INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

Arquitectura de Seguridad de Información en una entidad del estado

PRESENTA:

Claudia Patricia Camacho Correa

Código 1712010225

ASESOR TEMÁTICO:

M.Sc. Wilmar Jaimes Fernández

Mayo 2018

ÍNDICE GENERAL

ÍNDICE DE GRÁFICAS

ÍNDICE DE TABLAS

RESUMEN

La arquitectura empresarial es el proceso de traducir la visión empresarial y la estrategia en un cambio empresarial efectivo al crear, comunicar y mejorar los principios y modelos clave que definen el estado futuro de la empresa y permiten su evolución.

A su vez, la arquitectura de seguridad de la información empresarial es el proceso que entrega planificación, diseño y documentación de implementación (artefactos) en apoyo del programa de seguridad de la información. Es una herramienta clave para mejorar la planificación, implementación y operaciones de seguridad de la información

La arquitectura de seguridad es un proceso continuo, en lugar de una actividad única. El foco está en desarrollar y mantener un conjunto de requisitos, modelos, plantillas y principios en evolución, en lugar de entregar un conjunto de artefactos estáticos.

A nivel mundial se han desarrollado estándares, metodologías, mejores prácticas y herramientas que facilitan una gestión eficiente de la seguridad. El hecho de seguir estándares y mejores prácticas de gestión de la seguridad de la información permite a las organizaciones obtener un beneficio básico: la gestión efectiva y controlada de uno de sus activos fundamentales: la **información.**

La Comisión de Regulación de Comunicaciones requiere para el desarrollo de sus funciones la gestión de la seguridad de los Sistemas de Información; por tal motivo, la seguridad informática, vista como el conjunto de medidas preventivas y correctivas que permiten resguardar y proteger adecuadamente la confidencialidad, disponibilidad e integridad de la información de una organización, constituye un requisito fundamental para la buena marcha de una Entidad.

ABSTRACT

The security architecture of business information is the process that delivers the planning, design and documentation of the implementation.

The information security architecture provides companies with a strategic action plan, through which the guidelines on information security are implemented in each of the business processes. It is a key tool to improve the planning, implementation and operations of information security

The security architecture is a continuous process, rather than a single activity. The focus is on developing and maintaining a set of evolving requirements, models, templates and principles, rather than delivering a set of static artifacts.

At a global level, standards, methodologies, best practices and tools have been developed that facilitate an efficient management of security. The fact of following rules and best practices of information security management allows organizations to obtain a basic benefit: the effective and controlled management of one of the fundamental assets: information.

The Communications Regulation Commission requires the management of Information Systems security for the development of its functions; for this reason, computer security, seen as the set of preventive and corrective measures that allow protecting and protecting the confidentiality, availability and integrity of an organization's information, is a fundamental requirement for the proper functioning of an Entity.

PALABRAS CLAVE

Gestión de seguridad en la información, procesos de negocio, gobierno de seguridad de la información, políticas de seguridad, análisis de riesgos, arquitectura de seguridad en la información.

KEY WORDS

Information security management, business processes, information security governance, security policies, risk analysis, information security architecture.

INTRODUCCIÓN

La rápida evolución del entorno tecnológico requiere que, para proteger los sistemas de información, las organizaciones deben contar con un plan de seguridad a través del cual se proporcionen los controles mínimos adecuados, se establezcan las responsabilidades internas, se definan los propietarios de la información, de la red y se definan los procedimientos y protocolos a seguir para su correcta utilización.

Las entidades gubernamentales no pueden estar ausentes en las nuevas tecnologías de información, ni en el compromiso de adoptar los lineamientos del Ministerio de Tecnologías de Información (MINTIC), por lo cual se debe generar una estrategia que logre la actualización tecnológica que requiere la entidad, buscando la mejora en los servicios tecnológicos desde los temas de soporte, hasta la implementación de nuevas herramientas tecnológicas.

Un elemento crítico para el éxito y la supervivencia de las organizaciones es la administración efectiva de la información y de las Tecnologías de la Información (TI) relacionadas, como parte fundamental para alcanzar este objetivo se encuentra el aseguramiento de la seguridad de la información. Las organizaciones deben garantizar la integridad, confidencialidad, disponibilidad y privacidad de la información. La gran incógnita es ¿cómo se puede lograr esto? ¿Por dónde empezar? ¿Qué se necesita realmente? ¿Cuánto presupuesto se necesita?, ¿Quién es el responsable de implementarlo? La respuesta no es sencilla, teniendo en cuenta que las organizaciones resuelven los problemas de seguridad de una manera puntual, reactiva, correctiva y no desde un punto de vista estructurado.

