica la gestión y protección de la información, como dice (Cano M, 2013, pp.14) tiene que ver con la función de seguridad, es la caja de herramientas, una serie de actividades y acciones sin un propósito definido.

Es así, como es necesario completar esa caja de herramientas agregando un propósito el cual fundamenta el Gobierno de seguridad de la información, que es la parte naranja de la figura 6 y que se relaciona con alinear la seguridad de la información, con los objetivos estratégicos de la organización y dirigir desde el gobierno corporativo las estrategias que permiten generar acciones que orienten y dirijan la seguridad de la información con el fin de protegerla y salvaguardarla de los riesgos a que pueda estar expuesta.

Debido a lo anterior, han surgido nuevos modelos de negocios los especialistas de CIO executive board (CEB) (Cano M, 2016 pp.116-117) han diseñado un estudio basado en 4 arquetipos relacionados en la Tabla 3.

Tabla 2. Arquetipos de la función de seguridad de la información

Énfasis	**Operaciones**	**Gobierno**	**Operaciones y Gobierno**	**Operaciones, Gobierno, asp. legales**

Énfasis	Operaciones	Gobierno	Operaciones y Gobierno	Operaciones, Gobierno, asp. legales
Responsabilidades	• Seguridad informática • Monitoreo y análisis de eventos. • Respuestas incidentes y análisis forense • Gestión de Vulnerabilidades y amenazas	• Establecer el nivel del apetito del riesgo. • Gestión de riesgos de seguridad de la información. • Cumplimiento de Tecnologías de la Información. • Riesgos de Tecnologías de la Información. • Protección de	• Adicional a los que se tiene en operaciones y gobierno: • Gestión de riesgos de seguridad con terceras partes. Gestión de identidades y accesos. • Diseño de arquitecturas de seguridad.	• Notificación • de brechas de privacidad. • Protección de la información. • Descubrimiento electrónico (soporte electrónico de litigios) • Monitoreo y análisis de eventos. • Repuesta a incidentes y análisis forense. • Clasificación de información. • Gestión de vulnerabilidades

Énfasis	Operaciones	Gobierno	Operaciones y Gobierno	Operaciones, Gobierno, asp. legales
		la información. • Clasificación de la información.		y amenazas

Nota: (tomado y traducido de: CIO Executive Board CEB (2013) citado por (Cano M, 2016)

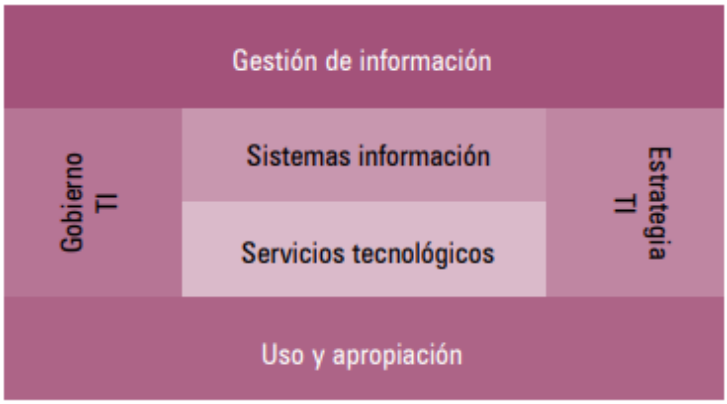
La tabla 3. muestra los patrones relacionados con el ejercicio de la función de seguridad de la información los cuales son: operaciones; gobierno; operaciones y gobierno; operaciones, gobierno y aspectos legales; patrones que actualmente las organizaciones orientan según la práctica de la función de seguridad, acorde al énfasis y dinámica de la empresa; cualquiera que sea el arquetipo elegido por la organización es pertinente comprender no solo el sector de la empresa, sino el ecosistema donde opera, para entender la convergencia tecnológica de los medios sociales, la computación móvil, la computación en la nube y la información. (Cano M, 2016, pp.118).

Gobierno y gestión de TI en Colombia

Para el gobierno y gestión de TI en Colombia el Ministerio de las Tecnologías de la Información y las Telecomunicaciones generó a través de Gobierno en línea en su plan Vive Digital el modelo

IT4 + está basado en la arquitectura de tipo empresarial para la gestión de las tecnología y sistemas de información del Estado colombiano, en seis dominios o dimensiones: estrategia, gobierno, información, sistemas de información, servicios tecnológicos y uso y apropiación. (Marulanda Echeverry, López Trujillo, & Valencia Duque, 2018, p. 83)

Figura 10. Modelo IT4 + para el Estado Colombiano



Fuente: (Marulanda Echeverry et al., 2018)

Según (MINTIC, 2016) el modelo busca que:

> La tecnología contribuya al mejoramiento de la gestión por medio del apoyo de los procesos para alcanzar mayor eficiencia y transparencia en su ejecución, facilitar la administración y el control de los recursos y brindar información objetiva y oportuna para la toma de decisiones en todos los niveles. Permite la alineación de la gestión de TI con los objetivos estratégicos de la entidad,

aumentar la eficiencia de la organización y mejorar la forma como se prestan los servicios misionales.

En esta estrategia del nuevo modelo de Gobierno planteado para las entidades del estado en Colombia, también se habla de la Seguridad de TI como se puede encontrar el sitio que se muestra a continuación:

Figura 11. Seguridad TI y Modelo de seguridad

Fuente: (MINTIC, 2016)

En este sitio se da a conocer los lineamientos sobre el modelo de seguridad y privacidad de la información (MSPI) donde se ofrecen una serie de guías a tener en cuenta en el cumplimiento del modelo y el instrumento de evaluación del MSPI que permite realizar el diagnóstico de madurez de la Entidad.

Modelos de gobierno de Seguridad de la información

En la figura 7, se observan tres modelos relacionados y corresponden a lo planteado por 3 organismos internacionales como son la Organización de Estándares Internacionales ISO, la ITGI Instituto para la Gobierno de Tecnologías de la Información y la NIST National Institute of Standards of Technology, quienes plantean componentes a tener en cuenta para definir un modelo gobierno de seguridad de la información para cualquier organización.

Figura 12.Relación de modelos de Gobierno de Seguridad de la información

Fuente: (Evans, 2011. p.28)

Para explicar más en detalle los modelos de gobierno descritos en el cuadro anterior se describirán a continuación;

Modelo de Gobierno Organización de Estándares Internacionales (ISO): Corresponde al estándar definido en la norma ISO 27014, que corresponde a una buena práctica del Gobierno de Seguridad de la información que hace parte de la Familia de Normas ISO

27000, la cual facilita orientación sobre los principios y conceptos para gobernar la seguridad de la información.

Los ***seis (6) principios*** que propone la ISO 27014 y los cuales se relacionan en el texto de (Mahncke, 2013) [traducido del inglés], son:

Principio 1: Establecer la seguridad de la información en toda la organización

Principio 2: Adoptar un enfoque basado en el riesgo

Principio 3: Establecer la dirección de las decisiones de inversión

Principio 4: Asegurar la conformidad con los requisitos internos y externos

Principio 5: Fomentar un ambiente de seguridad positiva

Principio 6: Revisar el desempeño en relación con los resultados comerciales

La figura 8 muestra el modelo para implementar el gobierno de seguridad de la información de acuerdo a la norma ISO 27014, la cual es muy enfática en que el Gobierno de seguridad es un subconjunto del gobierno corporativo, y muestra cómo interactúan los ***5 procesos*** del modelo que son evaluar, dirigir, monitorear, comunicar y asegurar son tareas a implementar por parte de la Gerencia Ejecutiva.

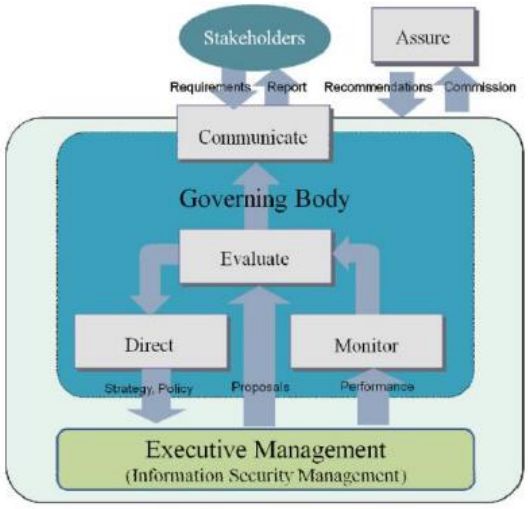


Figura 13. Implementación modelo gobierno de seguridad de la información (ISO/IEC 2014:2013)

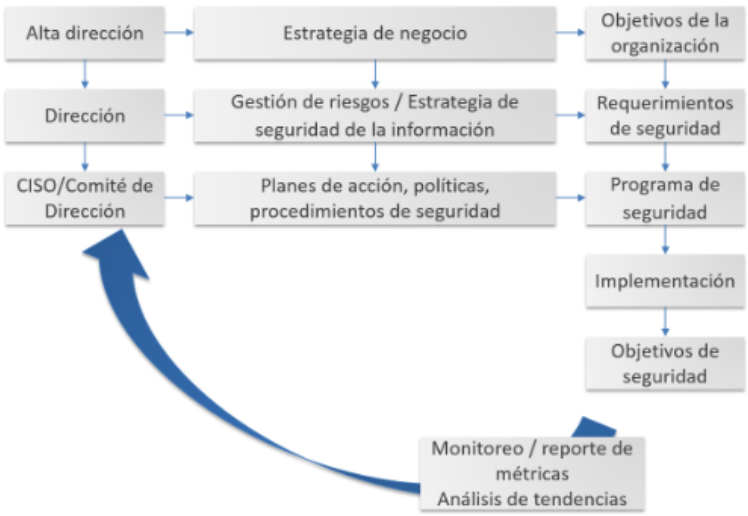
Fuente: (Mahncke, 2013)

Modelo de Gobierno NIST (National Institute of Standards and Technology): En cuanto a los modelos de gobierno de seguridad de la información tenemos el del NIST, según (Sarabia Bautista, 2018) ésta tipo de modelo es más orientado a un marco de gobierno enmarcado en la ciberseguridad debido a las amenazas cibernéticas que se introducen en las organizaciones se propone un gobierno de seguridad de la información que alcance cinco objetivos básicos para lograr un gobierno eficaz dentro del campo del ciberespacio, estos son:

- ✓ Alineación estratégica
- ✓ Administración de riesgos
- ✓ Entrega de valor

- ✓ Administrar recursos
- ✓ Medir el desempeño

Figura 14. Marco de Gobierno de seguridad de la información del NIST



Fuente: IT Governance Institute (2006) citado por (Sarabia Bautista, 2018)

La figura 9 muestra cómo interactúan los diversos elementos que componen el marco de seguridad de la información NIST, quienes son los involucrados y las estrategias que se alinean a las del negocio en busca de unas iniciativas que permiten dar cumplimiento a los objetivos de seguridad de la información.

Modelo de Gobierno Instituto de Gobernabilidad de Tecnologías de la Información (ITGI):

El ITGI es un instituto creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA), y este cuenta con cinco (5) pilares según lo expone (Evans, 2011, p.26)

- **Alineación Estratégica** de la seguridad de la información con la estrategia del negocio para soportar los objetivos organizacionales
- **Gestión de Riesgos** mediante la ejecución de medidas apropiadas para gestionar y mitigar los riesgos y reducir el impacto potencial en los recursos de información a niveles aceptables
- **Gestión de Recursos** mediante la utilización eficiente y efectiva del conocimiento de seguridad de la información y la infraestructura de la organización
- **Medición de la Ejecución** mediante la medición, monitoreo y reporte de métricas de gobierno de seguridad de la información que garantice alcanzar los objetivos de la organización
- **Entrega de Valor** mediante la optimización de las inversiones en seguridad de la información que soporten los objetivos del negocio

Al revisar estos modelos de gobierno de seguridad de la información se puede ver puntos en común, como son, todos se alinean a la estrategia, hacen énfasis en la gestión de riesgos, entrega de valor, medición del desempeño de las estrategias de gobierno y una parte importante la administración de recursos.

Lo anterior, impulsado y apalancado por la alta gerencia quien es la encargada de gestionar las estrategias para abordar el gobierno de seguridad de la información desde el gobierno corporativo, con la finalidad de asegurar la información de la organización con unas

direcciones claras e interacciones eficientes entre los responsables de la seguridad de la información desde cada uno de sus roles para que se dé lineamientos claros que permitan que las estrategias de seguridad de la información se den acertadamente en la organización .

Metodologías para Gestión de Riesgo de Seguridad de la información

El riesgo es inminente en todos los procesos de transmisión y manejo de información en cualquier organización; es así como también hace parte importante del Gobierno de seguridad de la información, porque toda la estrategia que se requiere diseñar para administrar los riesgos es primordial para que puedan ser administrados, gestionados y tratados de manera controlada y eficiente para minimizarlos y que la información se blinde ante la materialización de un riesgo.

Según (Gómez, Hernán Pérez, Donoso, & Herrera, 2010) Las organizaciones son cada vez más conscientes de los riesgos informáticos y de coexistir con ellos pero de manera controlada. Es por esto que se ha empezado a incluir dentro de las funciones de la organización un análisis de riesgo y un plan de mitigación, teniendo claro que siempre queda un riesgo remanente y latente para los procesos de misión crítica. El análisis y entendimiento de los riesgos involucran directamente al nivel gerencial entre ellos los gerentes y el Chief Information Office (CIO) quienes como directivos deben tener claridad y coherencia con la gestión de los mismos.

Actualmente existen diversas metodologías de riesgos de seguridad de la información, sin embargo, se pueden nombrar Octave, octave allegro, Mehari, Magerit, Cramm, Ebios, NIST SP

800- 30 que se muestran en la tabla 4, donde para cada metodología según el número asignado se puede observar que fases abordan para la gestión del riesgo.

Fases de las metodologías para el análisis de riesgos

FASES	METODOLOGÍAS							
	1	1A	1B	2	3	4	5	6
Caracterización del sistema	X	X	X	X	X	X	X	X
Identificación de amenazas	X	X	X		X	X	X	X
Identificación de vulnerabilidades	X		X			X		X
Análisis de controles	X	X	X	X	X		X	X
Determinación de la probabilidad								X
Análisis de impacto								X
Determinación del riesgo	X	X	X	X	X	X		X
Recomendaciones de control	X	X	X	X		X	X	X
Documentación de resultados	X			X				X
Establecimiento de parámetros			X		X			
Necesidades de Seguridad	X					X	X	

(1) OCTAVE, (1A) OCTAVE S, (1B) OCTAVE ALLEGRO, (2) MEHARI, (3) MAGERIT, (4) CRAMM, (5) EBIOS, (6) NIST SP 800 – 30

Tabla 3. Fases de las metodologías para análisis de riesgos

Fuente: (Abril; Pulido; Bohada, 2013. p.41)

También encontramos la ISO 27005, ésta es la norma de la familia de ISO27000 que es una guía para gestionar riesgos que pueden comprometer la seguridad de la información de la organización.

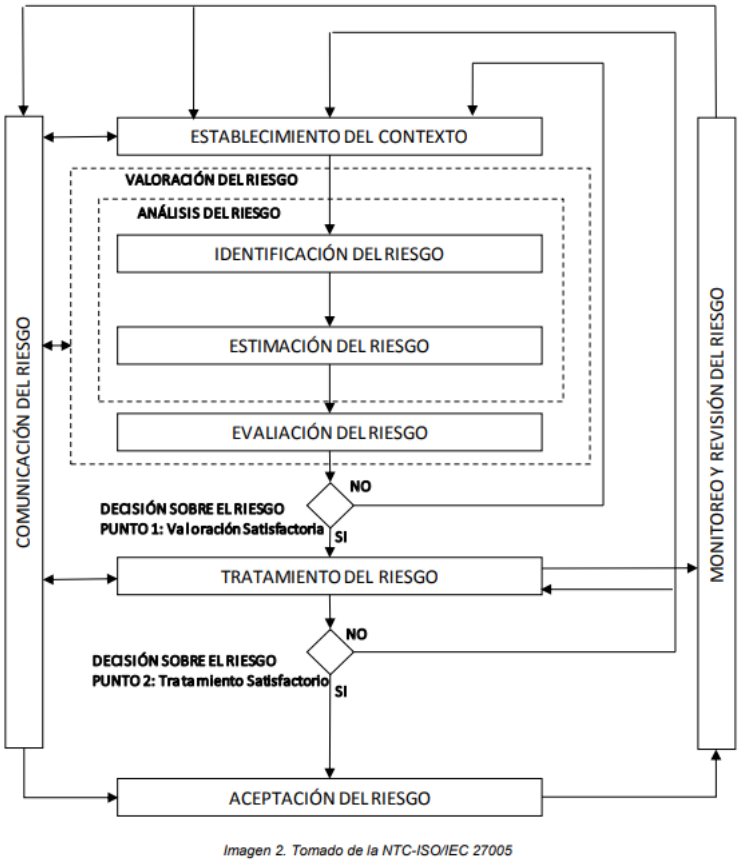


Figura 15. Proceso para la administración de riesgo en seguridad de la Información NTC-ISO-IEC 27005

Fuente: (Departamento Administrativo de la Función Pública, 2018)

Sin embargo, para las Entidades del Estado es el Departamento de la Función Pública quien define la metodología de riesgos a aplicar, ésta se ha basado en la norma ISO 31000 que contiene las fases que se observan en la figura 11, tomado del Procedimiento de Administración de Riesgos de la CGR.

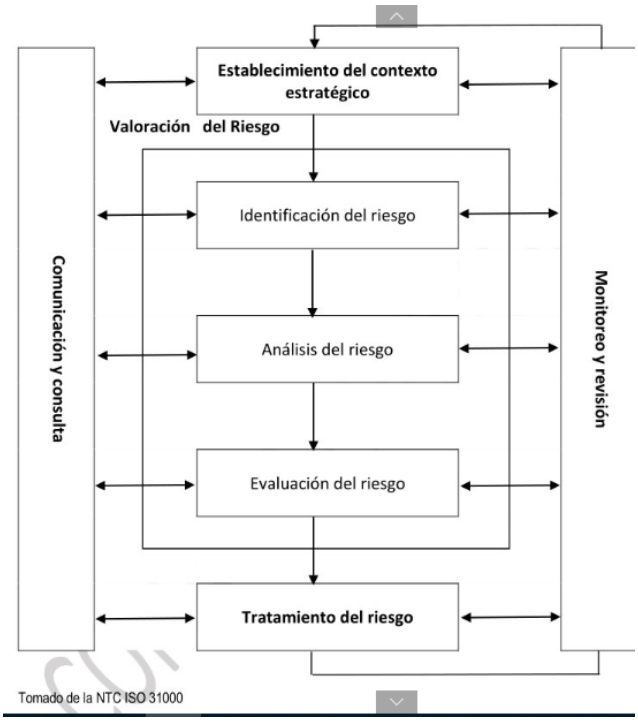


Figura 16. Marco metodológico para la gestión de riesgos en la CGR basado en la ISO 31000

Fuente:(García; Gómez, 2015)

Actualmente la CGR se rige con este procedimiento, sin embargo, en su metodología no se contemplaban los riesgos de seguridad de la información que para el caso de las entidades de gobierno y de acuerdo al CONPES 3854 deben visualizarse los riesgo de seguridad digital, el Ministerio de la Tecnologías de información y las comunicaciones en Octubre de 2018 publica la nueva Guía para la administración del riesgo y el diseño de controles en entidades públicas: Riesgos de Gestión, Corrupción y Seguridad Digital. Cabe anotar que la CGR aún no ha aplicado esta nueva metodología, aun no se está realizando la gestión de riesgos para los activos de información de la entidad, es una actividad pendiente por realizar.

Esta guía surge para unificar "la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de la herramienta gerencial para las entidades públicas y así evitar duplicidades o reprocesos" (Departamento Administrativo de la Función Pública, 2018a. p.6) consta de las siguientes fases:

Esquema 2. Metodología para la administración del riesgo

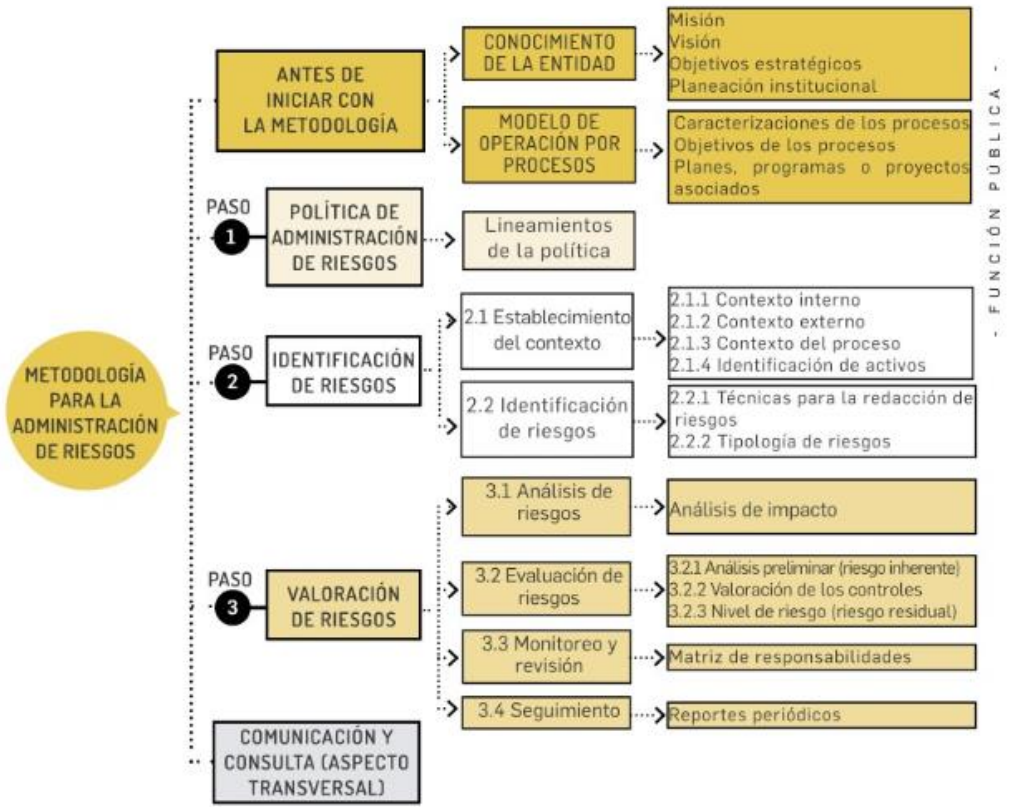


Figura 17. Metodología para la administración del Riesgo según la Guía de función pública para las Entidades del Estado

Fuente: (Departamento Administrativo de la Función Pública, 2018b.p.13)

La metodología incluye los riesgos de seguridad digital, se deben identificar los activos de información estos se definen según la guía (Departamento Administrativo de la Función Pública, 2018c.p.21) "activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes…". La figura 13 muestra los pasos a seguir para la identificación de activos de información y relaciona el anexo 4, el cual explica los lineamientos para la gestión del riesgo de seguridad digital en entidades públicas.

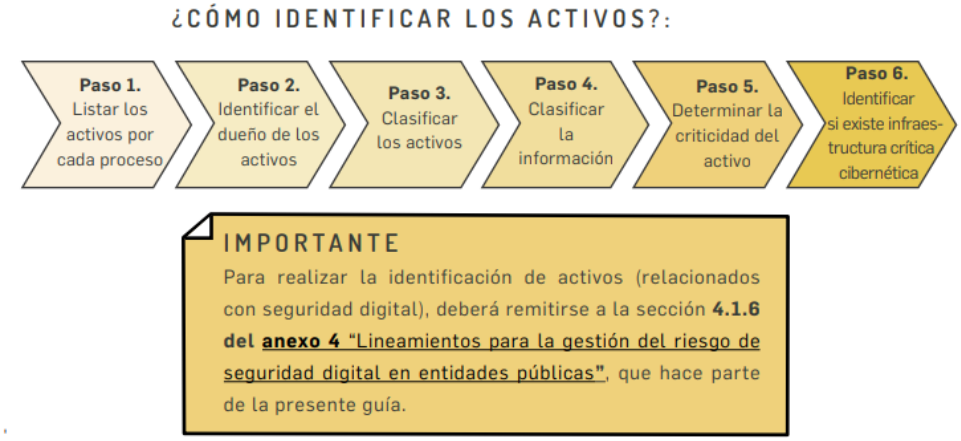
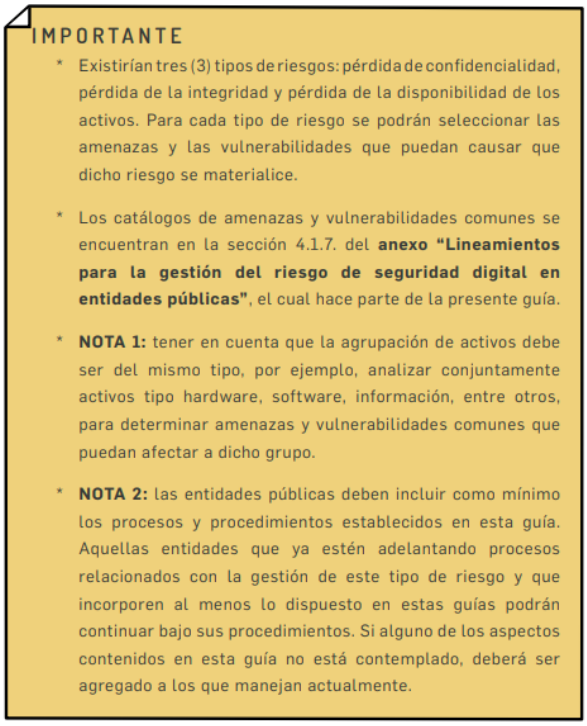


Figura 18. Como identificar los activos de información

Fuente: (Departamento Administrativo de la F. unción Pública, 2018d. p.22)



IMPORTANTE

* Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

* Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas"**, el cual hace parte de la presente guía.