A nivel nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, estableció un Modelo de Arquitectura de Seguridad y Privacidad de la Información (MSPI), el cual contiene componentes y criterios que guían a las entidades para tomar acciones que permitan fortalecer la relación de la entidad con el ciudadano. Con la implementación de este modelo por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de seguridad de la información como base de la aplicación del concepto de Seguridad Digital.

En línea con esto, la disponibilidad de los sistemas de información conlleva un papel fundamental para la ejecución y cumplimiento de las labores de las entidades públicas, las

repercusiones de la no disponibilidad en los sistemas, genera un traumatismo al interior de las áreas, ya que estos trámites tienen establecidos unas fechas de atención que si no se cumplen pueden generar sanciones y multas a la entidad.

Por estas razones, la dirección de Tecnologías y Sistemas de la Información de la entidad de índole nacional CRC, objeto del análisis del proyecto, debe definir e implementar un esquema de Gobierno TI alineado con la estrategia misional y con el Modelo Integrado de Planeación y Gestión. Como parte de este modelo debe definir la arquitectura de seguridad de la información que brindará a la organización un esquema estratégico con el cual se establezcan los lineamientos en materia de seguridad de la información para los diferentes procesos organizacionales, con lo cual permitirá identificar los elementos y los componentes necesarios para definir, normar, implantar, monitorear y auditar los requerimientos de seguridad con una visión de negocios apoyada en tres factores críticos de éxito: recursos humanos, procesos de negocio y tecnología.

OBJETIVO GENERAL

Definir e implementar un modelo de arquitectura de seguridad de la información para una entidad del estado. Identificando brechas que generen algún riesgo al desempeño de la organización y estableciendo las actividades necesarias para garantizar la seguridad de la información, apoyando a la entidad de forma estratégica en su mejoramiento continuo y alineada con la estrategia de gobierno digital.

1.1 OBJETIVOS ESPECIFICOS

- Definir e implementar un esquema de Gobierno TI alineado con la estrategia misional.
- Realizar el diagnostico de seguridad en la información sobre la situación actual.
- Adoptar el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Optimizar la gestión de la seguridad de la información.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

2 ARQUITECTURA DE SEGURIDAD EN LA INFORMACION

A lo largo de los últimos años, se han desarrollado varios modelos de arquitectura de seguridad de la información, entre los cuales se encuentran:

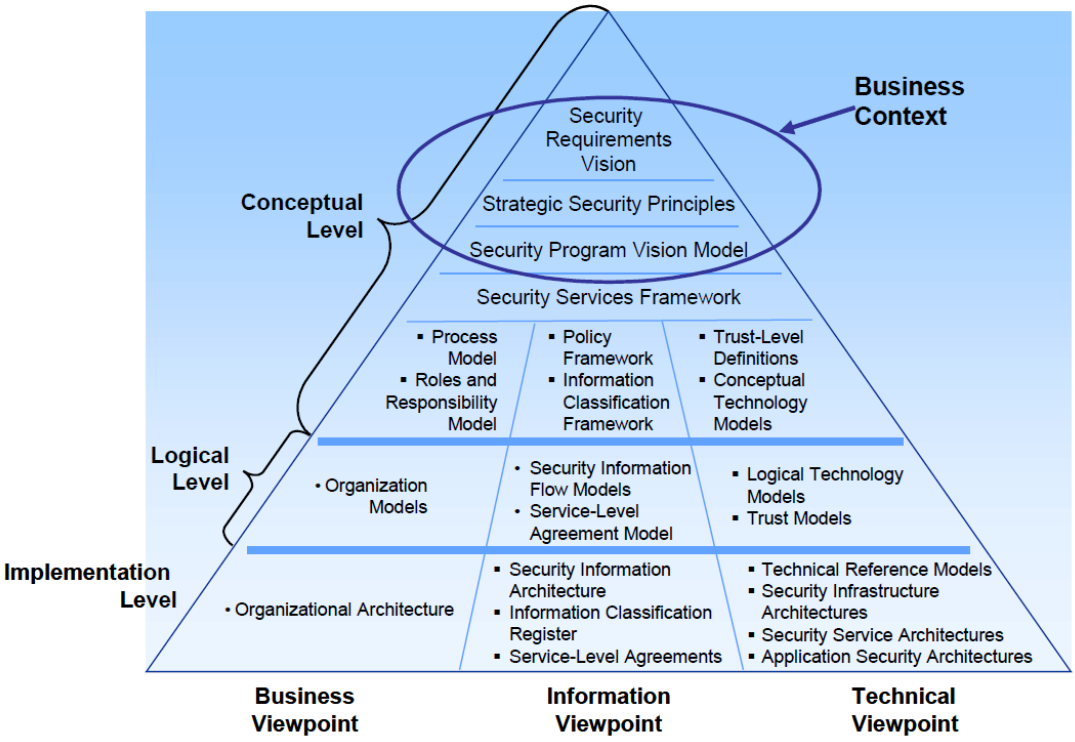
2.1 Marco de Arquitectura de Seguridad de la Información – Gartner

De acuerdo con la publicación de Gartner “An Introduction to Information Security Architecture” [1]: existen muchos síntomas de seguridad de la información empresarial ineficaz o ineficaz. Algunos ejemplos incluyen:

- Procesos de administración de seguridad dispersos
- Herramientas de seguridad duplicadas o superpuestas
- Las herramientas no funcionan o no son aceptadas por los usuarios
- Resultados de la auditoría y largos procedimientos de auditoría
- Dificultad para obtener fondos y aprobación para iniciativas de seguridad

Las razones por las cuales las empresas pueden no estar administrando la seguridad de manera efectiva, tomando las decisiones de implementación correctas o compartiendo los recursos varían. Sin embargo, las causas raíz a menudo tienen que ver con el fracaso en vincular la seguridad con la estrategia comercial, en determinar el valor de la seguridad para las partes interesadas, tomando las decisiones correctas entre alternativas de soluciones competitivas y administrando proyectos de manera efectiva. Las organizaciones grandes y pequeñas pueden usar prácticas de arquitectura de seguridad para ayudar a tomar decisiones sobre el proceso, la información y los cambios tecnológicos necesarios para apoyar la estrategia de negocios.

La arquitectura de seguridad de la información empresarial (EISA) es una parte de la arquitectura empresarial que se centra en la seguridad de la información en toda la empresa. La arquitectura de seguridad no es una ciencia precisa, a partir de la práctica se determina qué requisitos empresariales se deben establecer, qué soluciones y enfoques funcionan, y cuales enfoques son menos efectivos. Por lo tanto, hay una necesidad de centrarse en la mejora continua en la madurez de la práctica EISA. Y, mientras que la práctica de EISA (especialmente en el contexto del uso de los principios de EA) es comparativamente nuevo en la mayoría de las organizaciones, no es prematuro identificar los criterios de madurez que son específicos de la arquitectura de seguridad.



Gráfica 1 - Marco de arquitectura de seguridad en la información.

Fuente Gartner

Este modelo sirve para transmitir algunos principios importantes de la práctica de arquitectura de seguridad:

- El marco de la arquitectura de seguridad permite la planificación y el diseño a través de múltiples iteraciones (niveles de abstracción).
- Los artefactos de arquitectura de seguridad consisten en los modelos, principios y requisitos documentados de diversos niveles de abstracción.
- La arquitectura debe abordar, como mínimo, las perspectivas técnicas, comerciales y de información del entorno de seguridad de la información.
- El punto de partida para toda planificación de seguridad debe ser el contexto comercial, tal como se formalizó en una visión de requisitos (CRV), principios de seguridad estratégica y un modelo de visión común.
- La arquitectura de la solución para cualquier implementación de seguridad es una combinación del negocio, la información y artefactos tecnológicos requeridos para esa implementación.

2.2 Arquitectura de Seguridad de la información ISA – Jan Killmeyer [2]

Se parte de la comprensión de los requisitos para establecer un plan estratégico de seguridad dentro de la organización. También proporciona las directrices para la implementación del ISA con una guía paso a paso para analizar, desarrollar e implementar un programa lógico y efectivo para obtener el logro de los objetivos de seguridad de la organización.