* **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.

* **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

Figura 19.Clases de riesgos de seguridad digital y lineamientos

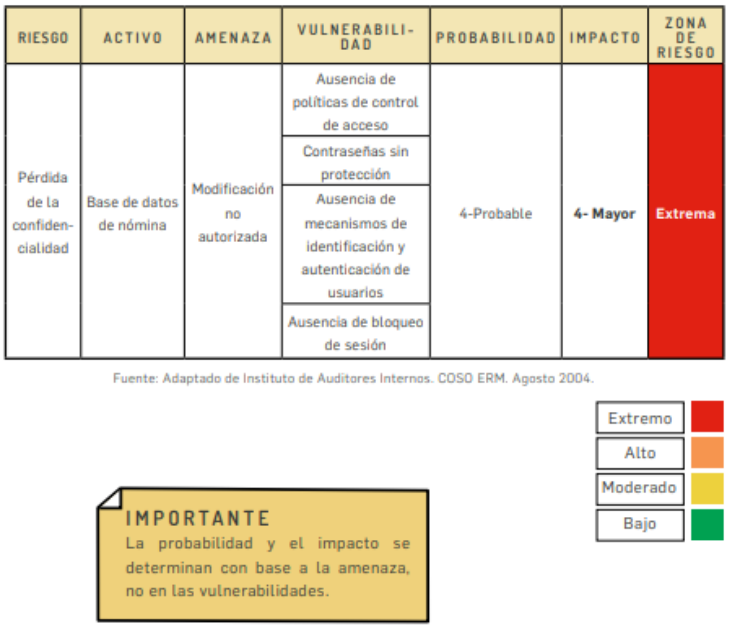
Fuente: (Departamento Administrativo de la Función Pública, 2018e. p.35)

En la figura 14 se define para los riesgos de seguridad digital tres (3) tipos: pérdida de confidencialidad (que la consulten y accedan a ella solo las personas autorizadas), pérdida de la integridad (qué este completa como originalmente se crea) y pérdida de la disponibilidad (poder acceder a la información en cualquier momento) que son los pilares de la información, asimismo se dan los lineamientos para la gestión del riesgo de seguridad digital en Entidades del Estado.

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
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.

Figura 20. Criterios para calificar el impacto- riesgos de seguridad digital

Fuente: (Departamento Administrativo de la Función Pública, 2018f. p.42)



RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la confiden-cialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Figura 21. Ejemplo de riesgo de seguridad digital y evaluación

Fuente:(Departamento Administrativo de la Función Pública, 2018g. p.44)

Modelo nacional de riesgos de seguridad digital MGRSD

El modelo nacional de riesgos de seguridad digital que tiene como objetivo “alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales y proteger a las personas frente a las amenazas de seguridad digital” minis b 2018

Este modelo plantea unas cuatro guías de orientación para la aplicación del modelo para las entidades del 1. Sector público y de Gobierno, 2. Sector mixto y privado, 3. Sector fuerza pública y 4. Dirigida a la ciudadanía.

Así también, este contempla algunos elementos necesarios para la aplicación del modelo como lo dice el documento de (Ministerio de las Tecnologías y las Comunicaciones, 2018, pp.35-36), es importante que la entidad cualquiera que sea su naturaleza,

> Establezca previamente un gobierno de seguridad de la información con base en las metodologías dispuestas para tal fin. Estas son: el modelo de seguridad y privacidad de la información (MSPI) del (MINTIC) (o del que haga sus veces) o un sistema de gestión de seguridad de la información (SGSI) de acuerdo con estándares como: NTC-ISO/IEC27001:2013 o NTC-ISO 27005:2011, entre otras.

Es importante acotar que las entidades del estado deben apropiar lo definido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas: Riesgos de Gestión, Corrupción y Seguridad Digital, así como alinearse con el modelo nacional de riesgos de seguridad digital y la Contraloría General de la República está en el proceso de actualizar su metodología de riesgos para incluir los de seguridad digital, propuesta que se está construyendo en conjunto entre USATI y la Oficina de Planeación, éstos últimos encargados de evaluar como tener en cuenta lo planteado en el modelo nacional de riesgos.

Metodologías de Madurez (Capability Maturity Model Integration) CMMI

CMMI es el Modelo de Madurez de Capacidades Integrado, enfoque de mejora de procesos que provee a las organizaciones de los elementos esenciales para un proceso efectivo, sirve para aplicar mejores prácticas que abordan el desarrollo y mantenimiento de productos y servicios que cubren el ciclo de vida del producto desde la concepción hasta la entrega y el mantenimiento.(Allsoft, 2008)

El CMMI tiene dos representaciones

- Por etapas
- Continuo

A continuación se muestran los niveles de madurez por etapas según (CCTI Consultoría de Tecnología, 2018) así:

Nivel 1 (Inicial): El proceso es impredecible, es reactivo y pobremente controlado.

Nivel 2 (Administrado): En este nivel, el proceso es reactivo y se caracteriza por su aplicación a proyectos.

Nivel 3 (Definido): En este nivel, el proceso se vuelve proactivo y se ve a nivel de organización.

Nivel 4 (Administrado Cuantitativamente): Este proceso es medido y controlado.

Nivel 5 (Optimizado): El Proceso se enfoca a una mejora continua

Niveles de madurez continúo: La siguiente gráfica muestra los niveles y la descripción de cada uno de ellos para el modelo CMMI.

Figura 22. Niveles de madurez continúo CMMI

Fuente: (Figura Niveles de madurez de CMMI, 2017)

Las áreas de proceso donde se puede aplicar son:

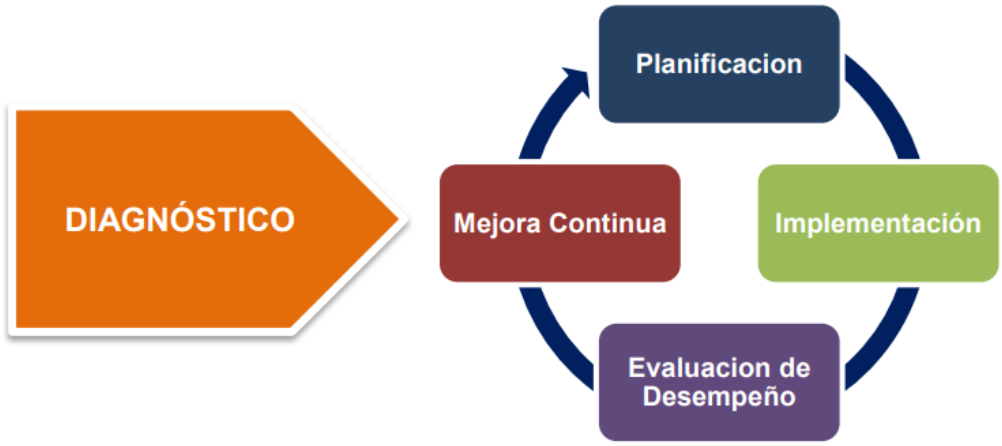
- Gestión de requisitos (REQM)
- Planificación de proyectos (PP)
- Monitoreo y Control de Proyectos (PMC)
- Gestión de Contratos con Proveedores (SAM)
- Medición y Análisis (M&A)
- Proceso y Garantía de Calidad del Producto.
- (PPQA)
- Gestión de la configuración (CM)

- Desarrollo de Requisitos (RD)
- Solución Técnica (TS)
- Integración de productos (PI)
- Verificación (VER)
- Validación (VAL)
- Enfoque en el proceso de la organización (OPF)
- Definición del Proceso de Organización (OPD)
- Capacitación Organizacional (OT)
- Gestión integrada de proyectos para IPPD.

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

Por otra parte y no menos importante para las entidades de gobierno como la Contraloría General de la República es mandatorio y relevante tener en cuenta el modelo de madurez de seguridad y privacidad de la Información (MSPI), de acuerdo a las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones el modelo de madurez a utilizar en las entidades del Estado colombiano es el Modelo de Seguridad y Privacidad de la Información (MSPI), el "cual contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información" (Mintic, 2016, p.20)

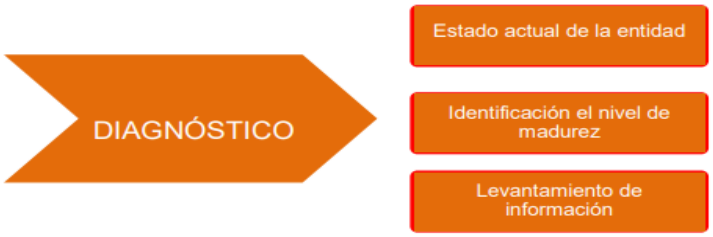
Figura 23. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información



Fuente: (Mintic, 2016, p.20)

Fase de Diagnóstico: se identifica el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Figura 24. Etapas previas a la implementación

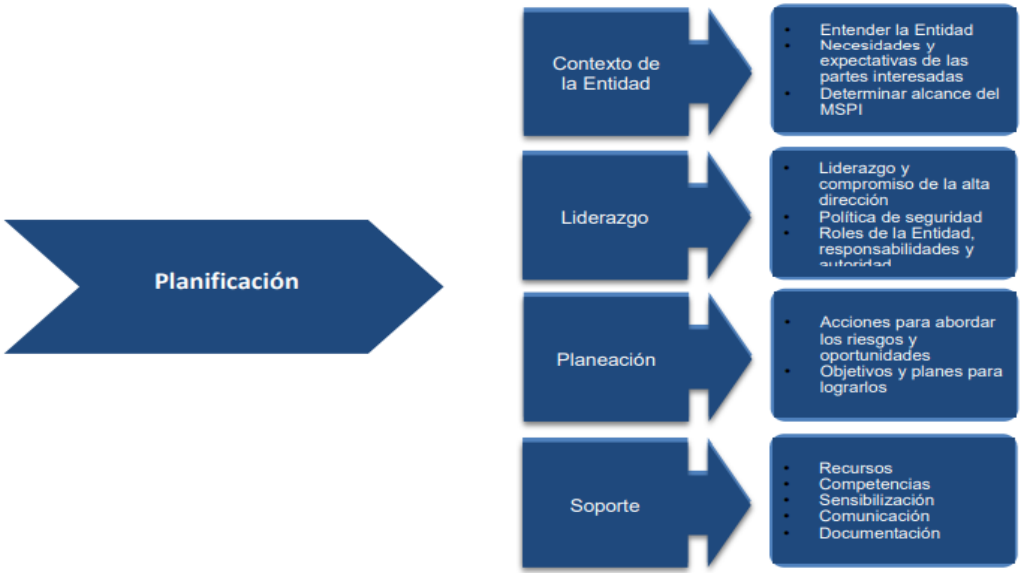


Fuente: (Mintic, 2016, p.21)

Fase de Planificación: se elabora el plan de seguridad y privacidad de la información alineada con el objetivo misional de la entidad, con el propósito de definir las acciones a

implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo. Este es un enfoque por procesos y se extenderá a toda la entidad.

Figura 25. Fase de Planificación



Fuente: (Mintic, 2016, p.24)

Fase de Implementación: se llevará a cabo la implementación de la planificación realizada en la fase anterior del MSPI.

Figura 26. Fase de Implementación

Fuente:(Mintic, 2016, p.29)

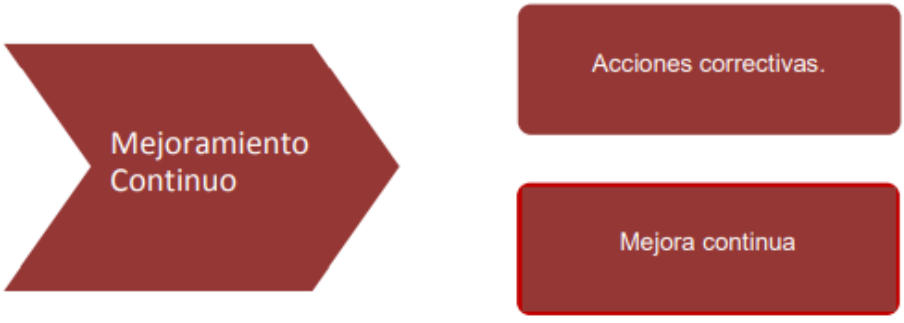
Fase de Evaluación y desempeño: se realiza el seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Figura 27.Fase de Evaluación del Desempeño

Fuente:(Mintic, 2016, p.32)

Fase de Mejora Continúa: se consolidan los resultados obtenidos en la evaluación de desempeño y se diseña el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

Figura 28.Fase de Mejora Continúa



Fuente: (Mintic, 2016, p.34)

Indicadores de gestión para la seguridad de la Información

En la guía de indicadores propuesta por (Mintic;Vive digital para la gente, 2016, p.7)se indica que se crean indicadores para la medición de "efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua"

De acuerdo a lo planteado en la guía de indicadores de (Mintic;Vive digital para la gente, 2016), los objetivos de estos procesos de medición en seguridad de la información son:

- Evaluar la efectividad de la implementación de los controles de seguridad.
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de análisis y tratamiento de riesgos.

Los indicadores están basados en la norma ISO 27004 según (ISOTools- Plataforma tecnológica para la gestión de la Excelencia, 2014) estándar que estructura el sistema de

medición, parámetros a medir, cuándo y cómo medirlos. Con el objetivo de medir o evaluar la eficiencia de la seguridad de la información, las etapas planteadas por ISO-27004 son:

1) Elección de los objetivos y procesos de medición
2) Descripción de las líneas principales
3) Selección de datos
4) Desarrollo de un sistema de medición
5) Interpretación de los valores medidos
6) Notificación de los valores de medición

En la actualidad en la Contraloría General de la República aún no hay indicadores de los procesos de seguridad de la información, se está avanzando en la madurez del Sistema de Gestión de Seguridad de la Información (SGSI) para logar establecer indicadores que permitan dar un nivel de madurez de la entidad en este tema.

Algunos indicadores propuestos de acuerdo a las fichas planteadas por a Guía de indicadores están:

Indicador de Organización de Seguridad de la información: Relacionada con el compromiso de la dirección y la asignación de personas y roles asignados a la SI al interior de la Entidad.

Indicador cubrimiento del SGSI en activos de información: Proceso de incluir un activo de información en todo su ciclo hasta la evaluación y gestión de riesgo, aplicación de controles.

Indicador tratamientos de eventos relacionados en marco de seguridad y privacidad de la información: Eficiencia en el tratamiento de eventos reportados por los usuarios en el marco de la seguridad.

Indicador Plan de sensibilización: permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales

Un ejemplo de ficha para la indicador es el siguiente:

INDICADOR – PLAN DE SENSIBILIZACIÓN					
IDENTIFICADOR	SGIN04				
DEFINICIÓN					
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.					
OBJETIVO					
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
VSI07: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.		(VSI07/VSI08)*100		Oficial de Seguridad de la Información, auditorías internas, atención al usuario, listas de asistencia	
VSI08: Total de personal a capacitar.				Total de funcionarios de la entidad.	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

Tabla 4. Ficha ejemplo de indicador plan de sensibilización

Fuente:(Mintic;Vive digital para la gente, 2016, p.10)

Capítulo 3

Marco Contextual

La Contraloría General de la República (CGR), es un organismo de control en la estructura del Estado Colombiano, se encuentra ubicada en la ciudad de Bogotá y cuenta con 32 Gerencias departamentales, cuenta con una planta de personal de 4057 cargos de los cuales 3934 son cargos de carrera administrativa y 123 de libre nombramiento y remoción.

Figura 29. Estructura del Estado Colombiano Componentes de la Arquitectura de Tecnologías de la Información

Fuente: (Departamento de la Función Pública, 2018a)

La CGR pertenece a los organismos de control del Estado Colombiano, al lado del Ministerio Público, las Contralorías Territoriales y la Auditoría General de la República como se observa en la siguiente figura donde se detallan los organismos de control.

Figura 30. Organismos de Control

Fuente: (Departamento de la Función Pública, 2018b)

Como lo menciona (Contraloría General de la República, 2016) y de acuerdo a lo establecido en la Constitución Política de 1991, en su artículo 267, "el control fiscal es una función pública que ejercerá la Contraloría General de la República, la cual vigila la gestión fiscal de la administración y de los particulares o entidades que manejan fondos o bienes de la Nación" (Párr 4)

La contraloría General de la República en cumplimiento del artículo 119 de la Constitución Nacional, "ejerce, en representación de la comunidad, la vigilancia de la gestión fiscal y de los particulares o entidades que manejan fondos o bienes de la Nación."

Misión

Para este nuevo cuatrienio cambio y el nuevo contralor le da mucho peso a que el control fiscal sea efectuado con base en el conocimiento a partir de la tecnología, esto hace que la CGR tenga un gran desafío apara afrontar los riesgos digitales y proteger su información según (Contraloría General de la República, 2019. Párr. 1) la misión es:

> Ejercer el control y vigilancia fiscal a los recursos públicos de forma oportuna, independiente y efectiva, garantizando la participación activa de la ciudadanía y la articulación regional, con base en el conocimiento y la tecnología, que contribuya al desarrollo sostenible y al cumplimiento de los fines esenciales del Estado.

Visión

Su visión para el 2022 según (Contraloría General de la República, 2019. Párr.2) es:

> La Contraloría General de la República, será reconocida a nivel nacional e internacional como un órgano de control y vigilancia fiscal líder, moderno y efectivo, con un enfoque preventivo y un control fiscal participativo y oportuno, que contribuya al buen manejo de los recursos públicos, y que genere una mejora en la gestión del Estado y calidad de vida de los colombianos.

Objetivos Estratégicos

A continuación y de acuerdo a lo planteado en (Contraloría General de la República, 2018a) los objetivos estratégicos de la Entidad desde 2018 a 2022, son los siguientes:

1. Fortalecer la gobernanza interna a través de las interacciones y acuerdos entre el control fiscal macro y micro en el nivel central y regional , para hacer más efectivo el control fiscal, la vigilancia y control del recurso público.
2. Vigilar la gestión fiscal con un control efectivo, a tiempo y articulado entre los macro procesos misionales.
3. Desarrollar el control fiscal participativo para la buena gestión pública y el fortalecimiento del control y la vigilancia fiscal a tiempo.
4. Fortalecer el apoyo técnico al congreso para el ejercicio de sus funciones legisltativas y de control político.
5. Habilitar las capacidades y servicios tecnológicos para impulsar la transformación digital de la Entidad por medio de la práctica de arquitectura empresarial.
6. Fortalecer el talento humano y la operación de la estructura organizacional , procesos y procedimientos de la Contraloría General de la República para cumplir de manera efectiva la misión de la Entidad.

Funciones

Asimismo realiza las siguientes funciones:

-Evalúa los resultados obtenidos por las diferentes organizaciones y entidades del Estado, al determinar si adquieren, manejan y/o usan los recursos públicos dentro del marco legal, sujetos a los principios de economía, eficiencia, eficacia, equidad y sostenibilidad ambiental.

-Examina la razonabilidad de los estados financieros de los sujetos de control fiscal y determina en qué medida logran sus objetivos y cumplen sus planes, programas y proyectos.

-Tiene a su cargo establecer la responsabilidad fiscal de los servidores públicos y de los particulares que causen, por acción o por omisión y en forma dolosa o culposa, un daño al patrimonio del Estado.

-Impone las sanciones pecuniarias que correspondan y las demás acciones derivadas del ejercicio de la vigilancia fiscal.

-Procura, igualmente, el resarcimiento del patrimonio público.En ejercicio de la denominada jurisdicción coactiva, intenta recuperar los recursos y bienes públicos que han sido objeto de deterioro como resultado de su mala administración o que han sido apropiados en forma indebida por los funcionarios o por los particulares.

-Adicionalmente, la Contraloría General de la República genera una cultura de control del patrimonio del Estado y de la gestión pública.

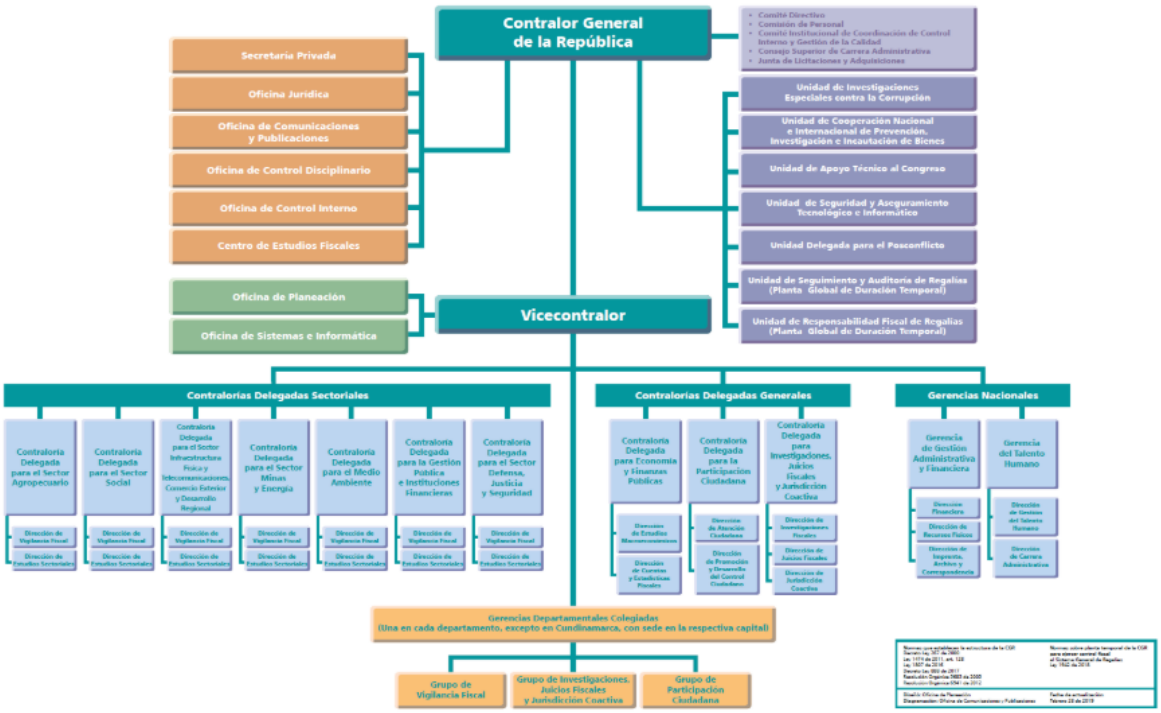
- El organismo fiscalizador promueve la transparencia en el uso de los recursos públicos, mediante un proceso estratégico y focalizado en aquellas entidades y/o áreas de alto riesgo previamente identificadas.

- La CGR vincula activamente a la ciudadanía en el control de la gestión pública y apoya técnicamente al Congreso de la República para el ejercicio del control político y el desarrollo de la función legislativa.(Contraloría General de la República, 2019. Párr. 11-20)

Organigrama

La Contraloría General de la República cuenta con la siguiente estructura orgánica:

Figura 31. Estructura orgánica Contraloría General de la República



Fuente: (Contraloría General de la República, 2019a)

Procesos actuales de Seguridad de la información en la CGR

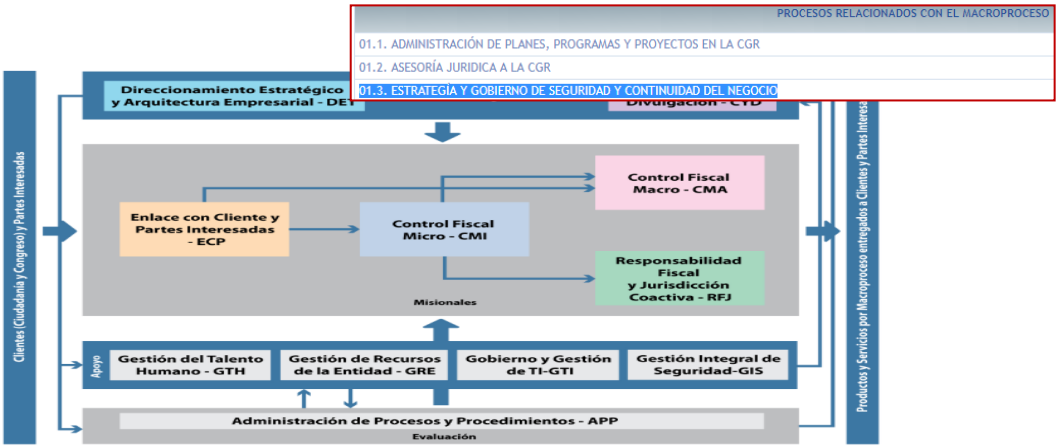
Es importante resaltar que al interior de la Entidad y de acuerdo a (Secretaria de Transparencia Presidencia de la República, 2011) el Estatuto Anticorrupción - Ley 1474 de 2011 establece la creación varias dependencias dentro de la estructura de la Contraloría General de la República, entre ellas la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI), la cual entre sus funciones se encarga de formular políticas de seguridad para la entidad.

Así también, la Contraloría General de la República contrató una consultoría para obtener un modelo operativo para el Gobierno de Tecnologías de la Información y la Oficina de Sistemas e Informática lidera la iniciativa; también, otra contratación para realizar la arquitectura empresarial de la Entidad en cabeza de la Oficina de Planeación, la cual deja insumos y proyectos que permitan organizar los procesos de negocio de la CGR siendo el componente de seguridad de información un eje transversal de la arquitectura.

La Unidad de Seguridad y Aseguramiento Tecnológico e Informático ha logrado la creación de dos procesos relevantes para su función, como se muestra en la Figura 1, el primero es el proceso estratégico de negocio denominado *Estrategia y gobierno de seguridad y continuidad del negocio,* está orientado a "Fortalecer la capacidad de la CGR para cumplir sus funciones constitucionales y legales ante situaciones que amenacen la continuidad del negocio, su reputación y la seguridad de sus servidores, bienes e información" . (Contraloría General de la

República, 2018b), a través de éste se formulan y orientan lineamientos de seguridad para toda la CGR.

Figura 32.Proceso de Seguridad Integral en la CGR, Direccionamiento Estratégico



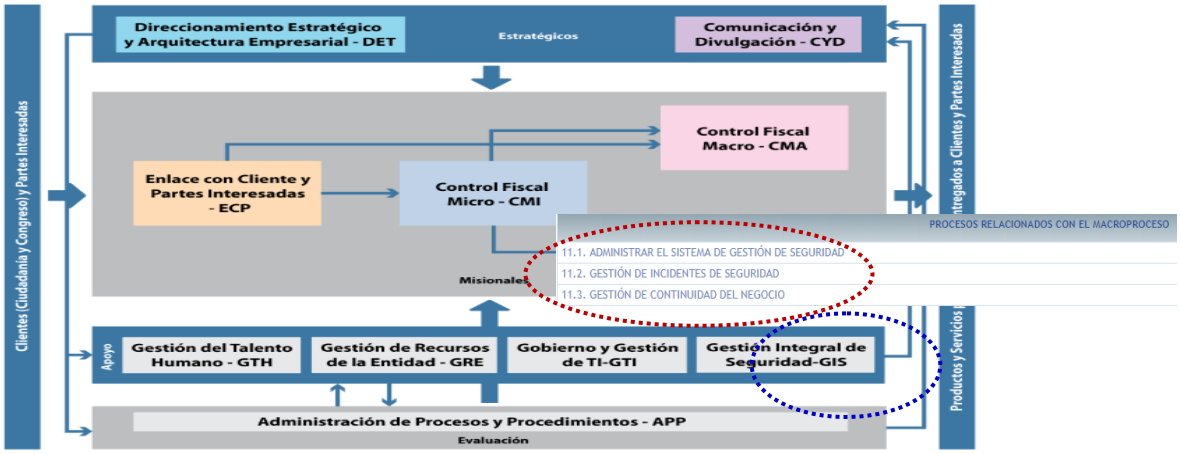
Fuente: (Contraloría General de la República, 2018b)

El segundo como se muestra en la Figura 27, es el proceso de Gestión Integral de Seguridad orientado a "Gestionar la seguridad de bienes, personas e información de la CGR conforme a lo establecido en la Ley 1474 de 2011.", (Contraloría General de la República, 2018), dicho proceso está incluido en la línea de apoyo de la entidad, en este se administran y realiza

En las actividades relacionadas con la seguridad integral en la CGR, desde los lineamientos y políticas planteadas en el contexto estratégico a través de tres procesos, 1) *Administrar el Sistema de Gestión de Seguridad*, en este se realizan actividades para fortalecer e implementar el SGS de la entidad en cuanto a la documentación del sistema, la apropiación del sistema y la generación de cultura de seguridad para los servidores públicos de la entidad, también se debe pensar un proceso sistemático para la realización de auditorías al SGS cuando se

encuentre más fortalecido y los planes de mejora, en este momento aún se está iniciando la implementación.

Figura 33. Proceso de Gestión Integral de la Seguridad (GIS) en la CGR



Fuente: (Contraloría General de la República, 2018b)

El 2) *Gestión de Incidentes de Seguridad,* está enfocado en realizar la administración de los incidentes de seguridad de información que puedan surgir en la CGR y como realizar el tratamiento de éstos desde su detección hasta la solución, bajo la implementación de un nuevo equipo de trabajo denominado CSIRT Centro de Respuesta a Incidentes de Seguridad al interior de la entidad, con el fin de realizar una adecuada gestión de incidentes e interactuar logrando una cooperación con otros entes de gobierno relacionados para aprender, compartir y minimizar cualquier actividad o situación que pueda poner en riesgo la seguridad de información de la CGR. El 3) *Gestión de Continuidad del negocio,* se crea para iniciar a generar los procesos y actividades relacionados con los planes de continuidad del negocio, sin embargo, en este momento no se ha generado se cuenta con información incipiente, aun no se ha desarrollado actividades de éste tema.

Capítulo 4

Diseño Metodológico

En este capítulo, se describe el diseño metodológico de la investigación a realizar, el cual aborda los instrumentos de recolección de datos a utilizar y descripción de estrategias para analizar la información encontrada en el trabajo de campo realizado en la Contraloría General de la República, cuya finalidad es proponer un modelo de gobierno de seguridad de la información, enmarcado en las buenas prácticas para gobernar la Seguridad de la Información en las organizaciones.

4.1. Tipo de Investigación a utilizar

El nivel investigativo será cualitativo de acuerdo a flick (2009) citado por (Ugalde Binda & Balbastre-Benavent, 2013), este tipo de diseño es idóneo para:

> Estudiar los cambios que tienen lugar en los procesos de carácter social y organizativo. Dada la implicación del investigador cualitativo en el contexto de su estudio, el mismo se posición encuentra en una más favorable para ver las vinculaciones entre los eventos y las actividades, así como para explorar las interpretaciones que las personas hacen de los factores que producen dichas interconexiones.

Esta investigación es pertinente para el trabajo desarrollado por cuanto el investigador está implícito en el entorno y contexto de estudio, es decir, este trabaja en la Organización y en la dependencia orientada a la protección de la seguridad de la información, por lo que se cuenta con la visión de seguridad de la entidad, de sus procesos y de varios insumos necesarios para estructurar un adecuado modelo de gobierno de seguridad de la información.

4.2. Desarrollo de la investigación

A continuación se proponen las fases previstas para el desarrollo de la investigación, acorde a la revisión de documentos y recolección de datos que permitan diagnosticar y analizar el estado de gobierno de seguridad de la información en la entidad y proponer un modelo que dé una solución a la CGR, como guía a seguir para establecer un Gobierno de seguridad de la información pertinente a las funciones de la Organización.

4.3. Fases para desarrollar la Investigación

Tabla 5. Descripción de fases para desarrollar la Investigación

	Fase	**Descripción**	**Actividades**
1	**Métodos de Recolección de**	a. Reunir documentos con información necesaria para	Documentos a revisar si existen: ✓ Misión, Visión, Funciones de la

	Fase	Descripción	Actividades
	Datos	revisar el estado actual del Gobierno de Seguridad de la información en la Entidad	CGR ✓ Organigrama ✓ Procesos seguridad de la información ✓ Libro de Políticas de seguridad de la información ✓ Gobierno de Tecnologías de la Información ✓ Resultados ejercicio Arquitectura empresaria –Proyectos de Seguridad de información.
		b. Definición de método a utilizar para recolectar datos.	✓ Definición del Instrumento a aplicar en la recolección de datos
		c. Aplicación del instrumento de medición de dimensiones de seguridad de la información en la CGR.	✓ Realizar Piloto del Instrumento ✓ Aplicación del Instrumento Dimensiones de seguridad de la información ✓ Relación de Dependencias y Gerencias de la CGR donde se aplica el instrumento

	Fase	Descripción	Actividades
2	**Resultados y análisis de la información recolectada**	a. Aplicación del Instrumento Dimensiones del Gobierno seguridad de la información	✓ Resultados y análisis de la vista Global del Gobierno seguridad de la información en la CGR b. Resultados Instrumento de medición del Gobierno seguridad de la información por variables (Cargos)
3	**Diagnóstico del nivel de madurez estado de Gobierno de Seguridad**	a. Verificar los resultados del nivel de madurez de las dimensiones o componentes de seguridad de la información, después de aplicado el instrumento.	✓ Resultado del nivel de madurez para la CGR.
4	**Formular propuesta**	Formular y presentar una propuesta de un modelo de gobierno de seguridad de la información ara la CGR	Diseñar el modelo de de gobierno de seguridad de la información para la CGR Diseñar rutas de los componentes del modelo propuesto

Fuente: Elaboración propia

Fase 1. Recolectar Información

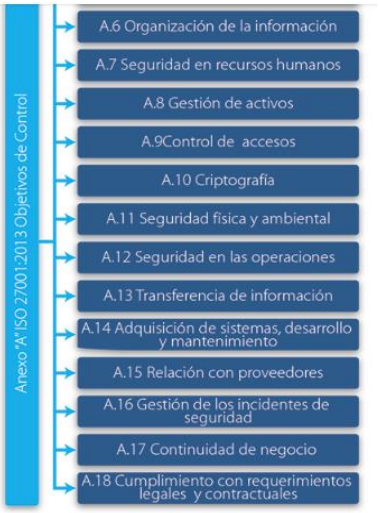
Revisión documental e Información de la Entidad

Reunir documentos con información necesaria para revisar el estado actual del Gobierno de Seguridad de la información en la Entidad

Tabla 6. Revisión documental e Información de la Entidad

	Documento	Utilización en la Investigación
1	Misión, visión y funciones	Se utilizan para tener un conocimiento de que hace la Entidad, la misión es un gran punto de partida porque se da importancia al conocimiento y a la tecnología para cumplir sus funciones y la visión marca la ruta de la CGR para realizar un control fiscal moderno y efectivo, lo que fundamenta el valor de la seguridad de la información.
2	Organigrama	Se usa para identificar las dependencias y las gerencias departamentales a las que se aplica la encuesta y para verificar la jerarquía de las Unidad de Seguridad y las áreas estratégicas necesarias para plantear el Modelo de Gobierno de Seguridad de la

		información.
	Procesos seguridad de la información	La revisión del proceso estratégico de Estrategia y Gobierno de seguridad y continuidad del negocio, y proceso de apoyo Gestión Integral de la Seguridad, en el Sistema de Control Interno y Gestión de la Calidad SCIGC relacionados con los procesos que administra y gestiona la Unidad de Seguridad y aseguramiento tecnológico informático – USATI, se usa para tener una visión global y establecer en el modelo los procesos de seguridad de la información en la CGR que aún falta madurar.
	Libro de Políticas de seguridad de la información Resolución creación SGSI  Fuente: Libro Políticas CGR.(Maya, Alonso, Halaby,	Este sirve en esta investigación para conocer los documentos de políticas, base documental adelantada en la CGR la cual consta en este momento de 31 políticas de seguridad y 18 normas de seguridad, basada en los dominios de la ISO27000, como se observa a continuación:

	& Altamiranda, 2018)	Figura 34. Dominios de control Anexo "A" de ISO 27001:2013  Fuente: (Scitum S.A. de C.V., 2017) Estas políticas dan lineamientos y principios importantes a tener presentes en la dimensión de principios o lineamientos Gobierno de seguridad de la información.
	Gobierno Tecnologías de la Información	Sirve para establecer el alcance de la Oficina de  Sistemas e Informática como actor de la operación de seguridad de la información, en su grupo de seguridad Informática, y permite delinear roles y

		responsabilidades a tener en cuenta en la propuesta Gobierno de seguridad de la información.
	Ejercicio de Arquitectura Empresarial	Se usa para tener claridad de las líneas de seguridad que se han venido generando como capacidades propuestas como resultado del ejercicio de arquitectura empresarial, el cual recomienda un Programa que da línea para fortalecer la seguridad digital en la Entidad que es el siguiente: **PRG008 Fortalecimiento del modelo de seguridad CGR** o Procedimientos, controles y tecnologías de seguridad implementados para la prevención, detección y contención de incidentes de seguridad. **PRG008 Fortalecimiento del modelo de seguridad CGR** o Modelo de Gobierno, Riesgo y Cumplimiento establecido permitiendo fortalecer las capacidades de gestión de activos, riesgos y cumplimiento. o Exposición segura de portales, protección frente a ataques, intercambio de información seguro manteniendo la confidencialidad e integridad de los datos. o Adecuada gestión de los usuarios y sus permisos para el consumo de las funcionalidades y servicios ofrecidos y habilitados en esta transición para CMI y RFJ. Fuente: (CGR, 2018)

Fuente: Elaboración propia

Definición de método a utilizar para recolectar datos.

- Definición del Instrumento a aplicar en la recolección de datos

Para esta fase se ha definido una técnica pues el método no basta, según (Ugalde Binda & Balbastre-Benavent, 2013), se hace necesario procedimientos y medios que hagan operativo los métodos, en este nivel se sitúan ***las técnicas***, donde existe una denominada ***técnica de interrogatorio***.

c. Para realizar esta técnica para el caso de la investigación que nos ocupa, se utiliza ***un instrumento*** de cuestionario denominado “Instrumento de medición de dimensiones del

Gobierno seguridad de la información, el cual podemos ver en la tabla 8 relacionada más abajo.

Este instrumento se aplica en forma escrita, solicitando al encuestado su opinión para valorar en forma personal, e interpretar la realidad del tema investigado, con el fin de evaluar ***el área de conocimiento*** del gobierno de seguridad de la información en la Contraloría General de la República y establecer la madurez de los componentes o dimensiones para fortalecer la capacidad de dirigir la Seguridad de la información en la entidad, que oriente a proponer un modelo adecuado a la CGR.

Al proponer este instrumento basado en una versión propia del Docente Andrés Ricardo Almanza, docente de la Universidad Externado; se tiene presente que según (Vivares, 2017) es más pertinente crear grillas de madurez por cuanto pueden compartir una estructura pero su contenido puede diferir de acuerdo al tema y Röglinger et al. (2012) citado por (Vivares, 2017, p.32) "argumentaron que un modelo de madurez debe servir para valorar el estado actual del dominio estudiado y proveer una guía para identificar medidas de mejoramiento que permitan su mejoramiento futuro".

En cuanto a los niveles de madurez (Vivares, 2017) indica que:

> Los niveles de madurez son aquellas etapas, niveles o estadios a lo largo de los cuales evoluciona y se analiza el objeto estudiado. Según se desprende de lo analizado anteriormente, son de los elementos centrales en un modelo de

madurez. La revisión de la literatura puso de manifiesto que lo más común es establecer cinco niveles de madurez”

En razón a esta argumentación para el instrumento de medición de dimensiones del Gobierno seguridad de la información se establecieron 5 niveles que se relacionan a continuación:

Tabla 7. Niveles definidos para el instrumento

No sabe	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**

Fuente: Elaboración propia

Y los principios o dimensiones definidas fueron siete (7), que son relacionadas con objeto de estudio ***: Cultura, Riesgo, Cumplimiento, Principios, Operaciones, Mediciones, y prácticas***; *que miden la madurez del gobierno de seguridad de la información este modelo madurez contemplado en el instrumento utilizado está* ***basado en los principios del modelo CMMI*** se han ajustado los niveles, sin embargo, los principios han sido tenidos en cuenta y las dimensiones definidas están apalancadas en los dominios de control de la ISO 27002, según figura 34 de este documento.

Este instrumento se revisa y ajusta en redacción algunas de las preguntas y niveles del instrumento original para que se adapte a la comprensión de los funcionarios de la Contraloría General de la República y sea aplicable a su entorno.

Tabla 8. Instrumento de medición de dimensiones de gobierno de seguridad de la información

INSTRUMENTO MEDICION DIMENSIONES GOBIERNO DE SEGURIDAD DE INFORMACIÓN
Este instrumento evalúa la **postura de seguridad de la información en sus siete dimensiones** y permite tener una visión integral de la seguridad de la información en la Contraloría General de la República, para poder **visualizar** cuales son **los componentes o dimensiones para fortalecer la capacidad de dirigir la Seguridad** de la información en la entidad. Esta información será utilizada en el entorno académico con propósitos de investigación. **Es importante aclarar que sus respuestas serán tratadas en forma confidencial y no serán utilizadas con otro propósito.**
Valoración de su nivel actual
Por cada dimensión (7), se hacen cinco preguntas que buscan determinar e***l nivel actual de avance*** en la dimensión relacionada. Marque con una (x) por pregunta revisada. Las escalas van avanzando en nivel donde la primera columna refiere a que usted no sabe si se aplica esta actividad, la segunda (No se aplica) es porque estas actividades de la dimensión aún no se realizan, la tercera indica que se piensa en ellas y se hacen sin regularidad, la cuarta se aplica pero se requiere un

control o alerta para realizarlo, y la última columna que es el nivel deseado al que debe llegar la organización, se hace de manera cotidiana, en forma autónoma, sin necesidad de control o alertas.

Agradecemos su colaboración en el diligenciamiento de este instrumento, este toma aproximadamente 15 minutos, para ser contestado.

Nivel del Cargo que ocupa en la Contraloría. Marque con una X el nivel que ocupa	**Coordinador**	**Profesional**	**Tecnólogo**	**Asistencial**
	Asesor		**Directivo**	
Dependencia				
	Niveles			
Dimensiones				
Cultura				

Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**
¿De qué forma se aplica el principio de considerar la protección de la información, como					

un valor en la organización?					
¿Se ejecutan con frecuencia los procesos de inducción, concienciación, entrenamiento y educación a toda la organización (directivos, ejecutivos, mandos medios, empleados, terceras partes, otros interesados, en materia de seguridad digital?					
¿Existen procesos de entrega de informes relacionados con los niveles de penetración de los programas de sensibilización en seguridad digital?					
¿Se trabaja de manera conjunta los procesos de construcción de cultura entre las áreas de RR.HH, Riesgos, y Seguridad para entregar los mensajes a la organización relacionados con seguridad de la información?					
¿Se aplican todos los procesos,					

procedimientos y políticas en materia de creación de cultura de seguridad de la información?					
Riesgos					
Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**
¿Su organización practica la gestión de riesgos de seguridad de la información como una disciplina constante y continua dentro de todos los procesos de la entidad?					
¿Su organización practica algún método, modelo, o desarrollo propio para la práctica de la gestión de riesgos en materia de seguridad de la información?					
¿Su organización aplica la gestión de riesgos al mundo de la seguridad					

de la información más allá del alcance del área de tecnología?					
¿Su organización presenta reportes de los estados de riesgos de seguridad de la información a la organización?					
¿Su organización desarrolla las prácticas necesarias para tratar los riesgos de seguridad de la información que involucra a las partes interesadas (terceros involucrados)?					
Cumplimiento					
Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**
¿Su organización atiende de manera continua los temas de cumplimiento en materia de					

seguridad de la información?					
¿Aplica su organización un trabajo interdisciplinario a la hora de pensar en procesos de cumplimiento?					
¿Su organización aplica el principio rector "debemos cumplir porque sino…."?					
¿Esta su organización continuamente revisando las posibles regulaciones, normas y leyes que puedan ser aplicables en materia de seguridad o solo cuando estas llegan?					
¿Esta su organización dispuesta a recibir de manera espontánea un proceso de auditoría sin que eso cause traumatismos?					
Principios					
Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin**	**Se aplica y se requiere de un**	**Se hace de manera cotidiana, en**

			regularidad	control o alerta para realizarlo	forma autónoma
¿Revisa su organización con frecuencia (anual, mensual, etc.) todo su marco de políticas o principios rectores relacionados con la seguridad de la información?					
¿Practica su organización los principios y/o políticas de seguridad de la información?					
¿Los principios y/o políticas de seguridad de la información creen que se definen y aplican acorde a la realidad de su organización?					
¿Existen procesos claros y ejecutados con periodicidad para validar la aplicación de los principios y/o políticas en su organización?					
¿Se presentan informes de cómo se siguen los principios de seguridad					

de la información en su organización?					
Operaciones					
Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**
¿Su área de seguridad atiende a los procesos definidos en materia de seguridad de la información?					
¿Existe un área de seguridad de la información que aplique con criterio e imparcialidad las funciones propias de su responsabilidad?					
¿Se aplican los procesos de seguridad de la información y se tiene un responsable que haga el seguimiento de dichas operaciones?					
¿Se tiene claro cuáles son las responsabilidades entre las áreas como					

Tecnologías de la Información, Riegos, Seguridad a la hora de realizar las operaciones en materia de seguridad de la información?					
¿Existen reportes de cómo la organización opera y gestiona la seguridad al interior y con sus partes interesadas (terceros involucrados)?					
Mediciones					
Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**
¿Practica la organización el proceso de crear métricas o mediciones para cuantificar el efecto de la seguridad en la organización?					
¿Existe algún proceso periódico de presentación de resultados relacionados con seguridad de la					

información?					
¿Los procesos/mediciones se aplican y son llevados a los distintos niveles de la organización?					
¿Se utiliza como práctica la integración de las mediciones con los programas de gestión de riesgos?					
¿Se definen planes de mejoras basados en los resultados de la mediciones y se hace seguimiento a los mismos de manera regular?					
Prácticas					
Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**
¿La organización usa algún marco de referencia como guía de buenas prácticas en materia de seguridad de					

la información?					
¿Las prácticas involucran a toda la organización o solo se aplican a áreas específicas?					
¿Las prácticas de seguridad de la información se definen basados en procesos de gestión de riesgos, o se hacen solo por que se cree que son necesarias?					
¿Existe solo un área responsable por implementar las prácticas de seguridad en su organización?					
¿Existen mecanismos o procesos formales y continuos para revisar la implementación de las prácticas y trabajar de manera interdisciplinar su implementación?					

Aplicación del instrumento de medición de dimensiones de seguridad de la información en la CGR.

- ✓ **Realizar Piloto del Instrumento:** Para verificar que el instrumento fuera comprensible y recolectará información relevante para la investigación, se realiza una primera aplicación

a un grupo de 10 personas quienes observan y comentan acerca de éste para realizar mejoras; entre las observaciones indicaron:

- ✓ Presentación e introducción del objetivo de la encuesta.
- ✓ Indicar el tiempo aproximado en contestar la encuesta.
- ✓ Verificar escalas 3 y 4 porque la personas comentan que se confunden.
- ✓ Agregar una nueva escala de no sabe, por cuanto algunas personas manifestaron no saber algunas de las preguntas realizadas y no estaba la escala de no sabe, y la opción no se aplica se refería a que lo preguntado no se realizaba, pero no referencia que el encuestado no sabe o no está enterado del tema.
- ✓ Se pensó en asignar una escala numérica, pero se concluye que se dejaría cualitativa porque se requería saber nivel de madurez de las actividades de cada pregunta en forma de cualidad.
- ✓ Los primeros niveles propuestos fueron las siguientes:

Tabla 9. Primeras Niveles propuestas para instrumento

No se aplica	Se piensa en ello y se hace sin regularidad	Se aplica y se requiere de verificación su aplicación	Se hace de manera cotidiana

Fuente: (Almanza, 2018)

Los niveles definitivos después del piloto son:

Tabla 10. Niveles definitivos para el instrumento a aplicar

No sabe	No se aplica	Se piensa en ello y se hace sin regularidad	Se aplica y se requiere de un control o alerta para realizarlo	Se hace de manera cotidiana, en forma autónoma

Fuente: (Basada en Almanza, 2018)

Aplicación del Instrumento Dimensiones de seguridad de la información

Después de definir el instrumento y realizar las correcciones identificadas en el piloto, se definió lo siguiente: La utilización de métodos cualitativos y como indica (Canales, Alvarado, & Pineda, 2008, p.120) "en la investigación cualitativa, la lógica de la muestra se basa en estudiar a profundidad algo a fin de que sea válido. Usualmente esto se hace en pocos casos seleccionados en forma intencionada."

Es por esto que para definir la muestra, y aplicar este instrumento se toma una de las estrategias descritas por (Quinn Patton, 1990) citado por (Canales et al., 2008) para seleccionar muestras en estudios cualitativos, ésta es:

> **Muestreo de máxima variabilidad.** En la muestra se incluyen las diferentes posibilidades de las variables más importantes. Por ejemplo, si se está realizando una evaluación de las egresadas de una escuela de enfermería y se estima que el área geográfica del desempeño es importante, en la extracción de los casos habría que asegurar incluir unas de área urbana, otras de área rural y unas del área semi-urbana.

Para el caso de la temática de Gobierno de Seguridad de la información, y el estudio de cómo se percibe éste en la Contraloría General de la República, es muy apropiado utilizar este método por cuanto desde los diferentes cargos y niveles jerárquicos existe una vista diferente e importante que permite definir que observa cada nivel y como percibe su aporte a este tema.

Otro factor importante a tener en cuenta es la triangulación la cual según explica (Sociedad Colombiana de Psiquiatría., 2005, p.120), ofrece la alternativa de poder visualizar un problema desde diferentes ángulos (sea cual sea el tipo de triangulación) y de esta manera aumentar la validez y consistencia de los hallazgos".

Teniendo en cuenta, lo planteado anteriormente, la investigación de este documento basa su aplicación del instrumento, así:

Cantidad de población: 4200 funcionarios

Muestra tomada: 60 Personas.