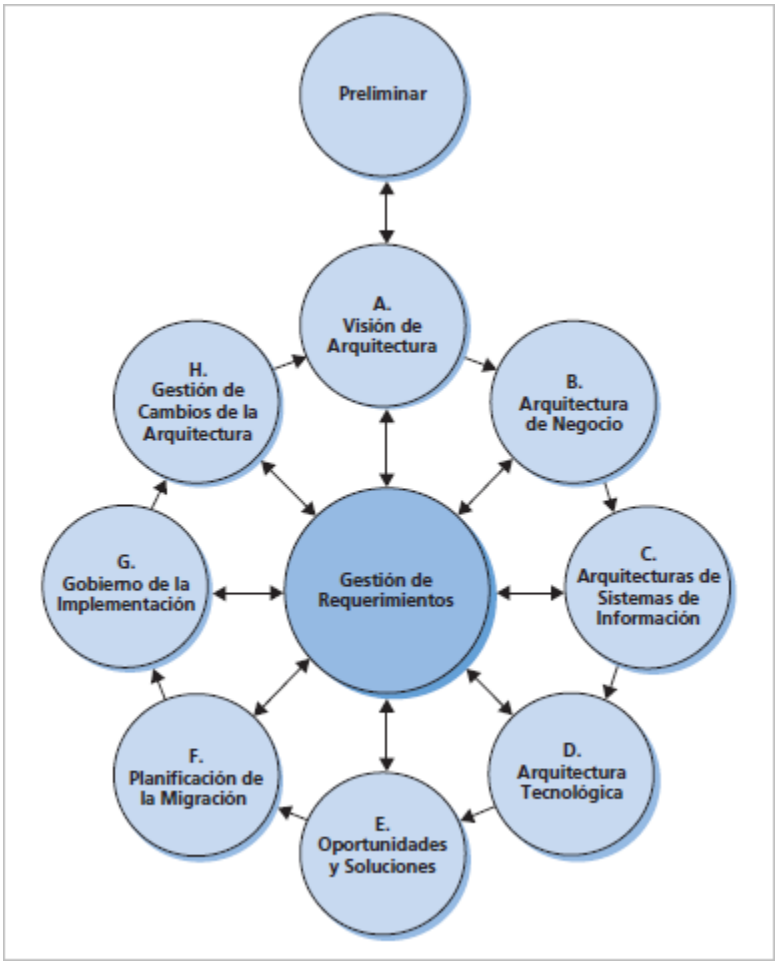
1. organización de seguridad e infraestructura
2. políticas de seguridad, estándares y procedimientos
3. Bases de seguridad y evaluaciones de riesgo
4. programas de concientización y capacitación sobre seguridad
5. cumplimiento

Es necesario que cada uno de los cinco componentes sea considerado y que los recursos adecuados están presupuestados para:

- Desarrollar una infraestructura de seguridad adecuada definiendo los roles y responsabilidades del personal clave en toda la organización
- Establecer políticas de seguridad, estándares y procedimientos que sean compatibles por la gestión y se adhirió a todos en y asociados con la organización
- Identificar las fortalezas y debilidades en el entorno de control de todas las plataformas de procesamiento, bases de datos, redes y aplicaciones y hacer correcciones a esas debilidades para la mejora continua.
- Desarrollar e implementar un programa efectivo de concienciación del usuario que comunica las políticas, estándares y procedimientos a todos los usuarios y los hace conscientes de los riesgos y consecuencias del uso indebido de recursos de información y procesamiento.
- Establecer un mecanismo para monitorear la efectividad de la seguridad programa a través de auditorías periódicas y pruebas de cumplimiento.

2.3 Arquitectura de Seguridad – The Open group [3]

Las políticas de seguridad y los estándares de seguridad se vuelven parte de la gestión de requisitos de la empresa proceso. La política de seguridad se establece a nivel ejecutivo del negocio, es duradera y resistente a un cambio caprichoso. La política de seguridad no está ligada a ninguna tecnología específica. Una vez que las políticas de seguridad se establecen, se los puede denominar requisitos para todos los proyectos arquitectónicos. El marco metodológico que propone, llamado Método de Desarrollo de Arquitectura (ADM en inglés) establece el desarrollo de metodologías en diferentes niveles: negocio, aplicaciones, datos y tecnología. En la metodología se establece varias fases, que se van desplazando a través de los dominios de arquitecturas descritos en la siguiente gráfica.



Gráfica 2 - El ciclo del método de desarrollo

Fuente TOGAF 9.1

2.4 Arquitectura Empresarial de Seguridad - SANS [4]

De acuerdo a su publicación de SANS (Instituto de Auditoria, Redes y Seguridad) “Information Systems Security Architecture: A Novel Approach to Layered Protection”, se establecen cinco fases para desarrollar una arquitectura de seguridad de sistemas de información en un entorno complejo con pocas medidas de seguridad, proporcionando un conjunto de pautas que pueden usarse para desarrollar componentes de arquitectura de seguridad que permitan una infraestructura escalable y segura:

1 Fase: Desarrollando Evaluaciones de la Seguridad.

2 Fase: Formulación de diseños de arquitectura de seguridad de destino

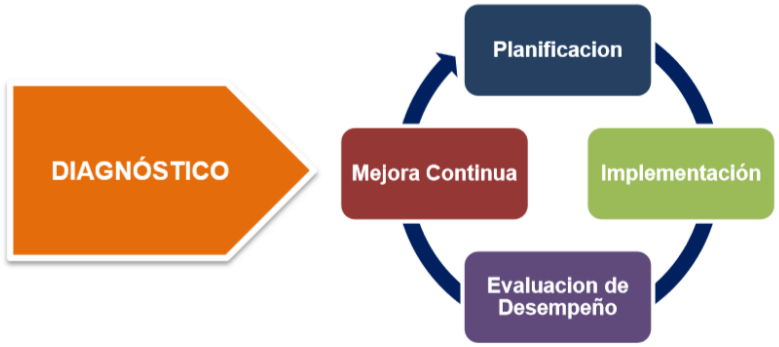
3 Fase: Construcción de Políticas y Procedimientos