Para construir una vista global de cómo se percibe las dimensiones de Seguridad de la información en la CGR, y las subvistas por cargo, de cómo cada nivel jerárquico lo percibe; para lo cual se definen las siguientes variables:

- **Directivos:** En esta variable se encuentran incluidos, Jefes, coordinadores, Directores, quienes ven el caso de estudio (gobierno de seguridad de la información en la CGR) desde la cúspide de la pirámide y desde su rol de dirección estratégica.
- **Asesores:** En esta variable se incluyen los asesores que corresponde al rol de asesoría al directivo por tener una experiencia y una especialidad de algún tema específico en el que este asesorando.
- **Profesionales:** En esta variable se incluyen los profesionales que corresponden a la parte media de la pirámide que tienen el rol de gestionar, ejecutar las actividades misionales de la Entidad desde su rol de experto en algún tema necesario para el logro de los objetivos de la entidad desde las diferentes dependencias.
- **Tecnólogos:** En esta variable se incluye todos los funcionarios de la CGR que tienen el rol de soporte de sistemas en las diferentes dependencias y Gerencias.
- **Asistenciales:** En esta variable se incluyen todos los oficinistas, mensajeros, personas de archivo que tienen un rol de asistentes administrativos en la CGR.

Tipo de Muestreo: Máxima variabilidad, tomando una o dos muestras de personas que corresponden en la mayoría de los casos a (1) una o hasta (5) cinco personas por dependencia del Nivel Central de la CGR, y (1) una persona en (11) once Gerencias Departamentales en la otras ciudades del país, para tener un cubrimiento de la tercera parte de las Gerencias, por cuanto en total son (31) treinta y una; para un total de **60 funcionarios** de diferentes cargos de acuerdo a las variables descritas anteriormente, lo que permite una variabilidad de casos relacionados con el cargo y nivel jerárquico de la persona, donde cada caso, muestra una vista del objeto estudio

(gobierno de seguridad de la información). El instrumento se aplica de acuerdo a lo relacionado en la Tabla 9.

Es así que se realiza esta muestra que corresponde a por lo menos 1 o 2 personas de diversos cargos con niveles jerárquicos diferentes para la CGR con visiones diversas de la madurez de seguridad de la información en la Entidad, como la percibe desde su rol, funcionarios que son tomados como variables, y que desde la vista del investigador que está inmerso en el estudio son funcionarios que son claves para obtener esa percepción de la madurez sobre el objeto de estudio.

Tabla 11. Relación de Dependencias y Gerencias de la CGR donde se aplica el instrumento

	Dependencias	**Cantidad encuestados**
1	Despacho del Contralor General de la República	1
2	Despacho del Vicecontralor	1
3	Secretaría Privada	1
	Oficinas de Apoyo	
4	Oficina de Comunicaciones y Publicaciones	2
5	Oficina Jurídica	1
6	Oficina de Control Interno	1
7	Oficina de Control Disciplinario	1

	Dependencias	**Cantidad encuestados**
8	Oficina de Planeación	2
9	Oficina de Sistemas e Informática	5
10	Centro de Estudios Fiscales	1
	Gerencia de Talento Humano	
11	Dirección de Talento Humano	2
	Gerencia Administrativa y Financiera	
12	Dirección Financiera	2
13	Dirección de Recursos Físicos	1
14	Dirección de Imprenta, Archivo y Correspondencia	2
	Unidades Especiales de Apoyo	
15	Unidad de Investigaciones Especiales Contra la Corrupción	1
16	Unidad de Cooperación Nacional e Internacional de Prevención, Investigación e Incautación de Bienes	1
17	Unidad de Apoyo Técnico al Congreso	1
18	Unidad de Seguridad y Aseguramiento Tecnológico e	5

	Dependencias	**Cantidad encuestados**
	Informático	
	Contralorías Delegadas	
19	Contraloría Delegada de Economía y Finanzas Públicas	2
20	Contraloría Delegada Sector Agropecuario	2
21	Contraloría Delegada Sector Defensa, Justicia y Seguridad	3
22	Contraloría Delegada Gestión Pública e Instituciones Financieras	1
23	Contraloría Delegada de Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo	2
24	Contraloría Delegada Sector Medio Ambiente	2
25	Contraloría Delegada Sector Minas y Energía	2
26	Contraloría Delegada Sector Social	2
27	Contraloría Delegada para Investigaciones, Juicios Fiscales y	1

	Dependencias	**Cantidad encuestados**
	Jurisdicción Coactiva	
28	Contraloría Delegada para la Participación Ciudadana	1
	Total Sede Nivel Central Bogotá	**49**
	Gerencias Departamentales	
1	Amazonas	0
2	Antioquia	1
3	Arauca	1
4	Atlántico	0
5	Bolívar	0
6	Boyacá	1
7	Caldas	1
8	Caquetá	0
9	Casanare	0
10	Cauca	1
11	Cesar	0
12	Choco	0
13	Córdoba	1
14	Guainía	0
15	Guajira	0
16	Guaviare	0

	Dependencias	Cantidad encuestados
17	Huila	0
18	Magdalena	0
19	Meta	0
20	Nariño	0
21	Norte de Santander	1
22	Putumayo	0
23	Quindío	1
24	Risaralda	1
25	San Andrés	0
26	Santander	1
27	Sucre	0
28	Tolima	1
29	Valle	0
30	Vaupés	0
31	Vichada	0
		11
		60

Fuente: Elaboración propia, ajustado directorio CGR

Fase 2. Resultados y análisis de la información recolectada

Después de realizadas las encuestas y con los instrumentos diligenciados por los funcionarios encuestados, se realiza la tabulación del instrumento de las dimensiones de seguridad de la información que explicó a continuación, se toma la Tabla 8. Escalas definitivas para el instrumento aplicado y se asigna un valor numérico, que corresponde al peso del criterio a evaluar dentro del modelo de calificación del instrumento, es decir, se decide dar dichos criterios basados en la importancia de cada uno, donde 0, es no sabe y el criterio más importante para obtener un nivel de madurez es el 5 así:

Tabla 12. Valoración de criterios

	No sabe	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**
Peso del Criterio	0	1,5	2,5	4	5

Fuente: Elaboración propia basada en las escalas del instrumento propuesto

Para explicar esta evaluación, observemos la tabla 11, donde en la columna 3, la cantidad de personas que contestan en esa escala corresponde a (16) personas, este valor es multiplicado por la valoración de criterios de la tabla 10 de acuerdo a la escala (Se piensa en ello y se hace sin regularidad=2,5), y se van sumando uno a uno la cantidad de encuestados que contestó cada pregunta, con los pesos de cada criterio; luego, se divide por la cantidad

total de personas que contestan la encuesta, para esta caso 60 personas, lo que permite calcular el promedio por pregunta.

Por último, se promedian los totales de cada pregunta para obtener el promedio general de cada Dimensión que para este caso es cultura y corresponde a 2.82.

Tabla 13. Explicación del cálculo por dimensión de seguridad de la información

Cultura						
Pregunta	**No sabe**	**No aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**	**Promedio por pregunta**
¿De que forma se aplica el principio de considerar la protección de la información, como un valor en la organización?	4	0	16	25	15	3,58
¿Se ejecutan con frecuencia los procesos de inducción, concienciación, entrenamiento y	4	4	23	23	6	3,09

Cultura						
Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**	**Promedio por pregunta**
educación a toda la organización (directivos, ejecutivos, mandos medios, empleados, terceras partes, otros interesados, en materia de seguridad de la información?						
¿E1isten procesos de entrega de informes relacionados con los niveles de penetración de los programas de sensibilización en seguridad de la información?	14	9	27	9	1	2,03
¿Se trabaja de manera conjunta los procesos de construcción de cultura entre las áreas de RR.HH, Riesgos, y Seguridad	7	10	28	13	2	2,45

Cultura						
Pregunta	**No sabe**	**No se aplica**	**Se piensa en ello y se hace sin regularidad**	**Se aplica y se requiere de un control o alerta para realizarlo**	**Se hace de manera cotidiana, en forma autónoma**	**Promedio por pregunta**
para entregar los mensajes a la organización relacionados con seguridad de la información?						
¿Se aplican todos los procesos, procedimientos y políticas en materia de creación de cultura de seguridad de la información?	5	5	23	21	6	2,98
Promedio Definitivo de la dimensión Cultura	6,8	5,6	23,4	18,2	6	**2,82**

Fuente: Elaboración Propia.

El final de la evaluación culmina cuando se realiza el mismo procedimiento con las 6 dimensiones restantes que propone el instrumento. Lo cual se consolida en un cuadro para sacar el porcentaje de percepción de la madurez global de seguridad de la información en la CGR según el instrumento como se observa aquí:

Tabla 14. Porcentajes por dimensión desde la visión Global de la CGR

Vista Global CGR	
Cultura	2,8
Riesgos	2,5
Cumplimiento	2,8
Principios	2,9
Operaciones	3,2
Mediciones	1,6
Prácticas	3,1
Total Dimensiones	**2,7**

Fuente: Elaboración propia. Excel Consolidado Visión global, calcula datos recolectados

Resultados y análisis de la vista Global de dimensiones de seguridad de la información en la CGR

La gráfica 8, muestra la percepción general de los encuestados, donde se observa que las dimensiones con mayor peso son Operaciones con 3,2, prácticas con 3,1, principios con 2,9, desde la experiencia que se tiene en la Entidad, se puede decir que esto se da porque a partir del año 2016, se viene trabajando en el establecimiento del Sistema de Gestión de Seguridad (SGS) generando principios y lineamientos de seguridad de la información, y comunicando a los funcionarios la existencia de dicha políticas, lo que hace que este indicador se encuentre alto.

Gráfica 1. Vista global de las dimensiones de seguridad de la información en la CGR

Después de realizado el análisis para la vista global de la CGR y teniendo en cuenta que se utiliza el método cualitativo y se realiza por **muestreo de máxima variabilidad**, en donde la variables diversas son los cargos distribuidos jerárquicamente, de la planta de personal de la Entidad. A continuación se muestra el consolidado de Cargos y totales de personas a las que se aplica el instrumento y con lo cual se grafican las diversas ***vistas de la población*** de las dimensiones de seguridad de la información.

Tabla 15. Cargos y totales personas a las que se aplica el instrumento

Cargos	**Directivo**	**Coordinador**	**Profesional**	**Tecnólogo**	**Asistencial**	**Asesor**
Total Encuestados	**2**	**3**	**29**	**8**	**11**	**7**

Fuente: Elaboración propia.

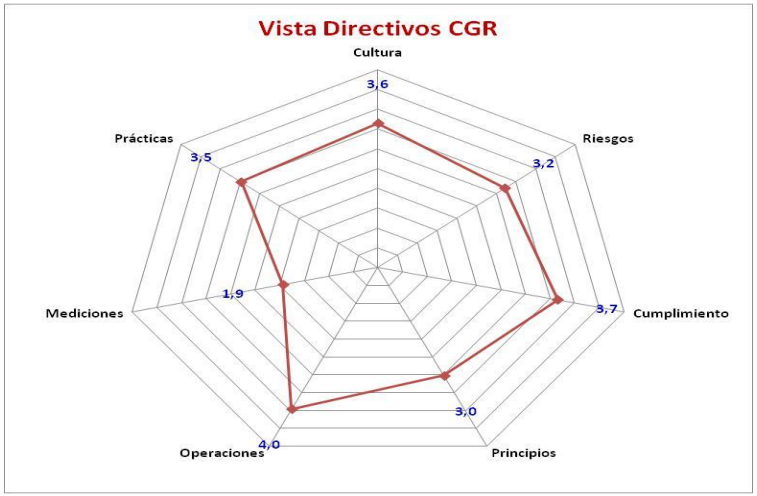
Resultados Instrumento de medición dimensiones de seguridad de la información por variables (Cargos)

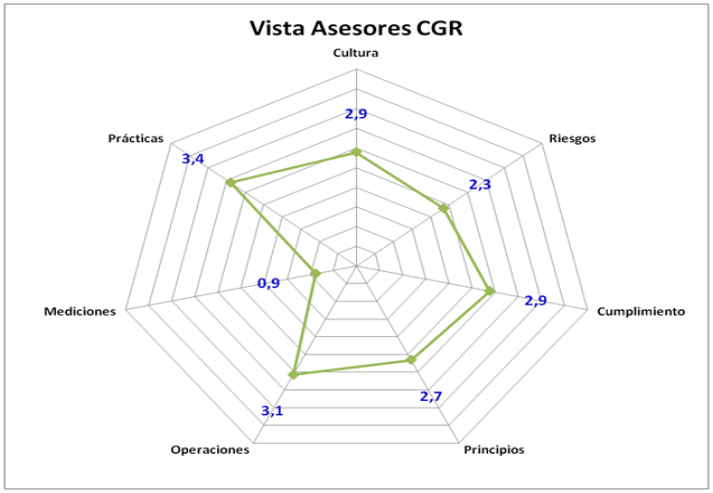
Para tener una mejor percepción y visión de las dimensiones de seguridad de la información en la Entidad se aplica el instrumento de manera cualitativa utilizando el muestreo de máxima variabilidad, donde desde diversos cargos o niveles de la pirámide jerárquica de la organización se recolectan percepciones de la seguridad de la información que permiten *la triangulación* de la información desde distintos ángulos, para tener una visión más precisa de la percepción de la madurez de la seguridad de la información en la entidad y como la observan los servidores públicos que hacen parte de la CGR desde sus diversos cargos y funciones.

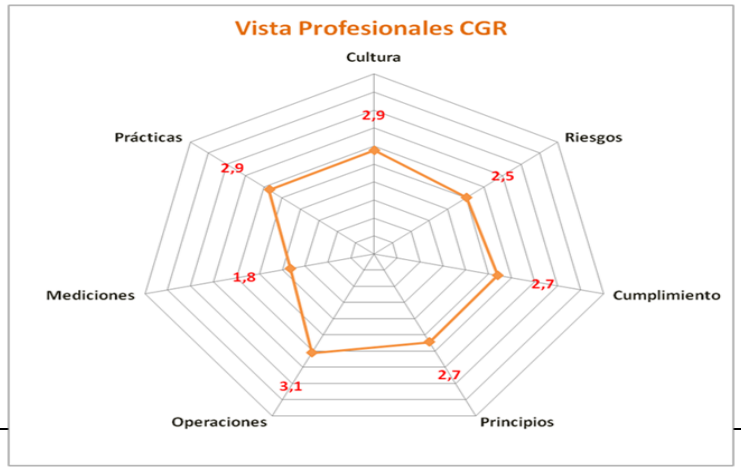
Al aplicar este instrumento a diversos cargos podemos ver como la triangulación provee una herramienta importante para visualizar el problema del Gobierno de seguridad de la información desde diferentes ángulos; como lo ve cada nivel jerárquico de la Entidad, lo que nos sirve para triangular la información recolectada y poder establecer las diversas vistas y obtener una global.

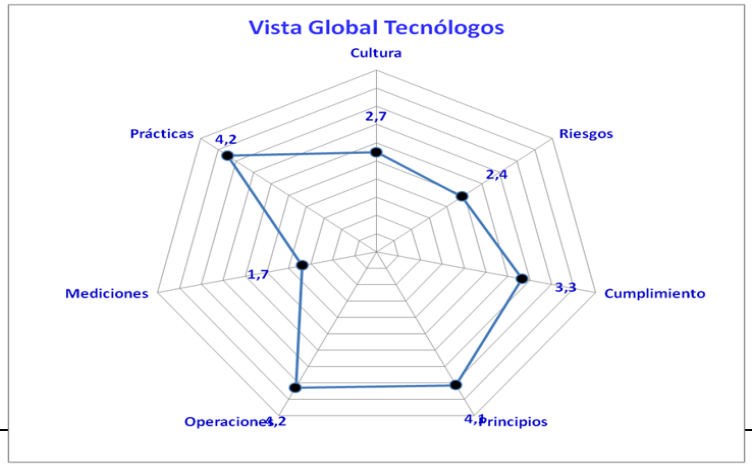
A continuación se realiza el análisis de las vistas desde los diferentes cargos Directivos, Asesores, Profesionales, Tecnólogos y Asistenciales, sobre cómo perciben las dimensiones de seguridad de la información en la Contraloría General de la República.

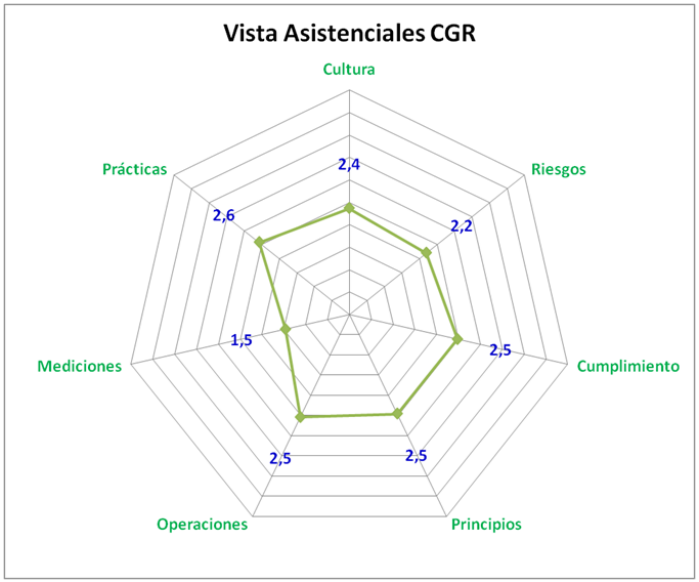
Tabla 16. Comparativo de vistas de diferentes cargos de dimensiones de seguridad de la información y percepción del nivel de madurez - Directivos CGR











Dimensiones con baja Madurez:

Mediciones y Riesgos son las dimensiones que se perciben con una menor madurez, esto es entendible porque aunque se realizan mediciones y gestión de riesgos, aun no se tienen incluidos los riesgos de seguridad de la información en el mapa

Dimensiones con Mayor Madurez:

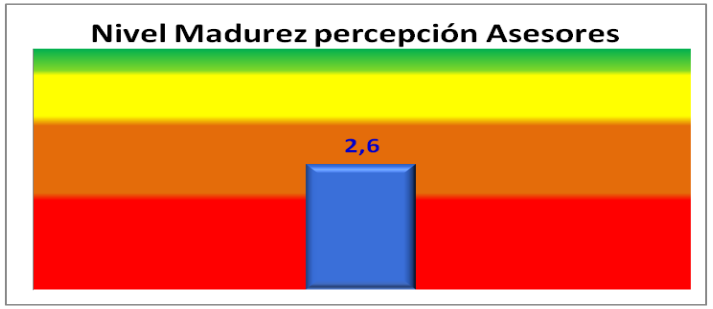
Las anteriores gráficas evidencian que los ***directivos y los tecnologos*** tienen una visión muy similar de las dimensiones de seguridad, esto en razón a que los tecnologos están siempre más conscientes de lo que la entidad avanza en seguridad digital, y los directivos con lo términos de cumplimiento, tienen una percepción de la seguridad digital como importante, por ser política de estado desde los CONPES generados para ello, siendo las dimensiones de ***Principios, cumplimiento***, ***operaciones y prácticas,*** las mas maduras para éstos dos niveles.

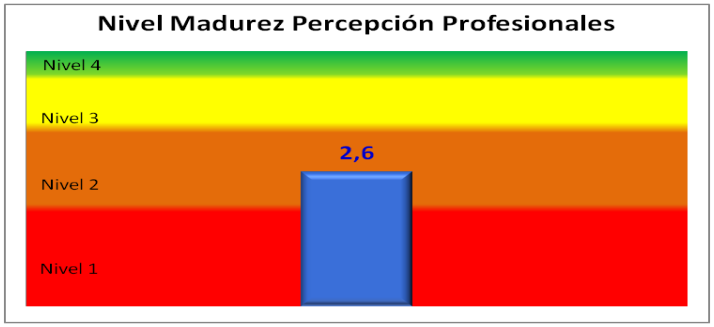
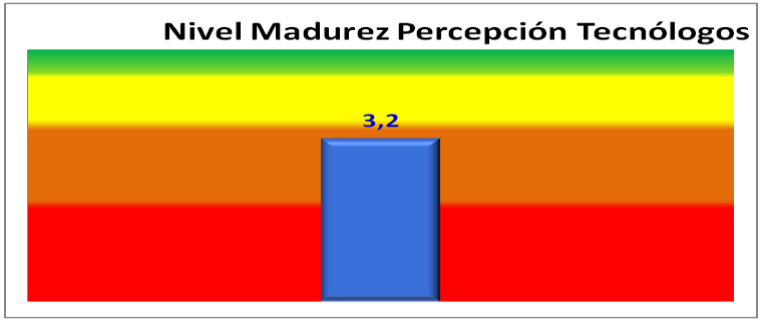
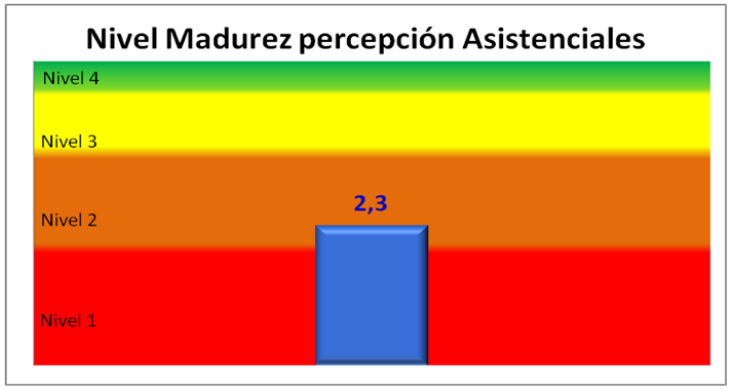
En cuanto a los niveles de ***asesor y profesionales***, son las dimensiones de ***operaciones, prácticas y cultura*** las que más madurez perciben ellos, esto por cuanto son el nivel medio que ejecuta, están más en función de generar cultura de seguridad en la

de riesgos de la Entidad, es sólo ahora con la Guía para la administración de Riesgos que publico el Departamento Administrativo de la Función Pública (DAFP), que la CGR esta incursionando en incluir a su gestión de riesgos esta capítulo. En cuanto a las mediciones en ese tema solo existe un indicador de incidentes de seguridad de la información y no se han definido un conjunto de indicadores de seguridad de la información que permita desde la Oficina de Planeación, tener una medición o evaluación de los mismos, por eso la percepción de todos los grupos es consistente con la realidad, aunque el grupo de asistenciales y algunos profesionales estas dos dimensiones no las tienen muy claras. La Dimensión de ***cultura***, también la ven un poco baja en relación con las otras, y éste tema si se puede considerar como alerta, por cuanto desde el año 2016, se inicia con la creación	organización y las operaciones y las prácticas son su día a día para liderar o ejecutar por esto tienen mayor claridad del avance de estas dimensiones En cuanto a los niveles ***asistenciales*** se observa una marcada diferencia de su percepción muy baja para la madurez de todas las dimensiones, esto en razón a que muchos de ellos dicen no saber ni entender algunas preguntas realizadas en las dimensiones planteadas en el instrumento; lo que evidencia que aunque desde el área de seguridad se comunica sobre la importancia y las buenas prácticas de la seguridad digital, aún no permea del todo en la parte base de la piramide jerarquica, las dimensiones de seguridad no las tienen claras y cuando se les preguntaba, comentaban que el tema era como de la Unidad de seguridad, de la Oficina de Planeación de la oficina de Sistemas, pero no ven su rol como importante para movilizar y vivenciar la seguridad digital en la Entidad.

del Sistema de Gestión de Seguridad (SGS) y desde el segundo semestre de 2017 la Unidad de Seguridad ha enfocado sus esfuerzos para fortalecer la cultura de seguridad de la información a través de tips publicitarios y eventos de seguridad de la información donde se explican y exponen estos temas y aunque ha tenido gran acogida por parte de los servidores públicos de la CGR a algunos no llega según los resultados obtenidos.	

Tabla 17. Análisis de la vista de dimensiones de seguridad de la información y Nivel de madurez

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td> 
</td>
<td>Son los Directivos y los tecnólogos quienes describen el porcentaje más elevado de madurez de la seguridad de la información con un promedio de 3,2, esto se da porque están más cerca a la tecnología (tecnólogos), y al cumplimiento (Directivos), en cuanto a los profesionales y asesores perciben un mismo nivel de madurez 2,6, esto se da porque son los encargados de liderar los procesos de seguridad de la información y ejecutar y operar los mismos, entonces perciben que la madurez avanza en un término medio.
Y los asistenciales perciben el nivel de madurez más bajo con un 2,3, se puede decir que desde la parte superior no se está realizando adecuadamente la comunicación de los avances realizados en las dimensiones de la seguridad digital, lo que permea en que el común</td>
</tr>
</table>

	del funcionario no conoce o no tiene claro los temas de seguridad de la información.

Fase 3. Diagnóstico del nivel de percepción de madurez del estado de Gobierno de Seguridad de la información- Vista Global CGR

Verificar los resultados del nivel de madurez de las dimensiones o componentes de seguridad de la información, después de aplicado el instrumento.

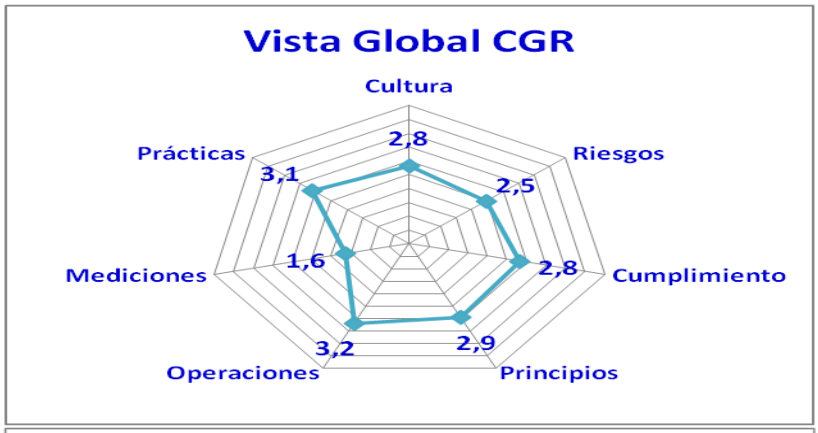
El resultado de sumar los totales de las siete (7) dimensiones, corresponde al nivel de madurez de la Entidad que para este caso y según la tabla es **2,7** (dos, siete), que corresponde a un ***Nivel 2***, que indica según la tabla 13 que la visión global o percepción de toda la población encuestada ven que la Contraloría esta en un nivel ***-donde se reconoce que la postura de seguridad de la información es necesaria para aportar al negocio. Sin embargo no existen sino intentos, o iniciativas por separado; posiblemente algunos esfuerzos y controles base.***

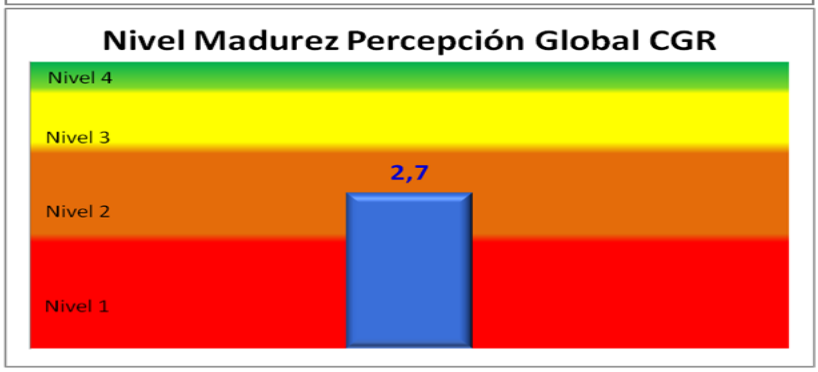
Tabla 18. Tabla de escalas de Nivel de madurez

Niveles	**X**	**Y**	**Inicial Valorativo**	**Descripción Nivel Madurez**
Nivel 1	1,25	1,25	0	No tiene claro que requiere hacer mejoras, identificar y reconocer que no hay un modelo o prácticas sostenidas en materia de seguridad de la información. Es posible que se ejecuten acciones, pero son aisladas, desconectadas y sin orden ni orientación.

Niveles	X	Y	Inicial Valorativo	Descripción Nivel Madurez
Nivel 2	1,25	3,75	1	En este nivel se reconoce que la postura de seguridad de la información es necesaria para aportar al negocio. Sin embargo no existen sino intentos, o iniciativas por separado; posiblemente algunos esfuerzos y controles base.
Nivel 3	3,75	3,75	0	En este nivel se sabe que hay algún conjunto de prácticas y modelos de seguridad; se realizan de manera secuencial, consistente y coordinada. Se requiere de esfuerzos para que el modelo se mantenga. Se sabe que se hace y se hacen todos los esfuerzos para que se siga sosteniendo el modelo
Nivel 4	3,75	1,25	0	En este nivel la postura de seguridad de la información está adherida a la cultura de la organización. Es intuitiva, ya existe una consciencia profunda de su valor, y por tanto, prácticas, procesos y procedimientos permean en todos los niveles de la misma.

Gráfica 2. Nivel de madurez de Seguridad de la información percepción global en la CGR


Vista Global CGR
Cultura
Riesgos
Cumplimiento
Principios
Operaciones
Mediciones
Prácticas
2,8
2,5
2,8
2,9
3,2
1,6
3,1


Nivel Madurez Percepción Global CGR
Nivel 4
Nivel 3
Nivel 2
Nivel 1
2,7

Fase 4. Formulación de la propuesta

Para Formular y presentar una propuesta del modelo de gobierno de seguridad de la información para la CGR, se analiza la información recolectada en el trabajo de campo realizado, y se encuentra que el modelo de de gobierno de seguridad de la información para la CGR, debe estar basado en las 7 dimensiones de seguridad de la información, ***Principios, Cultura, Riesgos, Mediciones, Cumplimiento, Operaciones y Prácticas***, el cual será plasmado en el siguiente modelo tomando su diseño en base al análisis de la información recolectada y sus resultados, para fundamentar un modelo de Gobierno de Seguridad de la información para la CGR, que permita orientar las iniciativas actuales y encausarlas para lograr dicho objetivo, el cual se describirá en el capítulo 5.

Capítulo 5

Diseño del Modelo de Gobierno de seguridad de la información para la CGR

A continuación se muestra el diseño del modelo propuesto el cual está basado en el avance realizado en n la implementación del ***Sistema de Gestión de Seguridad de la Información SGSI*** de la Entidad, que da un punto de partida para proponer el modelo, por cuanto esta formalizado en la CGR, sin embargo, de los avances que se han tenido en este sistema, salen insumos para alimentar el modelo en las dimensiones de políticas y principios, por cuanto existe una base documental del SGSI, libros, cartillas de políticas, así también, existen insumos para la parte cultura en relación con el plan de apropiación que se genera anualmente y los procesos de concientización y capacitación del SGSI, realizados en los procesos de inducción y re inducción a los funcionarios de la CGR, mesas de trabajo en donde se ha revisado la metodología de riesgos de la Entidad que está en revisión para incluir los riesgos de seguridad de la información, avances en el tema de cumplimiento en relación con el adelanto que se ha tenido con la política de tratamiento de datos personales, política de seguridad y privacidad y el avance que se ha realizado sobre el tema de Gestión Riesgo y Cumplimiento (GRC).

El modelo propuesto se basa en los principios de la ISO / IEC 27014 y se realiza una abstracción de lo solicitado por gobierno en línea en el Modelo IT4 + para el Estado Colombiano y en el MSPI Modelo de seguridad y privacidad de la información para lo cual se propone el siguiente modelo de gobierno de seguridad de la información para la CGR:

Modelo basado en 7 componentes, Cuatro (4) componentes que corresponden a GOBIERNO éstos son: Políticas o Principios, Cumplimiento, Riesgos y cultura y para completar el ciclo de la seguridad se tienen los otros componentes que hacen parte de GESTIÓN que corresponde a Operación, medición y prácticas y que son los encargados de ejecutar lo que se delinea desde la estrategia.

Figura 35. Modelo de Gobierno de Seguridad de la información propuesto para la CGR

Fuente: Elaboración propia

Componentes del Modelo de Gobierno Propuesto

Como resultado de la información recolectada en el instrumento de dimensiones de gobierno de seguridad de la información y la revisión de documentación del Sistema de Gestión de Seguridad SGSI que actualmente está avanzando en implementación en la CGR, se detalla explicación del nivel de madurez del componente y la ruta a seguir propuesta para madurar en éste.

1. Políticas o Principios

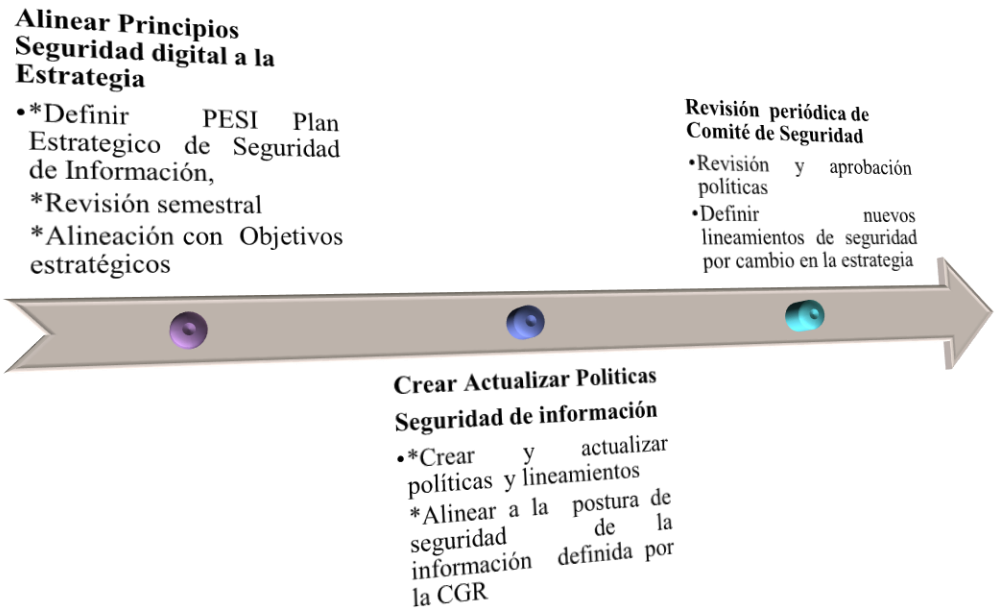
Dar lineamientos alineados a la estrategia, definir la postura de seguridad digital de la CGR

Para este componente se observa que la CGR, ha avanzado en la aprobación de 31 políticas de seguridad y 2 normas aprobadas, más 12 normas pendientes de aprobación, para lo cual se ha consolidado una base documental que parte de la resolución OGZ 0531 de 2016 (República, 2016), que crea y formaliza el Sistema de Gestión de Seguridad SGS de la Contraloría General de la República, luego se escriben y publican las políticas de seguridad las cuales se consolidan en el libro de políticas.

El modelo de seguridad de la información propuesto recomienda durante la implementación del Sistema de Gestión de Seguridad en su componente de información (SGSI) generar procesos para administrar este Sistema para tener una trazabilidad en el tiempo, con el fin de mantener la creación y actualización de políticas, normas y procedimientos que permeen a toda

la organización en materia de Seguridad de la información conservando la alineación con los objetivos estratégicos

Figura 36. Ruta para el componente Políticas o principios



Socios Estratégicos: Despacho Contralor, Oficina Planeación, USATI, Oficina Sistemas, Gerencia Talento Humano, Gerencia Administrativa y Financiera, Comité de Seguridad, y Comité de Arquitectura Empresarial

Fuente: Elaboración propia

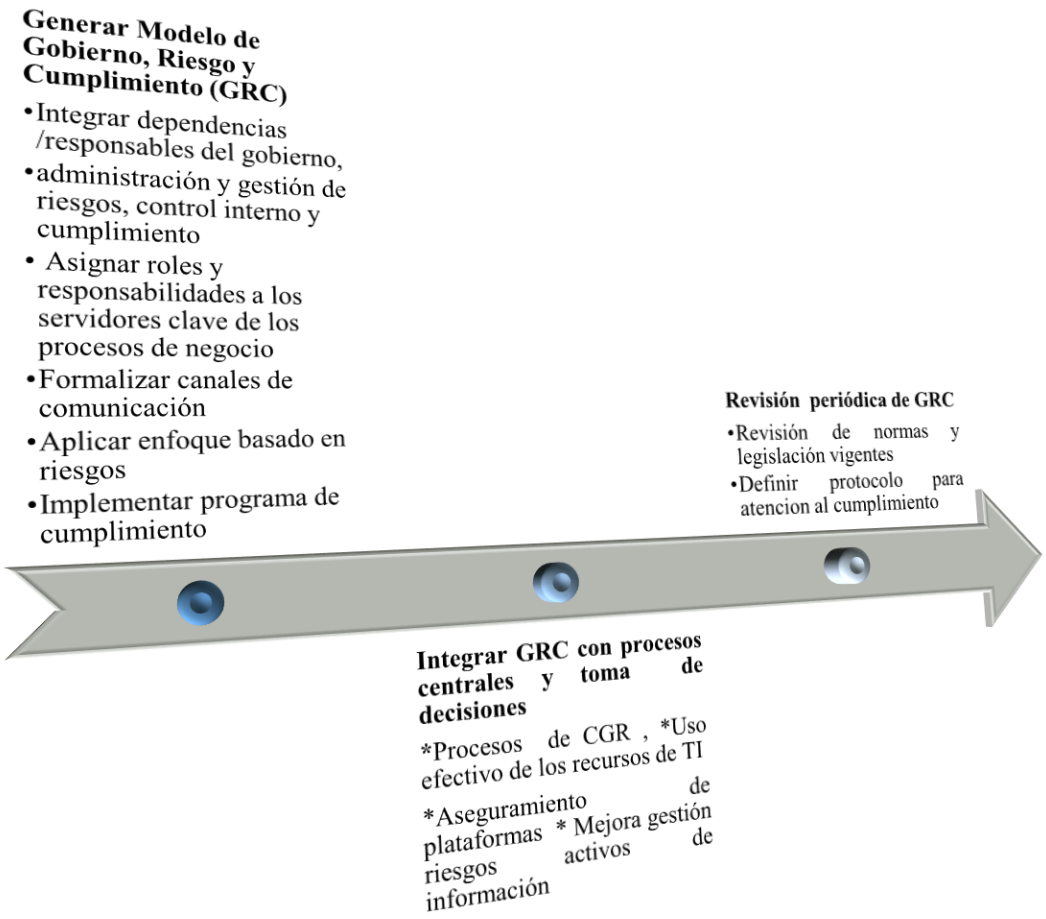
2. Cumplimiento

Atender y cumplir cambios legislativos y normativos, acatar regulaciones sobre protección de datos personales.

En este componente la CGR siempre está por la línea de cumplimiento por cuanto, es una Entidad del Estado enmarcado en un entorno donde siempre existen unas políticas de Estado que se debe cumplir, para el tema de Seguridad de Información se ha avanzado en los temas de Gobierno en Línea que ahora se denomina Gobierno Digital, en relación al modelo de privacidad y seguridad de la información

Actualmente, también se ha implementado a través de un proveedor jurídico el tema de avanzar sobre el tema de Gestión de Riesgo y Cumplimiento (GRC), para administrar la gestión de riesgos, definir roles y responsabilidades e implementar un programa de cumplimiento, para lograr este enfoque se propone la ruta recomendada en la figura 31.

Figura 37. Ruta para el componente de cumplimiento



Socios Estratégicos: Despacho Contralor, Oficina Planeación, Comité de Arquitectura empresarial, USATI, Oficina Sistemas, Comité de Seguridad

Fuente: Elaboración propia

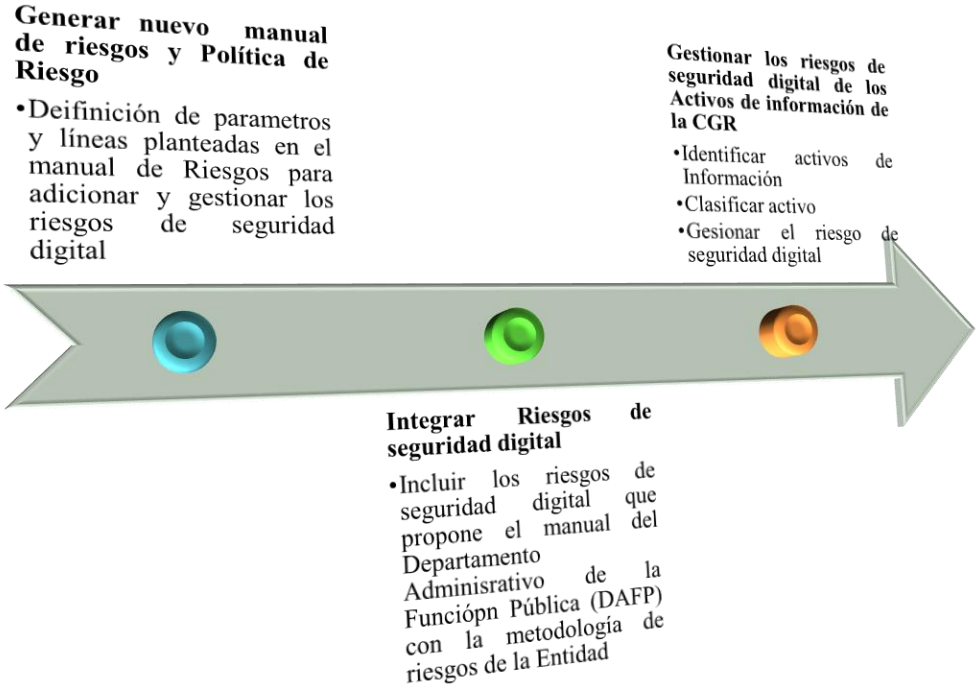
3. Riesgos

Proteger el modelo de generación de valor, desde el umbral de riesgo conocido que declara la Entidad.

En este tema la Entidad no ha avanzado mucho, hasta el momento la Oficina de Planeación llevaba a cabo la gestión de riesgos de toda la Entidad, articulando mesas de trabajo donde cada dependencia generaba su matriz de riesgos, pero no eran tenidos en cuenta los riesgos de seguridad de la información.

Solo es a partir de este año 2019 y con la publicación de la Guía para la administración del riesgo y el diseño de controles en entidades públicas y riesgos de gestión , corrupción y seguridad digital (Departamento Administrativo de la Función Pública, 2018) que la Oficina de Planeación ha planteado la actualización del procedimiento de riesgos, invitando a participar a la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI) para incluir los riesgos de seguridad digital.

Figura 38. Ruta para el componente de Riesgos



Socios Estratégicos: Oficina de Planeación (Admin Riesgos CGR), USATI (Riesgos seguridad digital) , Dirección de archivo imprenta y correspondencia (Riesgos documentales, Activos de Información), Gerencia Administrativa y Financiera (Riesgos de Bienes) , Gerencia Talento humano (Riesgos de Personas)

Fuente: Elaboración propia

4. Cultura

Generar y afianzar la cultura de seguridad, a través de sensibilización, capacitación y entrenamiento de los funcionarios para minimizar el riesgo de seguridad digital.

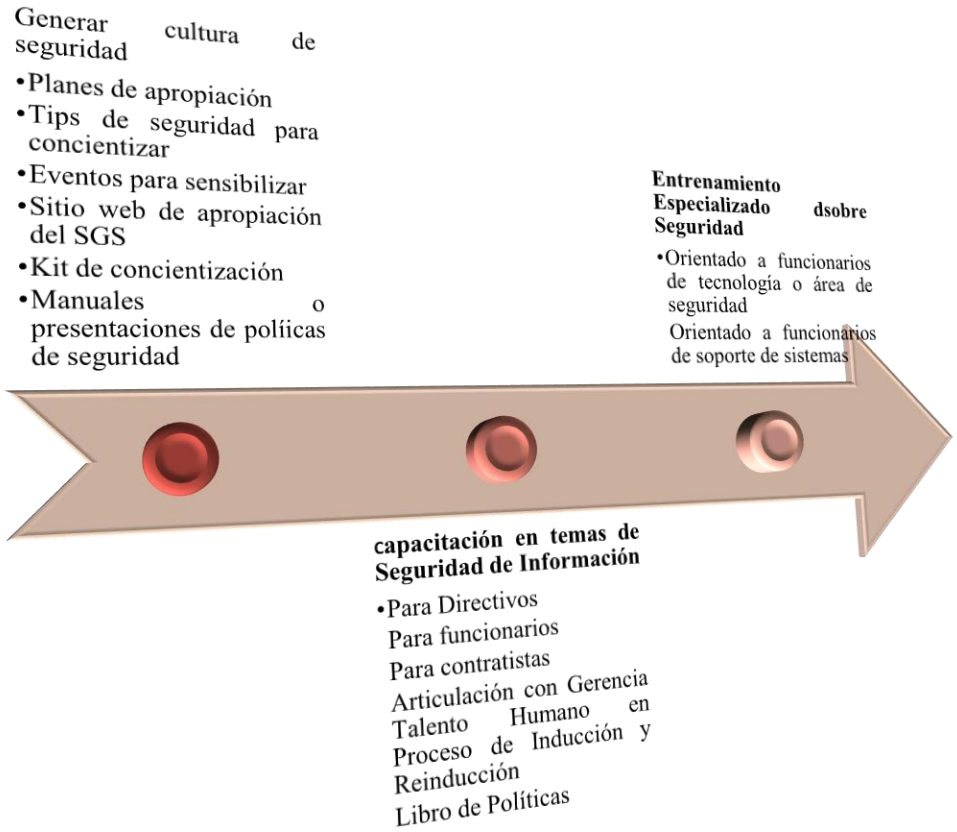
En este tema de cultura se ha venido realizando desde el segundo semestre de 2017 tips de sensibilización y actividades para afianzar la cultura de seguridad de la información a los servidores públicos de la Entidad, como los son la semana de seguridad, el mes de la ciberseguridad, ferias de sensibilización en temas relacionados con la seguridad de la información. Se ha avanzado en generar documentos o tips que permitan al funcionario apropiarse de la seguridad de la información como responsabilidad de todos.

Se realiza socialización de políticas de seguridad a los funcionarios de la CGR y Gerencias Departamentales para que conocieran los lineamientos de la entidad en cuanto a seguridad de la información.

Existen presentaciones e insumos a actualizar para fortalecer los procesos de inducción y reinducción desde la Gerencia del Talento Humano.

La cultura de seguridad de la información se debe trabajar articuladamente entre USATI de la Información, a Gerencia del talento Humano, el Centro de Estudios Fiscales para genera nuevos procesos que incluyan temáticas de seguridad de información.

Figura 39. Ruta para el componente de cultura



Socios Estratégicos: Despacho Vice contralor USATI, Centro de Estudios Fiscales CEF, Oficina de Comunicaciones, Control Interno

Fuente: Elaboración propia

5. Operación

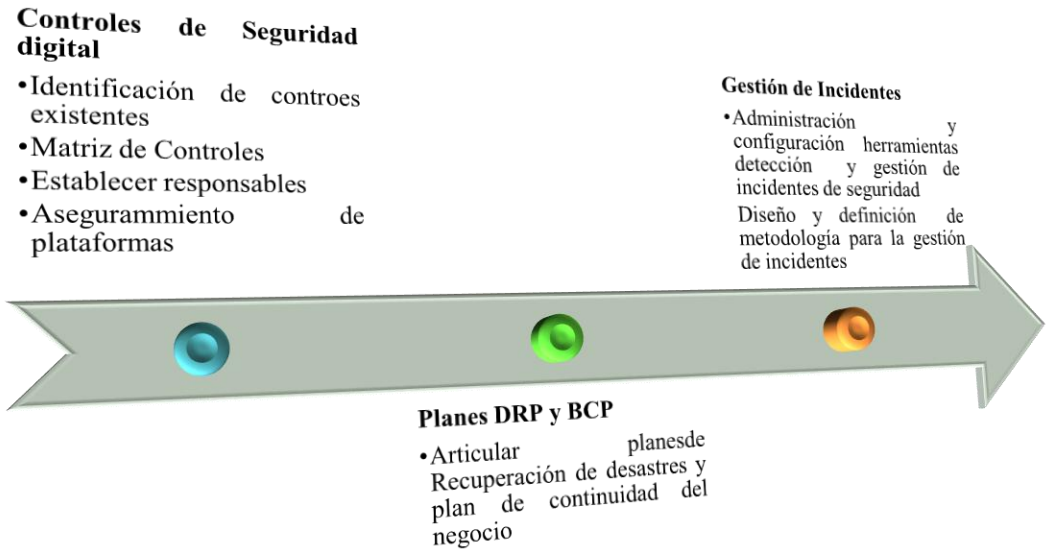
Enfatizar en los controles de tecnologías de seguridad, para el aseguramiento y protección de la información y así responder las expectativas de la alta gerencia.

En este tema existe un buen avance desde la Oficina de Sistemas en cuanto a herramientas y plataformas de seguridad informática como son generación de controles como firewall, dlp, antivirus, entre otros, los cuales se han ido identificando en una matriz de controles; en unión con la Oficina de Sistemas.

También se han adquirido plataformas de correlación de datos y firewall de aplicaciones que dan mayor visibilidad de posibles incidentes de seguridad de la información.

La Oficina de sistemas contrata la implementación del DRP Plan de recuperación de desastres, contratación que se está iniciando, así como se empieza a incursionar en BCP Plan de continuidad del negocio.

Figura 40. Ruta para el componente de Operaciones



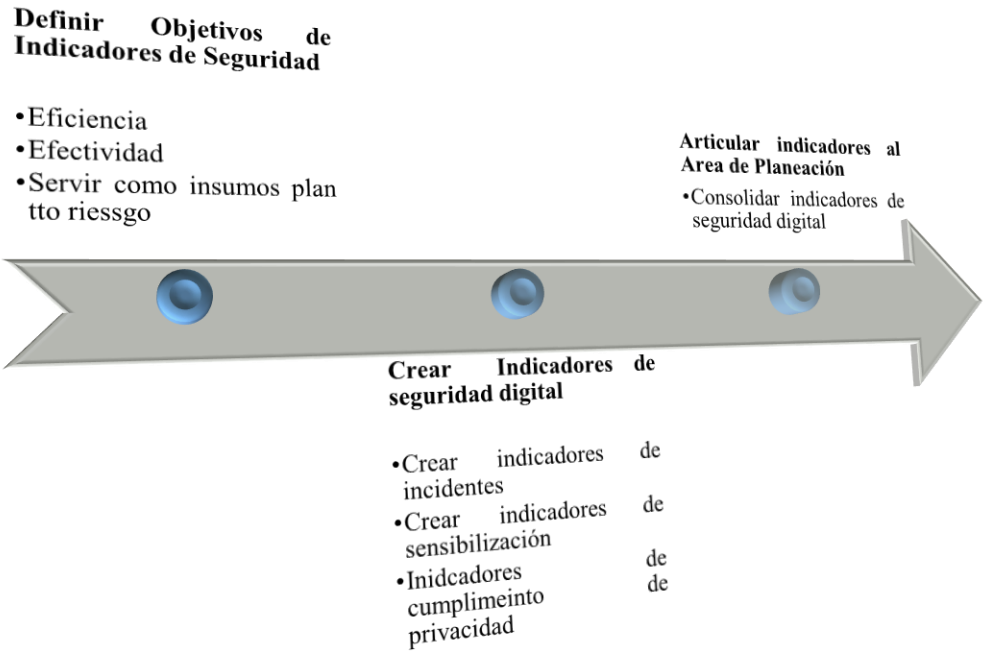
Socios Estratégicos: Oficina de Sistemas e Informática, USATI, Gerencias Departamentales

6. Medición

Definir indicadores que permitan medir la efectividad, eficacia y eficiencia de la Seguridad digital en la CGR.

En ese momento indicadores de seguridad de la información no se tienen, tan solo se rinde un indicador del número de incidentes presentados por mes. Este es una dimensión a trabajar.

Figura 41. Ruta para el componente de Mediciones



Socios Estratégicos: Oficina de Planeación (Administrador de indicadores de la Entidad) –USATI (definir indicadores de seguridad digital)

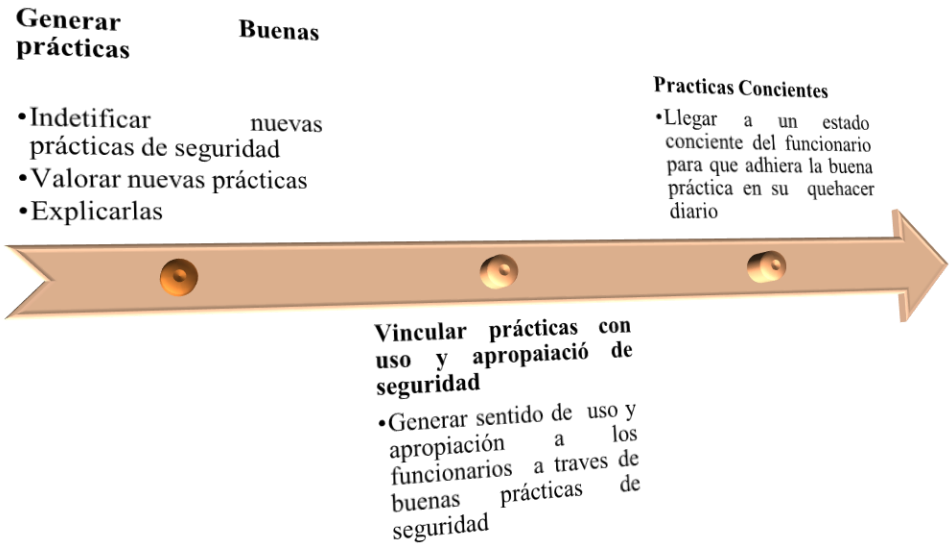
Fuente: Elaboración propia

7. Prácticas

Interiorizar y afianzar a nivel de Entidad buenas prácticas en el uso responsable de la seguridad de la información.

En este componente aunque los funcionarios dicen tener prácticas de seguridad de la información, éstas no se realizan frecuentemente y en forma consciente solo se hacen en algunas oportunidades o porque se vigila que se cumpla.

Figura 42. Ruta para el componente de Prácticas



Socios Estratégicos: Oficina de Sistemas e Informática, USATI, Gerencias Departamentales, Dependencias de la CGR

Fuente: Elaboración propia

Matriz de RACI de seguridad de la información propuesta para la CGR

En la siguiente tabla se propone una matriz RACI para las responsabilidades de la seguridad de l información en la CGR.

Tabla 19. Matriz RACI Seguridad de la Información para la CGR

MATRIZ RACI SEGURIDAD INFORMACION CGR												
	DESPACHO CONTRALOR - CEO	USATI - CSO	DIRECTOR USATI / CISO	COMITÉ DE SEGURIDAD	OFICINA DE COMUNICACIONES	OFICINA DE PLANEACION	GESTION DE INCIDENTES	SEGURIDAD INFORMATICA - CIO	OFICINA DE SISTEMAS E INFORMATICA - CIO	OFICINA JURIDICA CLO	OFICINA DE CONTROL INTERNO	LABORATORIO FORENSE
POLITICAS Y PRINCIPOS												
Definir la Estrategia de Seguridad de la Información	R	A	I	C	-	I	C	C	C	-	-	I
Aprobar la Estratégia de Seguridad de la Información	A	A	R	R	-	C I	I	I	I	I	I	I
Definir las Políticas de Seguridad de la Información	R	A	A	C	-	I	-	C	C	C	-	C
Aprobar las Políticas de Seguridad de la Información	R	A	R	R	I	C I	-	I	I	I	I	I
Definir los Procedimientos de Seguridad de la Información	R	C	A	C	C I	C	C	C	C	C	C	C
Aprobar los Procedimientos de Seguridad de la Información	I	A	R	C	I	C	I	I	I	I	I	I
Actualización de Políticas de Seguridad de la Información	I	A	A	C	-	C	C	-	C	-	-	C
Actualización de los Procedimientos de Seguridad de la Información	I	A	A	C	-	C	C	-	C	-	-	C
Gestionar la Mejora Continua del SGSI	C	I	I	-	-	R	-	-	I	-	-	I
Apoyar la mejora continua del SGSI	C	-	-	-	-	R	-	-	-	-	-	I
Definir Roles y Responsabilidades de Seguridad de la Información	C	I	A	R	I	C	C	C	C	-	-	I
Definir la Continuidad de la Seguridad de la Información	R	I	A	A	-	I	-	-	R	-	-	I

MATRIZ RACI SEGURIDAD INFORMACION CGR													
	DESPACHO CONTRALOR - CEO	USATI - CSO	DIRECTOR USATI / CISO	COMITÉ DE SEGURIDAD	OFICINA DE COMUNICACIONES	OFICINA DE PLANEACION	GESTION DE INCIDENTES	SEGURIDAD INFORMATICA - CIO	OFICINA DE SISTEMAS E INFORMATICA - CIO	OFICINA JURIDICA CLO	OFICINA DE CONTROL INTERNO	LABORATORIO FORENSE
Gestionar Partes Interesadas en Seguridad de la Información	C	I	I	A	-	-	-	-	I	-	-	I
Gestionar Presupuesto de Seguridad de la Información	R	A	R	A	-	-	-	C	C	-	-	C
Gerenciar Proyectos de Seguridad de la Información	I	R	I	A	-	-	C	-	R	-	-	R
Contactar Autoridades Relacionadas con Seguridad de la Información	C	R	I	A	I	-	-	-	I	-	-	I
Contactar Grupos de Interes de Seguridad de la Información	C	R	I	A	I	-	-	C	R	-	-	C
Apoyar la gestion de Partes Interesadas en Seguridad de la Información	I	R	-	A	C	-	-	-	-	-	-	R
CUMPLIMIENTO												
Identificar los Requisitos Legales y Contractuales de Seguridad de la Información	R	I	I	A	C	I	-	I	I	R A	I	I
Apoyar la identificación de los Requisitos Legales y Contractuales de Seguridad de la Información	R	-	-	A	C	I	-	-	-	R A	-	C
RIESGOS												
Definir la Estratégia de Riesgos de Seguridad de la Información	C	-	C	A	C I	R	C	-	-	-	-	-
Aprobar la Estratégia de Riesgos de Seguridad de la Información	R	A	R	A	I	C I	I	I	I	I	I	I
Definir la Estratégia de Identificación de Activos de Información	C	-	A	A	C I	R	-	-	-	-	-	-
Aprobar la Estratégia de Identificación de Activos de Información	R	A	R	A	I	C I	-	I	I	I	I	I
Definir los Niveles de Clasificación de Información	C	-	A	-	C I	R	C	-	-	C	-	-
Aprobar los Niveles de Clasificación de Información	C	A	C	-	I	R	I	I	I	I	I	I
Definir los Líneamientos de Etiquetado de Información	R	-	A	-	-	R	C	-	-	-	-	-
Coordinar el Analisis de Riesgos de Seguridad de la Información	-	I	I	-	R	A	-	-	I	-	-	I
Aprobar los Líneamientos de Etiquetado de	I	A	C	A	I	R	I	I	I	I	I	I

MATRIZ RACI SEGURIDAD INFORMACION CGR												
	DESPACHO CONTRALOR - CEO	USATI - CSO	DIRECTOR USATI / CISO	COMITÉ DE SEGURIDAD	OFICINA DE COMUNICACIONES	OFICINA DE PLANEACION	GESTION DE INCIDENTES	SEGURIDAD INFORMATICA - CIO	OFICINA DE SISTEMAS E INFORMATICA - CIO	OFICINA JURIDICA CLO	OFICINA DE CONTROL INTERNO	LABORATORIO FORENSE
Información												
Realizar Seguimiento a Plan de Tratamiento de Riesgos de Seguridad de la Información	-	I	A	I	R	I	-	-	-	-	-	C
Apoyar la implementación del Plan de Tratamiento de Riesgos de Seguridad de la Información	-	-	-	-	C	C	-	-	-	-	-	R
Acompañar la Ejecución de Auditorías de Seguridad de la Información	-	I	I	-	R	A	-	-	-	-	I	R
Coordinar Auditorias de Seguridad de la Información	-	I	A	I	R	C	-	I	I	I	I	I
Coordinar la Implementación de Acciones de Mejora	-	I	I	I	R	A	-	I	I	-	R	I
Apoyar la implementación de acciones de mejora	-	-	-	-	C	C	-	-	-	-	R	R
Coordinar la Subsanación de No Conformidades	-	I	I	I	R	A	-	I	I	I	C	I
Apoyar la Subsanación de No Conformidades	-	-	-	-	C	C	-	-	-	-	R	R
Verificar la Implentación de Controles de Seguridad de la Información	-	I	I	-	C	A	-	C	C	-	R	R
Apoyar la verificación la Implentación de Controles de Seguridad de la Información	-	-	-	-	C	C	-	-	-	-	R	R
Verificar la Funcionalidad de los Controles de Seguridad de la Información	-	I	I	-	C	A	-	-	-	-	R	R
Apoyar el análisis de riesgos de seguridad de la información	-	-	-	-	C	C	-	-	-	-	R	R
Ejecutar Auditorías de Seguridad	-	I	I	I	A	C	-	I	I	I	R	I
CULTURA												
Definir los Programas de Sensibilización de Seguridad de la Información	R	-	A	-	R	R	C	-	C	-	-	C
Aprobar los Programas de Sensibilización de Seguridad de la Información	R	A	C	C	C I	R	I	-	-	-	-	-
Apoyar el seguimiento al cumplimiento de las políticas de seguridad de la información	I	-	-	-	C I	C I	-	-	-	-	-	R
Realizar Capacitaciones Técnicas de Seguridad de la Información	I	R	A	-	C	C	I	-	C	-	-	-

MATRIZ RACI SEGURIDAD INFORMACION CGR													
	DESPACHO CONTRALOR - CEO	USATI - CSO	DIRECTOR USATI / CISO	COMITÉ DE SEGURIDAD	OFICINA DE COMUNICACIONES	OFICINA DE PLANEACION	GESTION DE INCIDENTES	SEGURIDAD INFORMATICA - CIO	OFICINA DE SISTEMAS E INFORMATICA - CIO	OFICINA JURIDICA CLO	OFICINA DE CONTROL INTERNO	LABORATORIO FORENSE
Ejecutar Plan de Toma de Conciencia de Seguridad de la Información	I	C	A	-	R	I	-	-	-	-	-	-
Apoyar las campañas de sensibilización y toma de conciencia en seguridad de la información	I	C	-	C	R	C	-	-	-	-	-	R
OPERACIÓN												
Analizar Requerimientos de Seguridad en Proyectos	I	-	-	-	C	C	-	-	-	-	-	R
Participár en la identificación de los requerimientos de seguridad de los proyectos	I	I	I	-	R	A	-	-	I	-	-	I
Definir la Arquitectura de Seguridad de la Información	I	I	C	A	I	C	R	C	-	-	-	-
Implementar la Arquitectura de Seguridad de la Información	I	I	-	I	R	A	R	I	-	-	-	-
Coordinar la Gestión de Incidentes de Seguridad de la Información	I	I	A	-	R	C I	-	C	C	-	-	I
Apoyar la gestión de incidentes de seguridad de la información	I	-	-	-	C	C I	-	-	-	-	-	R
Apoyar la gestión de incidentes de seguridad de la información	-	-	-	-	C	C	-	-	-	-	-	R
Investigar Incidentes de Seguridad de la Información	-	-	-	-	R	A	-	R	R	-	-	-
Responder Incidentes de Seguridad de la Información	-	I	I	-	R	A	-	R	R	-	-	-
Coordinar el Análisis de Vulnerabilidades de Seguridad de la Información	-	C	A	C	R	C	-	C	-	-	-	-
Realizar Análisis de Vulnerabilidades de Seguridad	-	I	I	I	A	C	-	-	-	-	-	-
Coordinar Plan de Mitigación de Vulnerabilidades de Seguridad	-	I	I	I	R	A	-	C	-	-	-	-
Coordinar Pruebas de Ingeniería Social		I	A	-	R	C	-	-	-	-	-	-
Instalar Herramientas de Seguridad de la Información	-	I	C	A	C	C	-	R	I	-	-	I
Priorizar Tareas del Equipo de Seguridad de la Información	-	I	A	-	R	R	-	-	C	-	-	-
Implementar Controles de Seguridad de la Información	-	C	C	I	C	A	-	C	R	-	I	I
Coordinar la Revisión de Código Seguro	-	I	A	C	R	C	-	-	-	-	-	-

MATRIZ RACI SEGURIDAD INFORMACION CGR												
	DESPACHO CONTRALOR - CEO	USATI - CSO	DIRECTOR USATI / CISO	COMITÉ DE SEGURIDAD	OFICINA DE COMUNICACIONES	OFICINA DE PLANEACION	GESTION DE INCIDENTES	SEGURIDAD INFORMATICA - CIO	OFICINA DE SISTEMAS E INFORMATICA - CIO	OFICINA JURIDICA CLO	OFICINA DE CONTROL INTERNO	LABORATORIO FORENSE
Monitorear las Herramientas de Seguridad de la Información	-	I	I	I	C	A	-	I	-	-	-	-
Configurar las Herramientas de Seguridad de la Información	-	I	I	I	C	A	-	R	I	-	-	-
Apoyar la implementación de los controles de seguridad de la información en las áreas	-	-	-	-	C	C	-	-	-	-	-	R
Generar Informes de Gestión de Seguridad de la Información	-	I	-	-	R	A	-	-	C	-	-	-
Generar Informes Técnicos de Seguridad de la Información	-	I	I	I	A	I	-	C	-	-	-	-
Analizar Cambios de Seguridad de la Información	-	I	I	I	A	C	C	C	R	-	-	C
Gestionar Cambios de Seguridad de la Información	-	I	A	I	R	R	-	-	-	-	-	I
Apoyar la gestión de cambios de seguridad de la información	-	-	-	-	C	C	-	-	-	-	-	R
Documentar Anexos Técnicos Relacionados con Seguridad de la Información	-	I	I	I	R	A	-	C	C	C	-	C
Coordinar el Levantamiento del Inventario de Activos de Seguridad de la Información	-	I	I	-	R	A	-	-	I	-	-	I
Apoyar la actualización del Inventario de Activos de Información	-	-	-	-	C	C	-	-	-	-	-	R
Revisar Anexos Técnicos Relacionados con Seguridad de la Información	-	I	A	-	C	R	-	-	-	-	-	-
Gestionar la Continuidad de la Seguridad de la Información	C											
Acompañar a los líderes de proceso en la actualización de documentación de seguridad de la información	-	-	-	-	C	C	-	-	-	-	-	R
Atender las solicitudes del equipo de seguridad de la información	-	-	-	-	C	C	-	-	-	-	-	R
MEDICION		C	A	-	C	R	C	-	C	-	-	I
Definir Indicadores de Seguridad de la Información	R	R	A	I	-	C	-	-	I	-	-	I
Gestionar Indicadores de Seguridad de la Información	C	R	-	-	C	C	-	-	-	-	-	R

MATRIZ RACI SEGURIDAD INFORMACION CGR	DESPACHO CONTRALOR - CEO	USATI - CSO	DIRECTOR USATI / CISO	COMITÉ DE SEGURIDAD	OFICINA DE COMUNICACIONES	OFICINA DE PLANEACION	GESTION DE INCIDENTES	SEGURIDAD INFORMATICA - CIO	OFICINA DE SISTEMAS E INFORMATICA - CIO	OFICINA JURIDICA CLO	OFICINA DE CONTROL INTERNO	LABORATORIO FORENSE
Apoyar el seguimiento a medición de indicadores	C	C				R						
PRACTICAS		A	R	-	-	-	-	-	-	-	-	-
Supervisar la Gestión del Equipo de Seguridad de la Información	-	R	R	-	C	C	-	-	-	-	-	R
Apoyar la gestión a los procedimientos de seguridad de la información	-	A	I	C	I	C	R	C	C	-	-	-
Documentar Requisitos de Arquitectura Segura	-	A	I	A	R	C	C	R	-	-	-	-
Documentar Protocolos de Arquitectura Segura	-	A	I	A	R	C	C	R	-	-	-	-
Documentar Procedimientos de Arquitectura Segura	-	A	I	A	I	C	C	R	-	-	-	-
Documentar Estandares de Arquitectura Segura	-	A	A	-	R	C	-	C	-	-	-	-
Coordinación de Análisis Forense de Seguridad de la Información	-	A	C	C	C	C	C	C	R	-	-	R
Analizar Nuevas Tecnológias y Sistemas de Información	-	C	A	C	C	R	-	C	C	C	-	C

Fuente: Elaboración propia

Tabla 20. Descripción de cada Rol

Rol			Descripción
R	*Responsible*	Responsable	Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea
A	*Accountable*	Aprobador	Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A) de que la tarea sea ejecutada por su Responsable (R).
C	*Consulted*	Consultado	Este rol posee alguna información o capacidad necesaria para realizar la tarea.

Rol			Descripción
I	*Informed*	Informado	Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea. A diferencia del consultado (C), la comunicación es unidireccional.

Fuente: Elaboración propia

Conclusiones

- El gobierno de seguridad de la información propuesto, recomienda a partir de la estrategia y con apoyo de la alta gerencia, fortalecer la capacidad de dirigir la seguridad de la información de la entidad, alineada a los objetivos misionales identificados.
- En el modelo propuesto se definen 7 componentes, los cuales son: Principios, cumplimiento, riesgos, cultura, operaciones, indicadores y buenas prácticas, que delinean la postura de seguridad de la información de la Contraloría General de la República, orientada al arquetipo de Gobierno, operaciones y aspectos legales en razón a que por ser Entidad del Estado está enmarcada en cumplimiento.
- Se identifica el nivel de madurez de la CGR en relación con las dimensiones de seguridad de la información, con un 2,7, lo que corresponde en la escala de evaluación del instrumento aplicado a que es una Entidad: "*donde se reconoce que la postura de seguridad de la información es necesaria para aportar al negocio. Sin embargo no existen sino intentos, o iniciativas por separado; posiblemente algunos esfuerzos y controles base.",* como resultado de esto se proponen algunas rutas para madurar aún más a partir del modelo propuesto.
- El modelo de Gobierno planteado esta dado por 7 dimensiones donde 4 de ellas corresponde a gobierno éstas son: cultura, Riesgos, cumplimiento y Principios son la sombrilla para la gestión de la seguridad de la información que cubre las otras 3

dimensiones Operación, Medición y Prácticas que se encargan de ejecutar lo estipulado desde el Gobierno.

- Los componentes de seguridad de la información son reconocidos y evaluados desde el instrumento permitiendo obtener una visión de rutas a seguir, para lograr madurar cada uno de los componentes del modelo de seguridad de la información que se plantea y lograr solucionar la problemática planteada para la asignación de roles y responsabilidades, gestión de riesgos e incidentes de seguridad de la información y que la entidad tome las buenas prácticas para optimizar su seguridad de la información.
- Existen avances en algunos componentes lo que permite articular y delinear las rutas a seguir como recomendación desde el modelo propuesto.

Glosario Términos Técnicos

Término	Definición
Activo de información	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).(MINTIC, 2017)
Amenaza	Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.(MINTIC, 2017)
Análisis de Riesgo	Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001. (MINTIC, 2017)
Antivirus	Categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles. (MINTIC, 2017)
Botnet	Computador o dispositivo de comunicación zombi los cuales son equipos controlados a distancia. (Instituto Nacional de Ciberseguridad INCIBE, 2016)
Ciberdefensa	Capacidad del Estado para prevenir y contrarrestar toda amenaza o

	incidente de naturaleza cibernética que afecte la soberanía nacional. (Departamento Nacional de Planeación, 2011)
Ciberespacio	Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización de la electrónica, la informática y la cibernética. (Departamento Nacional de Planeación, 2011. p.3.)
Ciberseguridad	Condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio. (Ona Systems, 2018) Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (Departamento Nacional de Planeación, 2011)
Diferencia Seguridad Informática y de Información	La seguridad informática se describe como la distinción táctica y operacional de la seguridad, mientras que la seguridad de la información es la línea estratégica de la seguridad. (ISOTools Excellence, 2017)
Gusano	Gusano informático es un código malicioso capaz de multiplicarse en varios computadores, se propaga sin intervención humana. (Instituto Nacional de Ciberseguridad INCIBE, 2016)
Host **Malware**	Se refiere a cualquier computador o dispositivo. (Instituto Nacional de Ciberseguridad INCIBE, 2016) Programa con código informático malicioso.

Política de Seguridad	Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información. (INCIBE, 2017)
Seguridad	Es un proceso multidimensional que debe tenerse en cuenta en la definición, en la gestión y en la reingeniería de las empresas y procesos del negocio. (Areitio Bertolín, 2008)
Seguridad de la Información	Medidas preventivas y de reacción del individuo, la organización y las tecnologías, para proteger la información; buscando mantener en esta la confidencialidad, la autenticidad e Integridad. (Universidad Libre de Colombia, 2018). La seguridad de la información se encarga de regular y establecer las pautas a seguir para la protección de la información. (ISOTools Excellence, 2017)
Seguridad Digital	Es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. (Presidencia de la República de Perú, 2018) Este término surge en Colombia a raíz del creciente uso del entorno

	digital para desarrollar actividades económicas y sociales, el cual acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente, el no hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno. (Departamento Nacional de Planeación, 2016)
Seguridad Informática	Protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene, implementa medidas técnicas que preservaran las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa. (ISOTools Excellence, 2017)
Seguridad Integral	Este concepto para la Contraloría General de la República –CGR corresponde a la gestión de la seguridad de personas, bienes e información en la Entidad.
Virus:	Tiene como objetivo alterar el funcionamiento de cualquier computador, solo se propaga con intervención humana. (Instituto Nacional de Ciberseguridad INCIBE, 2016)

Anexos

Eventos y amenazas de incidentes de seguridad de la información en la CGR

Esta sección corresponde a la ampliación de la problemática planteada en el capítulo 1, relacionada con los eventos y amenazas de incidentes de seguridad de la información que se han venido presentando en la CGR.

La Entidad cuenta con un Sistema de monitorización de eventos de seguridad (SIEM) el cual es:

> Una herramienta capaz de monitorizar el estado en cuanto a seguridad de una organización, debe estar perfectamente integrada con todos los sistemas ya que debe entender el comportamiento de toda la infraestructura de Tecnologías de la Información y las Comunicaciones (TIC). Mediante la recopilación de eventos de login, acceso a bases de datos, logs de firewall, proxy, IPS, logs de aplicaciones, etc, un SIEM es capaz de monitorizar y predecir el comportamiento futuro de la plataforma de Tecnologías de la Información y las Comunicaciones (TIC) de tal manera que ante una conducta inusual de la plataforma puede generar una alerta y/o realizar una acción determinada (Ona System, 2018)

Las siguientes gráficas corresponden al recuento de eventos de amenazas y riesgos que se materializaron en la CGR según el monitoreo realizado por el Sistema de monitorización de

eventos de seguridad (SIEM) del fabricante McAfee administrado por la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI).

Para el entendimiento de la siguiente tabla tener en cuenta estos conceptos basados de (Instituto Nacional de Ciberseguridad INCIBE, 2016):

Gusano: Gusano informático es un código malicioso capaz de multiplicarse en varios computadores, se propaga sin intervención humana.

Botnet: Computador o dispositivo de comunicación zombi los cuales son equipos controlados a distancia.

Host: Se refiere a cualquier computador o dispositivo.

Virus: Tiene como objetivo alterar el funcionamiento de cualquier computador, solo se propaga con intervención humana.

Malware: programa con código informático malicioso.

Como se observa en las gráficas, los eventos de ataques presentados en la Entidad, mes a mes durante el primer cuatrimestre del año 2019, indican que han venido aumentando, de acuerdo al reporte dado por el software SIEM, el cual se compara en la tabla 1 Comparativo de ataques presentados en la CGR, 1-cuatrimestre de 2019, y cuya explicación es la siguiente:

1. **Malware:** se observa que de 106 eventos presentados en enero, se incrementan a 118, baja en marzo a 113, pero suben nuevamente a 128, por lo que se observa que la presencia de malware en diferentes tipos, como gusano, malware o virus, se han venido presentando en

la CGR, siendo más predominante la aparición de gusanos, después malware y con mayor ocurrencia los virus, lo cual deja ver que de no controlarse, tiende a estar en riesgo la información que maneja la Entidad; por lo anterior, es necesario generar estrategias que permitan afrontar este problema.

2. **Eventos Subtipo (Event Subtype):** En esta categoría se observa eventos de fallo, bloqueo y acciones que después de analizadas son correctas, presentándose con mayor frecuencia los fallos, los cuales a enero fueron 67, Febrero 76 marzo 78 y incrementando en abril a 109, incrementando bastante su porcentaje y los bloqueos, por el contrario disminuyen de 33 presentados en enero, a 19 eventos que se dan en el mes de abril de 2019.

Tabla 21. Comparativo de ataques presentados en la CGR, 1-cuatrimestre de 2019

Ataque	Descripción Tipos	Enero	Febrero	Marzo	Abril
1. Malware	Gusano	73	85	51	73
	Malware	22	22	35	36
	Virus	11	11	27	19
	Total Tipos de malware encontrados	106	118	113	128
2. Eventos Subtipo (Event Subtype)	Fallo	67	76	78	109
	Bloquear	33	33	31	19
	Correcto	6	9	4	0
	Total Eventos no seguros presentados	106	118	113	128
3. Mensajes	Attack - posible conficker work	73	85	35	19

de regla	activity				
de Malware	Attack – malware sent from internal host	11	11	25	36
(Malware rule message)	Malware increasing number of malware events occurring on internal hosts	11	11	26	36
	File is infected	10	11	27	32
	Botnet Command and Control (C&C) Comunication	1	0	0	4
	Attack malware activity on local host	0	0	0	1
	Mensaje de regla de malware	106	118	113	128

Fuente: Elaboración propia. Datos tomados de reporte del SIEM.

3. **Mensajes de regla de Malware (Malware rule message):** El ataque con mayor frecuencia es Attack - posible conficker work activity, este virus lo que hace en los computadores según (Panda security, 2018) es:

> Reduce considerablemente el nivel de protección del ordenador, ya que impide que, tanto el usuario como el ordenador, puedan conectarse a numerosas páginas web relacionadas con programas antivirus.
>
> Por otra, utiliza contraseñas débiles para acceder a las cuentas de usuario del ordenador afectado y modificar sus políticas de seguridad.

El otro con su punto máximo en 85 eventos durante febrero de 2019 y disminuyendo a 19 en Abril, es el Attack – malware sent from internal host, este es un evento que según reporta Mcaffe es una regla de correlación que configurada previamente, permite establecer que un malware ha sido enviado desde un dispositivo o computador interno.

También, se observa que el reporte de archivos infectados (File is infected) incrementa, de 10 casos presentados en Enero a 32 presentados en Abril de 2019.

En cuanto a los Botnet (equipos controlados a distancia) Command and Control (C&C) Comunication, que en enero de 2019 presentaron 1 y febrero y marzo 0, en abril nuevamente se comprometen computadores, teniendo 4 reportes.

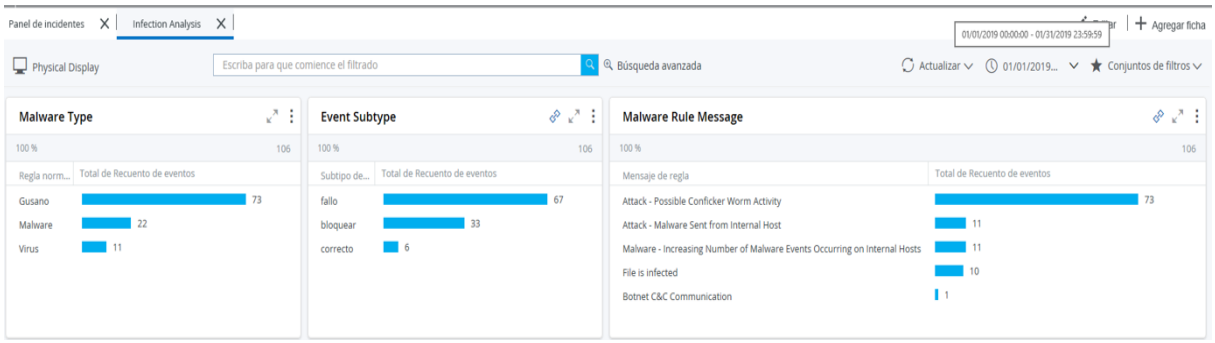
Y por último, en abril aparece un reporte en la regla de correlación de attack malware activity on local host, que indica que un computador tienen actividad de malware de forma local, es decir, el computador tiene el código malware en sus archivos.

Cabe anotar, que algunos de estos eventos fueron bloqueados, o limpiados por la solución antivirus de la Entidad y otros subsanados internamente a través del área de soporte de la CGR, pero algunos siguen apareciendo sin poder tener una solución efectiva.

A continuación, se muestran las gráficas 3, 4, 5 y 6 que sustentan la explicación dada anteriormente en la tabla 16 comparativo de ataques presentados en la CGR, 1-cuatrimestre de

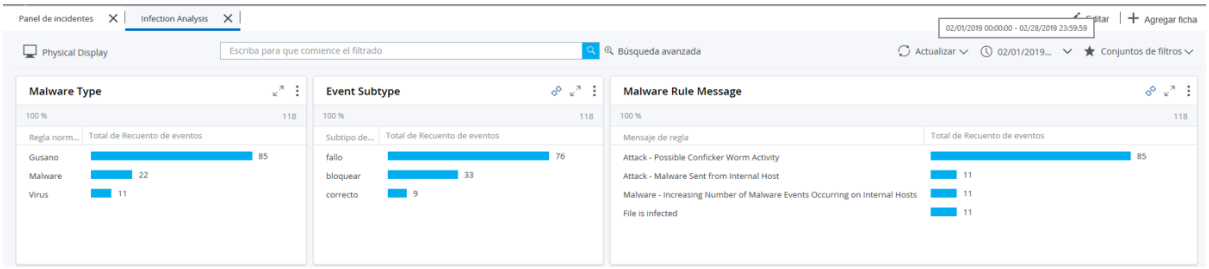
2019, es importante aclarar que estás fueron tomadas del reporte que realiza mes a mes el Sistema de monitorización de eventos de seguridad (SIEM) McAfee, administrado por la CGR.

Gráfica 3. Reporte de ataques - MES DE ENERO DE 2019



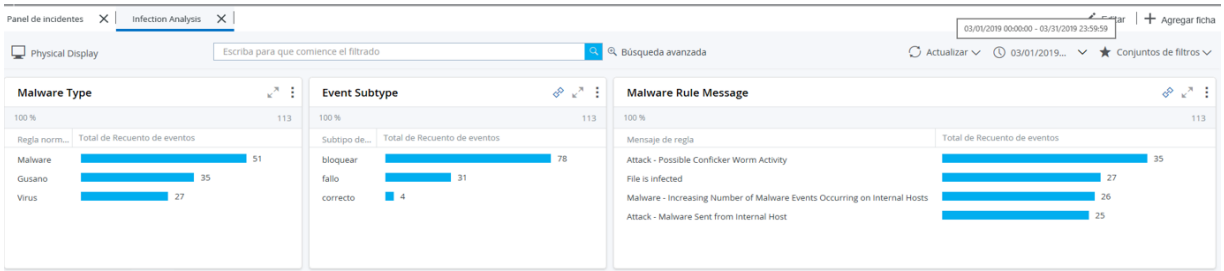
Fuente: Datos tomados de reporte del SIEM.

Gráfica 4. Reporte de ataques - MES DE FEBRERO DE 2019



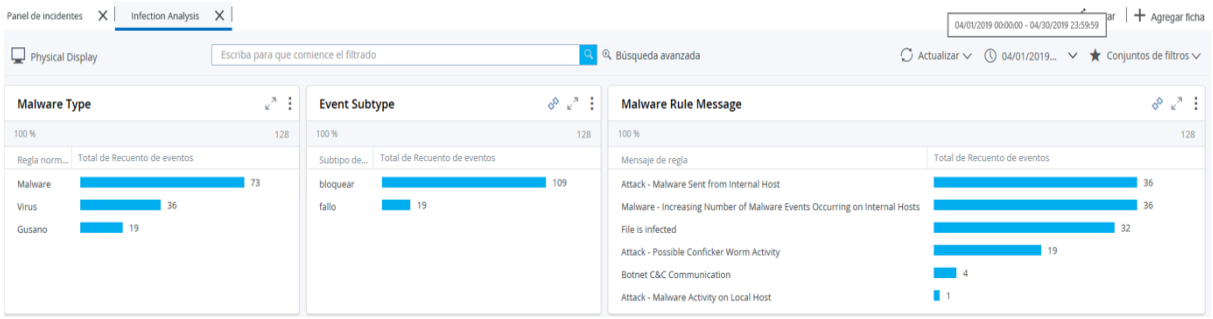
Fuente: Datos tomados de reporte del SIEM.

Gráfica 5. Reporte de ataques - MES DE MARZO DE 2019



Fuente: Datos tomados de reporte del SIEM.

Gráfica 6. Reporte de ataques - MES DE ABRIL DE 2019



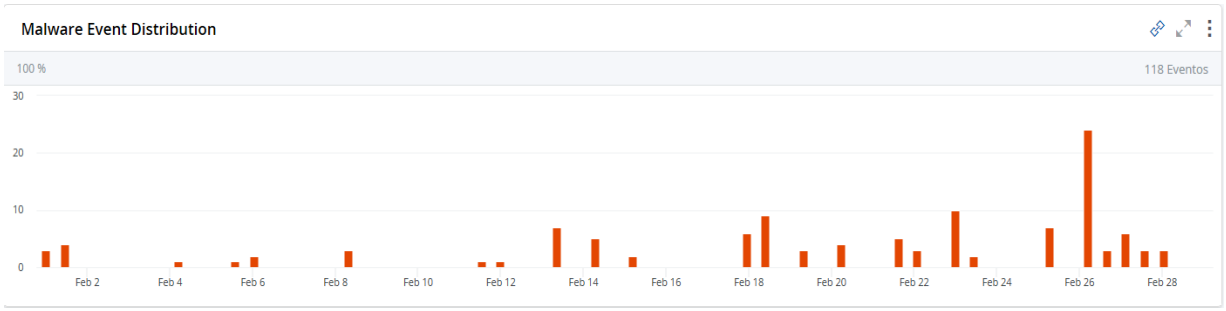
Fuente: Datos tomados de reporte del SIEM.

Gráfica 7. Eventos de distribución de Malware – Enero 2019

Fuente: Datos tomados de reporte del SIEM.

La gráfica 7, muestra el 8, el 18 y el 30 de enero, se recibió una carga de distribución de malware mayor lo que evidencia que los atacantes se concentraron en distribuir malware en esas fechas del mes de enero de 2019, y se evidencia el pico más alto el 9 de enero de 2019.

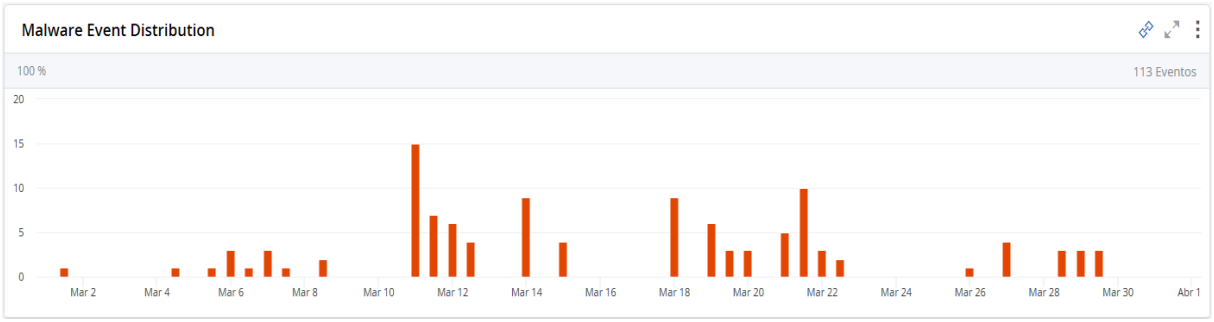
Gráfica 8. Eventos de distribución de Malware –Febrero 2019



Fuente: Datos tomados de reporte del SIEM.

La gráfica 8, muestra el 26, el 18 y el 14 de enero, se recibió una carga de distribución de malware mayor lo que evidencia que los atacantes se concentraron en distribuir malware en esas fechas del mes de febrero de 2019, y se evidencia el pico más alto el 26 de febrero de 2019.

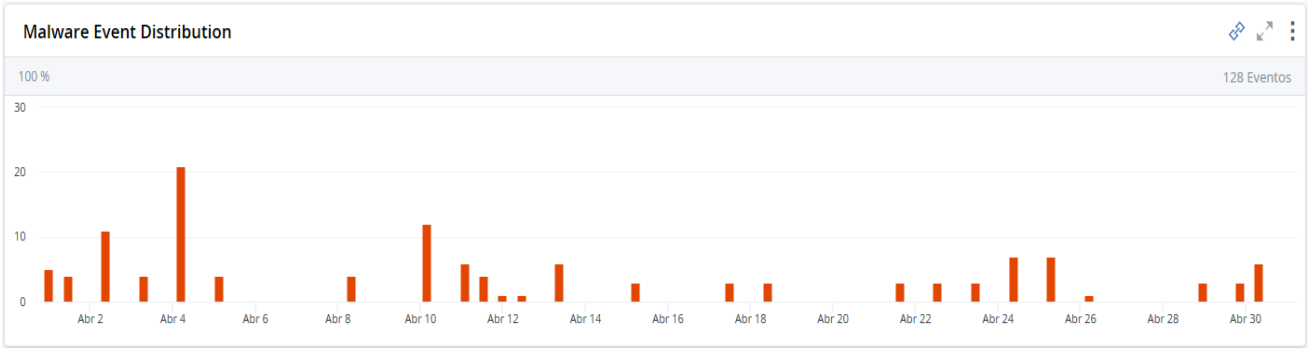
Gráfica 9. Eventos de distribución de Malware –Marzo 2019



Fuente: Datos tomados de reporte del SIEM.

La gráfica 9, muestra que el 11, 14, 18 y 22 de marzo, se recibió una carga de distribución de malware mayor, lo que evidencia que los atacantes se concentraron en distribuir malware en esas fechas del mes de marzo de 2019 y se evidencia el pico más alto el 11 de marzo de 2019.

Gráfica 10. Eventos de distribución de Malware –Abril 2019

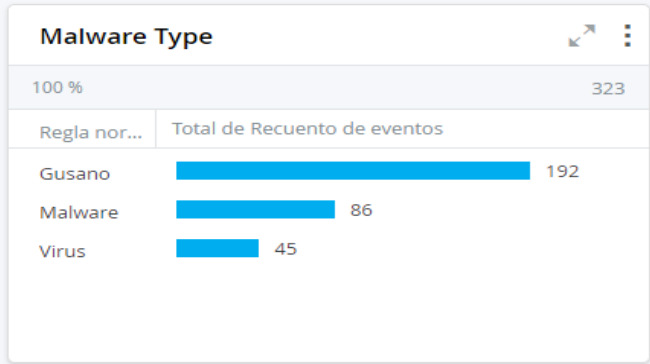
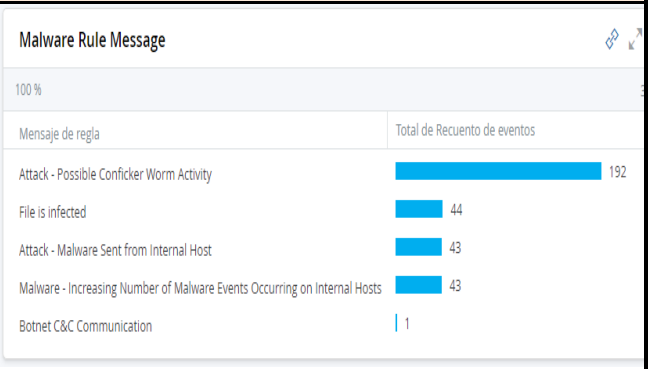


Fuente: Datos tomados de reporte del SIEM.

La gráfica 10, muestra el 4 el 10, 14, 24 y 30 de abril, se recibió una carga de distribución de malware mayor lo que evidencia que los atacantes se concentraron en distribuir malware en esas fechas del mes de febrero de 2019, y se evidencia el pico más alto el 4 de abril de 2019.

También se muestra los tipos de eventos y amenazas consolidadas del primer trimestre de 2019 para tener un panorama global de los ataques explicados anteriormente.

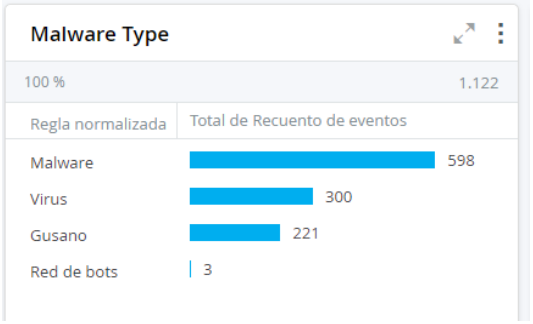
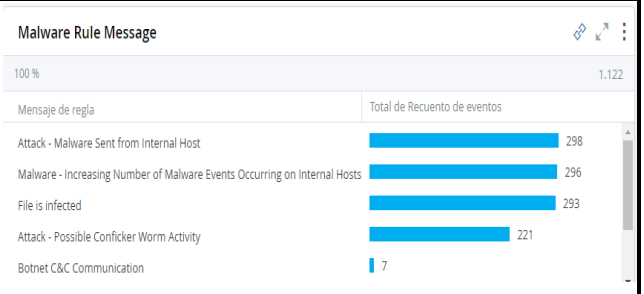
Tabla 22. Amenazas identificadas eventos de seguridad. Consolidado primer trimestre de 2019.

TIPOS DE EVENTOS DE AMENAZAS –Primer Trimestre 1 Enero a 20 Marzo de 2019	
	
Gráfica 11.Tipos de Malware	Gráfica 12. Eventos de mensaje de Regla de

	Malware
En esta figura se observa que los tres tipos de amenazas que más han tenido recuento de eventos son el gusano con 192, después el malware con 86 y el virus con 45 recuentos.	Existen 192 eventos de ataques de posible actividad del gusano (worm) Conficker, se genera 44 archivos infectados, 43 ataques de la variante de malware enviados desde host (computadores o dispositivos) internos, 43 incrementos de número de malware de eventos ocurridos en Host internos y se ha identificado en este primer semestre de 2019 1 botnet de comunicación

Nota: Tomado del Sistema de monitorización de eventos de seguridad (SIEM) McAfee administrado por la CGR.

Tabla 23. Amenazas identificadas Software correlacionador de eventos de seguridad de información Año 2019

TIPOS DE EVENTOS DE AMENAZAS	
	
Gráfica 13. Tipos de Malware	Gráfica 14. Eventos Mensaje de Regla de

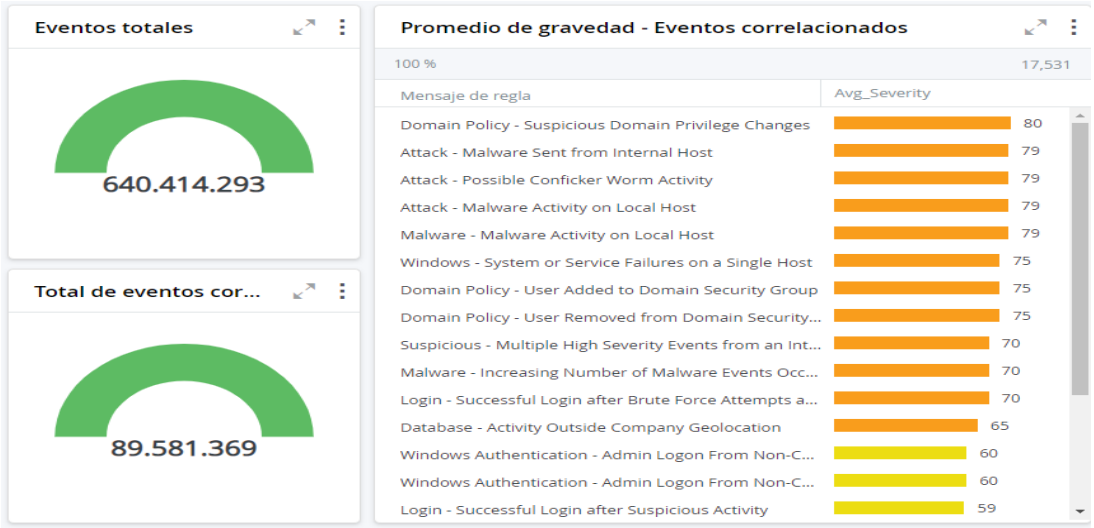
	Malware
En esta figura se observa que los tres tipos de amenazas que más han tenido recuento de eventos son malware con 598, virus con 300, gusano con 221 y red de bot o zombis	Existen 298 ataques de la variante de malware enviados desde host (computadores o dispositivos) internos, 296 incrementos de número de malware de eventos ocurridos en Host internos, se genera 293 archivos infectados, 221 eventos de ataques de posible actividad del gusano (worm) Conficker, y se ha identificado en este primer semestre de 2019 7 botnet (computador o dispositivo zombi) de comunicación.

Nota: Tomado del Sistema de monitorización de eventos de seguridad (SIEM) McAfee administrado por la CGR.

Eventos SIEM Año 2018

En la gráfica 15 se observa que el SIEM registró un total de 640.414.293 millones de eventos durante el año 2018 y logró corregir 89.581.369 millones. Los tres mensajes de regla que tuvieron más eventos fueron por política de dominio sospecha de cambio de privilegios en el dominio (80), ataques – Malware enviado desde Host interno (79) y ataque-posible actividad de gusano Conficker (79).

Gráfica 15**.** Promedio de gravedad – eventos correlacionados año 2018.



Fuente: Tomado del Sistema de monitorización de eventos de seguridad (SIEM) McAfee administrado por la CGR.

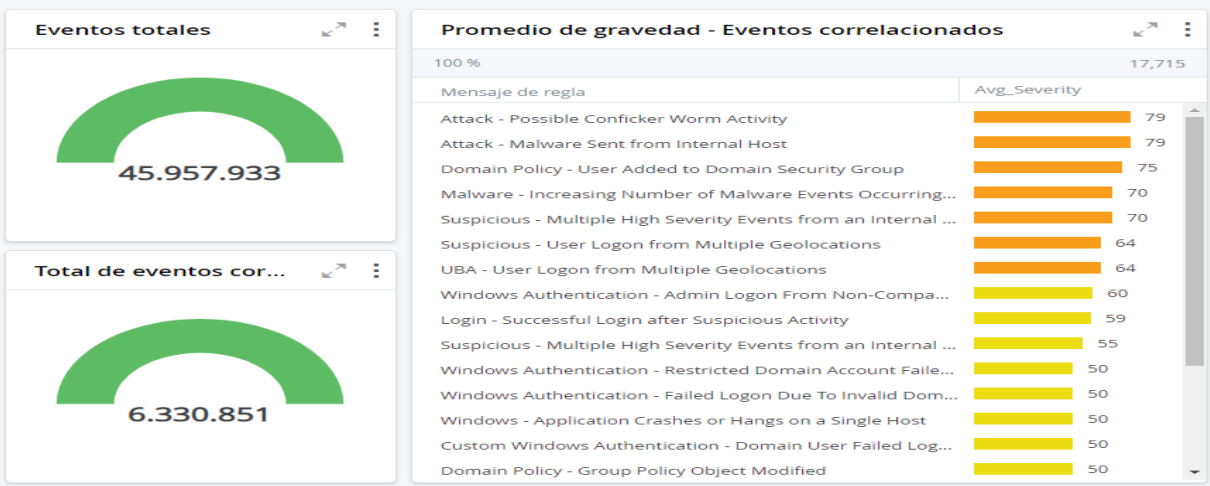
Eventos correlacionados primer trimestre Año 2019

En la gráfica 16 se observa que el SIEM ha registrado durante el primer trimestre de 2019 un total de 45.957.933 millones de eventos durante el año 2018 y logró corregir 6.330.851 millones.3

Los tres mensajes de regla que tuvieron más eventos fueron por ataque-posible actividad de gusano Conficker (79), Malware enviado desde Host interno (79) y política de dominio adicionar usuario a un dominio de grupo seguro (75). Según (Microsoft, 2000) “un dominio es una partición física de la base de datos de Active Directory, puede estructurarlos por la función empresarial (recursos humanos, ventas o contabilidad) o por la ubicación (geográfica o relativa).” el Active

Directory es un Directorio de los componentes y elementos de la organización para ser encontrados en la red informática.

Gráfica 16. Promedio de gravedad – eventos correlacionados Primer trimestre 2019.



Fuente: Tomado del Sistema de monitorización de eventos de seguridad (SIEM) McAfee administrado por la CGR.

Incidentes reportados a Unidad de Seguridad y Aseguramiento Tecnológico e Informático

De acuerdo a los datos registrados en la Unidad de Seguridad y Aseguramiento Tecnológico e Informático en el año 2018 se presentó una serie de incidentes relacionados con la seguridad de la información un 63% de incidentes de seguridad corresponde a incidentes de control de acceso, 15% sobre pérdida de dispositivo de almacenamiento, 11% de protección de datos personales, un 4% sobre perdida de expedientes, otro 4% perdida de computadores y un 3% de incidentes donde se encontraron documentos en la basura, según lo muestra la gráfica 17.

Gráfica 17. Incidentes de Seguridad de la información 2018 CGR

Fuente: Base de Datos incidentes reportados a la Unidad de Seguridad y Aseguramiento Tecnológico e Informático

Las anteriores estadísticas han sido tomadas de los registros de la base de datos de incidentes que se han materializado en la entidad y reportadas a la USATI.

Anexo Normativa de Seguridad Digital

A continuación se relaciona el Anexo C que hace parte del documento del Consejo Nacional de Política Económica y Social CONPES 3854 (Departamento Nacional de Planeación, 2016, pp.73-78) de Colombia que relaciona la normatividad relacionada con el tema de seguridad digital.

Anexo C: Normativa nacional relacionada con asuntos de seguridad digital

Norma	Contenido
Constitución Política de Colombia	Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros. Por ejemplo, Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6º, 8º, 7º, 28º, 12º y 13º), la autenticación electrónica (artículo 17º), la firma electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012).
Ley 594 de 2000 (Ley General de Archivos)	Habilita el uso de nuevas tecnologías de manera general, es posible establecer que para satisfacer los requerimientos establecidos en esta norma sea viable usar firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código Penal)	Por la cual se expide el código penal colombiano.
Ley 600 de 2000 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal.
Ley 679 de 2001 (Pornografía y explotación sexual con menores)	Esta Ley contempla en el artículo 4, un sistema de autorregulación, en virtud del cual el Gobierno nacional, por intermedio del Ministerio de Comunicaciones – hoy Ministerio de Tecnologías de la Información y las Comunicaciones·, promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información, estos códigos se elaboraran con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.
Ley 906 de 2004 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal (corregida de conformidad con el Decreto 2770 de 2004)
Ley 962 de 2005 (racionalización de trámites y procedimientos)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1032 de 2006 (derechos de autor y conexos)	Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).

Norma	Contenido
Ley 1150 de 2007 (medidas para la eficiencia y la transparencia)	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública (SECOP).
Circular Externa SFC 052 de 2007	Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad.
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales en relación al derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009 (Delitos Cibernéticos)	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 TIC".
Ley 1336 de 2009 (Explotación, pornografía y el turismo sexual con niños)	A través de esta ley se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Esta ley establece dos medidas para contrarrestar la explotación sexual y la pornografía infantil que se relacionan tangencialmente con las TIC, en primer lugar establece en el artículo 4 (autorregulación de café internet – códigos de conducta) que todo establecimiento abierto al público que preste servicios de internet o de café internet deberá colocar en un lugar visible un reglamento de uso público adecuado de la red, y deberá indicar que la violación a este genera la suspensión del servicio al usuario.
Ley 1341 de 2009 (Sector TIC)	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Decreto 1727 de 2009 (Habeas Data)	Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.
Decreto 2952 de 2010 (Habeas Data)	Este Decreto reglamenta los artículos 12 y 13 de la Ley 1266 de 2008, en este sentido establece que con fundamento en el principio constitucional de solidaridad surgen obligaciones a cargo del Estado y de los ciudadanos, en virtud de las cuales cuando se presenten situaciones de fuerza mayor, es posible otorgar a las víctimas de secuestro, desaparición forzada y personas secuestradas, debido a su estado de debilidad manifiesta, un tratamiento diferenciado en la administración de su información financiera, crediticia y comercial.
Ley 1437 de 2011 (Uso de medios electrónicos Procedimiento Administrativo Electrónico)	Consagra la utilización de medios electrónicos en el procedimiento administrativo permitiendo adelantar los trámites y procedimientos administrativos por medios electrónicos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes

Norma	Contenido
	electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen por medios electrónicos con validez jurídica y probatoria.
Ley 1453 de 2011 (Estatuto de seguridad ciudadana)	Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.
Ley 1474 de 2011 (Uso de medios tecnológicos)	Esta norma permite la utilización de medios tecnológicos en los trámites y procedimientos judiciales, en las diligencias, práctica de pruebas y notificaciones de las decisiones.
Ley 1480 de 2011 (Estatuto del Consumidor - Comercio electrónico y publicidad)	Se incluye en la definición de las ventas a distancia, aquellas que se realizan a través del comercio electrónico. El artículo 26 de esta Ley, consagra que la SIC determinará las condiciones mínimas bajo las cuales operar la información pública de precios de los productos que se ofrezcan a través de cualquier medio electrónico.
Ley 1564 de 2011 (Uso de las TIC)	Permite el uso de las TIC en todas las actuaciones de la gestión y trámites de los procesos judiciales con el fin de facilitar el acceso a la justicia.
Resolución CRC 3066 de 2011	Se establece el régimen integral de protección de los derechos de los usuarios de los servicios de comunicaciones. En particular, se establece que los proveedores de servicios de comunicaciones deberán implementar procesos formales de tratamiento de incidentes de seguridad de la información propios de la gestión de seguridad del proveedor.
Resolución CRC 3067 de 2011 "Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones"	Está Resolución establece en el artículo 2.3, que los proveedores que ofrezcan acceso a internet deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad de la red y la integridad del servicio, para evitar la interceptación, interrupción e interferencia del mismo.
Resolución CRC 3502 de 2011 (Neutralidad de Internet)	A través de la Resolución CRC 3502 de 2011, se establecen condiciones regulatorias relativas a la neutralidad en internet, en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011 (PND 2010 – 2014). Se contempla en el artículo 3 los principios de libre elección, no discriminación, transparencia e información, que deben aplicar los proveedores que prestan el servicio de acceso a internet.
Ley 1581 de 2012 (Habeas Data)	Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
Ley 1712 de 2012 (Uso de las TIC)	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la

Norma	Contenido
	información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.
Decreto 1704 de 2012 (Interceptación legal de comunicaciones)	Este Decreto determina que la interceptación legal de comunicaciones, es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos de inteligencia. De esta manera, se determina que los proveedores que desarrollen su actividad comercial en el territorio nacional, deben implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del fiscal general de la nación, con todas las labores inherentes a la interceptación de las comunicaciones requeridas.
Decreto 2758 de 2012 (Modifica la Estructura del Misterio de Defensa)	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del Viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente le encarga a la Dirección de seguridad pública y de infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.
Decreto Ley 019 de 2012 (Entidades de Certificación Digital)	Establece las siguientes actividades que las entidades de certificación acreditadas podrán realizar en el país, tales como emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, y emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999, entre otras.
Resolución SIC No. 76434 de 2012 (Habeas Data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.
Decreto 2364 de 2012 (Firma electrónica)	Establece la reglamentación del artículo 7º de la Ley 527 de 1999, complementando el marco jurídico de los mecanismos de autenticación previstos en Colombia. Se definen algunas características que benefician el uso de los medios electrónicos, tales como la definición de los criterios de confiabilidad y apropiabilidad en el uso de los mecanismos de autenticación, la fijación de la relación de género y especie entre firmas electrónicas y firmas digitales, señalando las diferencias en su tratamiento probatorio, pues en el último mecanismo existe una inversión probatoria, y el uso de la firma electrónica mediante acuerdo de las múltiples partes de una relación jurídica, entre otras.
Resolución 3933 de 2013	Creó el Grupo colCERT y asignó funciones a la dependencia de la Dirección de seguridad pública y de infraestructura del Ministerio de Defensa Nacional respecto a promover el desarrollo de capacidades locales o sectoriales para la

Norma	Contenido
del Ministerio de Defensa Nacional (Crea y organiza grupos internos de trabajo)	gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.
Decreto 1377 de 2013 (Habeas Data)	Se reglamenta parcialmente la Ley 1581 de 2012, facilitando la implementación y el cumplimiento de la Ley 1581 de 2012, reglamentando aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados.
Ley 1621 de 2013 para la función de inteligencia y contrainteligencia en Colombia)	Esta ley expide normas para fortalecer el marco jurídico que permita a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal.
Decreto 0032 de 2013 (Creación de la Comisión Nacional Digital y de Información Estatal)	El Ministerio de Tecnologías de la Información y las Comunicaciones en cumplimiento de los lineamientos señalados en el Documento CONPES 3701, creo a través de este Decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano.
Decreto 333 de 2014 (Habeas Data)	Se reglamenta el artículo 160 del Decreto 019 de 2012), definiendo el régimen de acreditación de las entidades de certificación abierta, en desarrollo de lo que define el artículo 160 del Decreto 019 de 2012 y se deroga el Decreto 1747 de 2000, que reglamenta de manera parcial la Ley 527 de 1999, referente a las entidades de certificación digital, certificados y firmas digitales, de manera que las entidades que deseen seguir prestando los servicios de certificación digital, deberán iniciar la correspondiente acreditación, ya no ante la Superintendencia de Industria y Comercio, sino ante el Organismo de Acreditación en Colombia (ONAC).
Decreto 886 de 2014 (Registro Nacional de Base de Datos)	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al registro nacional de bases de datos. Se reglamenta la información mínima que debe contener dicho registro, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del tratamiento.
Decreto 2573 de 2014 (Gobierno en Línea)	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 compilatorio 1070 de 2015	Por medio del cual se reglamenta la Ley estatutaria 1621 de 2013, que establece el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, para cumplir con su misión constitucional y legal. Adicionalmente, establece la reserva legal, los niveles de clasificación y el sistema para la designación de los niveles de acceso a la información y clasificación de documentos.
Decreto 1074 de 2015 (Decreto Único Reglamentario del Sector de Comercio, Industria y Turismo)	Por medio del cual se expide el Decreto único reglamentario del sector de comercio, industria y turismo, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector. Compilación de los Decretos 2364 de 2012, 333 de 2014, entre otros.

Norma	Contenido
Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC)	Por medio del cual se expide el Decreto único reglamentario del sector TIC, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector.
Circular Externa SIC 02 del 3 de noviembre de 2015	Por la cual la Superintendencia de Industria y Comercio impartió instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el registro nacional de bases de datos a partir del 9 de noviembre de 2015.

Fuente: Adaptado de CRC, 2015

REFERENCIAS BIBLIOGRÁFICAS

Abril, Ana; Pulido, Jarol; Bohada, J. (2013). Análisis de riesgos de seguridad de la información. *Revista Ciencia, Innovación y Tecnología (RCIYT)*, *1*. Retrieved from https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121/113

Allsoft. (2008). *El Modelo CMMI*. México. Retrieved from http://www.allsoft.mx/recursos/ElModeloCMMI.pdf

Almanza, R. (2018). Instrumento de medición de dimensiones de seguridad. Bogotá.

Areitio Bertolín, J. (2008). *Seguridad de la información : redes, informática y sistemas de información* (Paraninfo). Madrid: Paraninfo Cengage Learning. Retrieved from https://books.google.com.co/books?id=_z2GcBD3deYC&lpg=PP1&dq=que es seguridad de la informacion&hl=es&pg=PA2#v=onepage&q=que es seguridad de la informacion&f=false

Augusto, L., & Focazzio, M. (2011). *Gobierno de la Seguridad y el Modelo del Negocio para la Seguridad de la Información Agenda Para qué la Seguridad? Gobierno de la Seguridad de la Información Modelo del Negocio para la Seguridad de la Información Conclusiones*. Bogotá. Retrieved from http://52.0.140.184/typo43/fileadmin/Base_de_Conocimiento/XI_JornadaSeguridad/PresentacionLucioMolinaFocazzio.pdf

Ballester, M. (2018). JOnline: Gobierno de las TIC ISO/IEC 38500. Retrieved December 1, 2018, from https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Gobierno-de-las-TIC-ISO-IEC-385001.aspx

Canales, F. H. De, Alvarado, E. L. De, & Pineda, E. B. (2008). Unidad II: Base filosófica del conocimiento. ¿Cuál es el fundamento filosófico de la investigación? *Metodología de La*

Investigación, 276. Retrieved from https://apps.who.int/iris/handle/10665/310238

Cano M, J. J. (2013). *Inseguridad de la Información, Una visión Estratégica*. Bogotá: Alfaomega Colombiana S.A.

Cano M, J. J. (2016). *Manual de un Ciso* (Primera Ed). Bogotá: Ediciones la U.

CCTI Consultoría de Tecnología. (2018). ¿Sabías qué? (CMMI) - CCTI - Consultoría en Tecnología. Retrieved July 9, 2019, from https://www.ccti.com.co/index.php/es/blog/197-sabias-que-cmmi

CGR. (2018). *ARQUITECTURA EMPRESARIAL CONTRALORÍA GENERAL DE LA REPUBLICA Plan de implementación y migración versión inicial*. Bogotá. Retrieved from https://congenrep.sharepoint.com/sites/ResultadosEjerciciosdeAE/SiteAssets/SitePages/Consolidado/2589842880Oportunidades y Soluciones Ciclo 2.pdf

Congreso de la república de colombia. Ley de Delitos Informáticos en Colombia, Pub. L. No. Ley 1273 (2009). http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html. Retrieved from http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. Ley 1266 de 2008 - Gestor Normativo Función Pública, Pub. L. No. Ley 1266 (2008). Retrieved from https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de la República de Colombia. (2012). Ley 1581 de 2012 sobre Habeas Data en Colombia - Departamento de Propiedad Intelectual. Retrieved January 28, 2019, from https://propintel.uexternado.edu.co/ley-1581-de-2012-sobre-habeas-data-en-colombia/

Contraloría General de la República. (2018a). PLAN ESTRATEGICO CGR 2018 - 2022.PDF. Bogotá. Retrieved from https://www.contraloria.gov.co/documents/20181/1341740/PLAN+ESTRATEGICO+CGR+2

018+-+2022.PDF/f20ab90f-a6aa-4376-b765-dd9d9117996c?version=1.0

Contraloría General de la República. (2019a). Estructura de la Contraloría General de la República.

Contraloría General de la República. (2019b). *La Entidad - Contraloría General de la República*. Bogotá. Retrieved from https://www.contraloria.gov.co/contraloria/la-entidad

Contraloría General de la República, O. de planeación. (2018b). *Macroproceso de Apoyo Gestión Integral de la Seguridad - GIS*. Bogotá. Retrieved from https://estrategicos.contraloria.gov.co/cdisc/principal.asp

De Oliveira Alves, Gustavo Alberto; Da Costa Rust Carmen, Luiz Fernando; Ribeiro de Almeida Dutra, A. C. (2006). Enterprise Security Governance, *00*(C), 71–80.

Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas: Riesgos de Gestión, Corrupción y Seguridad Digital, 1–93. Retrieved from http://www.funcionpublica.gov.co/documents/418548/34150781/Guía+para+la+administración+del+riesgo+y+el+diseño+de+controles+en+entidades+públicas+-+Riesgos+de+gestión%2C+corrupción+y+seguridad+digital+-+Versión+4+-+Octubre+de+2018.pdf/68d324dd-55c5-11e0-9f

Departamento de la Función Pública. (2018a). Manual de Estructura del Estado - Función Pública. Retrieved January 30, 2019, from http://www.funcionpublica.gov.co/eva/gestornormativo/manual-estado/index.php

Departamento de la Función Pública. (2018b). Organismos de Control - Manual del Estado - Función Pública. Retrieved January 30, 2019, from http://www.funcionpublica.gov.co/eva/gestornormativo/manual-estado/organismos-

control.php

Departamento Nacional de Planeación. (2011). Consejo Nacional de Política Económica y Social CONPES 3701. Retrieved July 5, 2019, from https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Departamento Nacional de Planeación. (2016). Consejo Nacional de Política Económica y Social CONPES 3854. Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Evans, J. D. (2011). *Modelo de Seguridad de la Información - Gobierno de Seguridad*. áBogota. Retrieved from http://52.0.140.184/typo43/fileadmin/Base_de_Conocimiento/XI_JornadaSeguridad/PresentacionJavierEvans.pdf

Figura Niveles de madurez de CMMI. (2017). METODOLOGIA RUP Y METODOLOGIA CMMI.: NIVELES DE MADUREZ DE CMMI. Retrieved July 9, 2019, from http://rupandcmmi.blogspot.com/p/niveles-de-madurez.html

Francavilla, C. (2014). *Como aporta COBIT 5 y gobernanza de TI a la gobernanza empresarial*. Montevideo. Retrieved from www.isaca.org.uy

García, Granados Monica Liliana; Gómez, L. J. N. (2015). Procedimiento Administración de Riesgos CGR. Retrieved from https://estrategicos.contraloria.gov.co/cdisc/documentos/200.pdf

Gómez, R., Hernán Pérez, D., Donoso, Y., & Herrera, A. (2010). *Metodología y gobierno de la gestión de riesgos de tecnologías de la información Methodology and Governance of the IT Risk Management*. Retrieved from http://www.scielo.org.co/pdf/ring/n31/n31a12.pdf

INCIBE. (2017). Glosario de términos de ciberseguridad. Retrieved from

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Information Security Forum. (2011). Foro de Seguridad de la Información. Retrieved July 9, 2019, from https://www.securityforum.org/

Instituto Nacional de Ciberseguridad INCIBE. (2016). Descubre los diferentes tipos de malware que pueden afectar a tu pyme | INCIBE. Retrieved April 20, 2019, from https://www.incibe.es/protege-tu-empresa/blog/descubre-tipos-malware

ISO/IEC Organización Internacional de Normalización. (2013). ISO / IEC 27014: 2013 - Tecnología de la información - Técnicas de seguridad - Gobernanza de la seguridad de la información. Retrieved April 18, 2019, from https://www.iso.org/standard/43754.html

ISO. (2013). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved July 8, 2019, from http://www.iso27000.es/sgsi.html

ISO / IEC. (2013). ISO / IEC 27014 gobierno de seguridad de la información. Retrieved July 9, 2019, from https://www.iso27001security.com/html/27014.html

ISO 22301 Sistema de Gestión y Continuidad del Negocio. (2016). Contenido de la Norma ISO 22301 | ISO 22301. Retrieved July 8, 2019, from http://normaiso22301.com/contenido-de-la-norma-iso-22301/

ISO27000.es. (2012). Ciclo Deming (2005)- mejora continua. Retrieved April 17, 2019, from http://www.iso27000.es/sgsi_implantar.html#seccion1

ISOTools- Plataforma tecnológica para la gestión de la Excelencia. (2014). ISO/IEC 27004. Evaluación de la Seguridad de la Información. Retrieved April 20, 2019, from https://www.isotools.cl/isoiec-27004/

ISOTools. (2016). ISO 22301: Pasos para gestionar la Continuidad de Negocio. Retrieved July 8,

2019, from https://www.isotools.cl/iso-22301-pasos-gestionar-la-continuidad-negocio/

ISOtools Excellence. (2014). Desarrollo de la familia de normas ISO 27000. Retrieved July 8, 2019, from https://www.pmg-ssi.com/2014/04/desarrollo-de-la-familia-de-normas-iso-27000/

ISOTools Excellence. (2017). ¿Seguridad informática o seguridad de la información? Retrieved July 5, 2019, from https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Lopez, N. R. S. (2012). El portal de ISO27001 en español. Retrieved from http://www.iso27000.es/faqs.html#seccion2

Mahncke, R. J. (2013). The Applicability of ISO/IEC27014:2013 For Use Within General Medical Practice. https://doi.org/10.4225/75/5798124731b3f

Marulanda Echeverry, C. E., López Trujillo, M., & Valencia Duque, F. J. (2018). Gobierno y gestión de ti en las entidades públicas. *AD-Minister*, (31), 75–92. https://doi.org/10.17230/ad-minister.31.5

Maya, V., Alonso, M., Halaby, R., & Altamiranda, P. (2018). *Sistema de Gestión de Seguridad-SGS para la Contraloría General de la República*. Bogotá. Retrieved from https://clic-online.contraloria.gov.co/USATI/Documents/libro_SGS_USATI_FINAL_web.pdf

Microsoft. (2000). Introducción a Active Directory. Retrieved April 20, 2019, from https://support.microsoft.com/es-co/help/196464

Ministerio de las Tecnologías y las Comunicaciones. Decreto 1078 de 2015 (2015). Colombia. Retrieved from https://www.mintic.gov.co/portal/604/w3-article-9528.html

Ministerio de las Tecnologías y las Comunicaciones. (2018). *articles-61854_documento*. Bogotá. Retrieved from https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

Ministerio de Tecnologías de información y las comunicaciones. (2018). Componentes conoce. Retrieved June 3, 2019, from https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-

8110.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). Contexto - Arquitectura TI. Retrieved April 15, 2019, from https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8109.html

Mintic;Vive digital para la gente. (2016). Guía de indicadores de gestión para la seguridad de la información, (9). Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

Mintic. (2016). *Modelo de Seguridad y Privacidad de la Información*. Bogotá. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Mintic. (2018a). Fortalecimiento de la Gestión de TI en el Estado Iniciativas. Retrieved from https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6781.html

Mintic. (2018b). Seguridad TI. Retrieved from https://www.mintic.gov.co/gestionti/615/w3-article-4767.html

MINTIC. (2016). Gestión IT4+. Retrieved from https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-6204.html

MINTIC. (2017). Glosario. Retrieved July 5, 2019, from https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html

Ocampo, D. (2015). Modelo de Seguridad de la Información para las entidades del Estado Colombia. Retrieved from http://polux.unipiloto.edu.co:8080/00002024.pdf

Ona System. (2018). Información de seguridad y administracion de eventos SIEM. Retrieved April 7, 2019, from https://www.onasystems.net/siem/

Ona Systems. (2018). *Glosario Seguridad*. Retrieved from https://www.onasystems.net/wp-content/uploads/2016/10/Glosario-seguridad-Ona-systems-2016.pdf

Panda security. (2018). Virus Conficker.C. Retrieved May 26, 2019, from https://www.pandasecurity.com/spain/mediacenter/malware/virus-famosos-conficker/

Presidencia de la República. Decreto 1377 de 2013 - Gestor Normativo Función Pública, Publicado en el Diario Oficial 48834 de junio 27 de 2013 § (2013). Retrieved from http://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Presidencia de la República de Perú. Ley de Gobierno Digital: Tecnología al servicio de los ciudadanos - Perú Bicentenario | 200 años de Independencia (2018). Perú. Retrieved from https://perubicentenario.pe/actualidad/ley-de-gobierno-digital-tecnologia-al-servicio-de-los-ciudadanos/

Quinn Patton, M. (1990). *Qualitative Evaluation and Research Methods*. (Second). Sage.

República, C. G. de la. Resolución OGZ-0531-2016.pdf (2016). Bogotá. Retrieved from https://clic-online.contraloria.gov.co/USATI/Documents/Resolución OGZ-0531-2016.pdf

Sarabia Bautista, R. X. (2018). ¿Gobierno de la ciberseguridad? | Revista .Seguridad. *Revista.Seguridad*. Retrieved from https://revista.seguridad.unam.mx/numero27/¿gobierno-de-la-ciberseguridad

Scitum S.A. de C.V. (2017). ISO-27001:2013 ¿Qué hay de nuevo? – Magazcitum. Retrieved May 22, 2019, from http://www.magazcitum.com.mx/?p=2397#.XOYF5BeJLIU

Secretaria de Transparencia; Presidencia. (2015). *ABC de la Ley de transparencia y del derecho de acceso a la información pública nacional*. Bogotá. Retrieved from https://www.ramajudicial.gov.co/documents/5067224/14535305/ABC+LEY+DE+TRANSPARENCIA.pdf/68516da7-3ea2-4d64-9ca6-32bfb3737190

Secretaria de Transparencia Presidencia de la República. (2016). *Estatuto Anticorrupción Ley 1474 de 2011. Avances y desafíos tras cinco años de su expedición* (No. 1474). Bogotá,

Colombia. https://doi.org/978-958-18-0443-6

Sociedad Colombiana de Psiquiatría., M. G.-R. C. (2005). *Revista colombiana de psiquiatría. Revista Colombiana de Psiquiatría* (Vol. XXXIV). Sociedad Colombiana de Psiquiatría. Retrieved from https://www.redalyc.org/html/806/80628403009/

Sylvester, D. (2011). ISO 38500 — Why Another Standard ? *COBIT Focus*, *2*(April), 1–3. Retrieved from https://www.isaca.org/Knowledge-Center/Documents/COBIT-Focus-ISO-38500-Why-Another-Standard.pdf

Tharakan, Devassy Jose, C. I. 27001 L. I. P. (2016). Protegiendo la Información—Estrategias Prácticas para CIOs y CISOs. *ISACA, JOURNAL*, *3*. Retrieved from https://www.isaca.org/Journal/archives/2016/volume-3/Pages/protecting-information-practical-strategies-for-cios-and-cisos-spanish.aspx

Ugalde Binda, N., & Balbastre-Benavent, F. (2013). Investigación Cuantitativa E Investigación Cualitativa: Buscando Las Ventajas De Las Diferentes Metodologías De Investigación. *Ciencias Económicas*, *31*(2), 179–187. https://doi.org/ISSN:0252-9521

Universidad Libre de Colombia. (2018). Seguridad de la Información. Retrieved July 5, 2019, from http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion

Vargas-Bermúdez, F. A. (2017). Marcos de control y estándares para el gobierno de tecnologías de información (TI). *I3+*, *2*(1), 4. https://doi.org/10.24267/23462329.71

Vivares, vergara J. A. (2017). *Modelo de madurez para valorar el sistema de producción y formular la estrategia de manufactura*. Retrieved from http://bdigital.unal.edu.co/62160/1/18617391.2017.pdf