4 Fase: Implementación del diseño de la arquitectura de seguridad de destino.

5 Fase: Integración de las prácticas de seguridad para mantener el estado de seguridad.

2.5 Modelo de Seguridad y Privacidad de la Información - MINTIC [4]

El Ministerio de las Tecnologías de Información y las Comunicaciones institucionalizó el Modelo de Seguridad y Privacidad de la Información que contiene el paso a paso que deben realizar las entidades nacionales y territoriales para la implementación del SGSI, contempla un ciclo de operación que consta de cinco (5) fases que se relacionan en la siguiente gráfica, con las cuales las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.



Gráfica 3- Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

En el presente Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	SUFICIENTE
Repetible	INTERMEDIO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Gráfica 4- Nivel de madurez Instrumento de MinTIC.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno digital, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información. Para lograr que los sistemas de información de la administración pública estén conectados, articulados, cumplan estándares y adopten las mejores prácticas en cuanto a su desarrollo y al manejo de la información se ha creado la Arquitectura TI Colombia, cuyo principal instrumento es el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI. Con él se busca habilitar las estrategias de Gobierno en línea de TIC para Servicios, TIC para la Gestión, TIC para el Gobierno Abierto y Seguridad y la Privacidad de la Información.

2.5.1 FASE- ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En la fase previa a la implementación del MSPI se alcanzarán las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.

2.5.2 FASE - PLANIFICACIÓN

Esta fase tiene la finalidad de generar un plan de seguridad y privacidad alineado con el propósito 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.

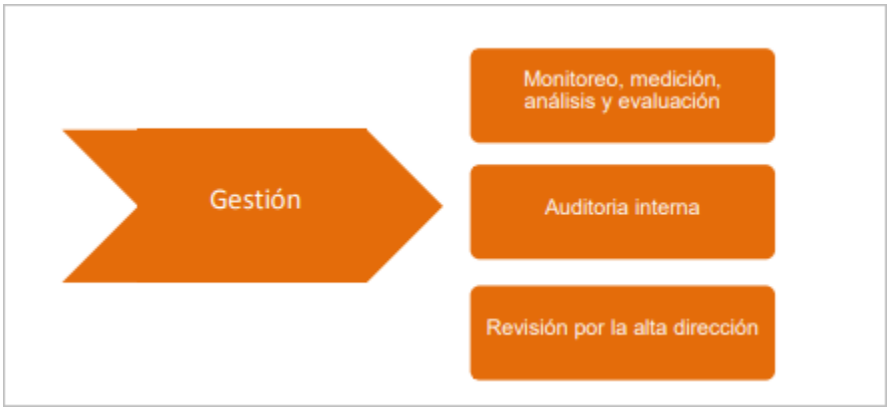
2.5.3 FASE- IMPLEMENTACIÓN

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase de planificación del MSPI, teniendo en cuenta los aspectos más relevantes en los procesos de implementación del MSPI.

Gráfica 5 - Fase de implementación
Fuente: MINTIC – 2017

2.5.4 FASE – EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base en los resultados que arroja los indicadores de la seguridad de la información propuestos para verificación de la eficacia y efectividad de los controles implementados.



Gráfica 6 - Fase de Evaluación de desempeño
Fuente: MINTIC – 2017

2.5.5 FASE – MEJORA CONTINUA

Esta fase le permitirá a la Entidad, consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI.

Gráfica 7 - Fase de mejoramiento continuo
Fuente: MINTIC – 2017

3 ESTRATEGIA METODOLOGICA

El modelo de Arquitectura de Seguridad de la Información seleccionado es el Modelo de Seguridad y Privacidad de la Información del MINTIC, para dar cumplimiento con lo establecido en Gobierno Digital. A continuación, se desarrolla para la entidad gubernamental CRC.

3.1 Fase 1 – ETAPA DE DIAGNOSTICO

3.1.1 Marco metodológico para encontrar el nivel de Madurez.

Se utiliza una metodología que permite evaluar el nivel de madurez de la CRC respecto a los lineamiento y guías de la estrategia de Gobierno en línea, para la cual se describe a continuación.

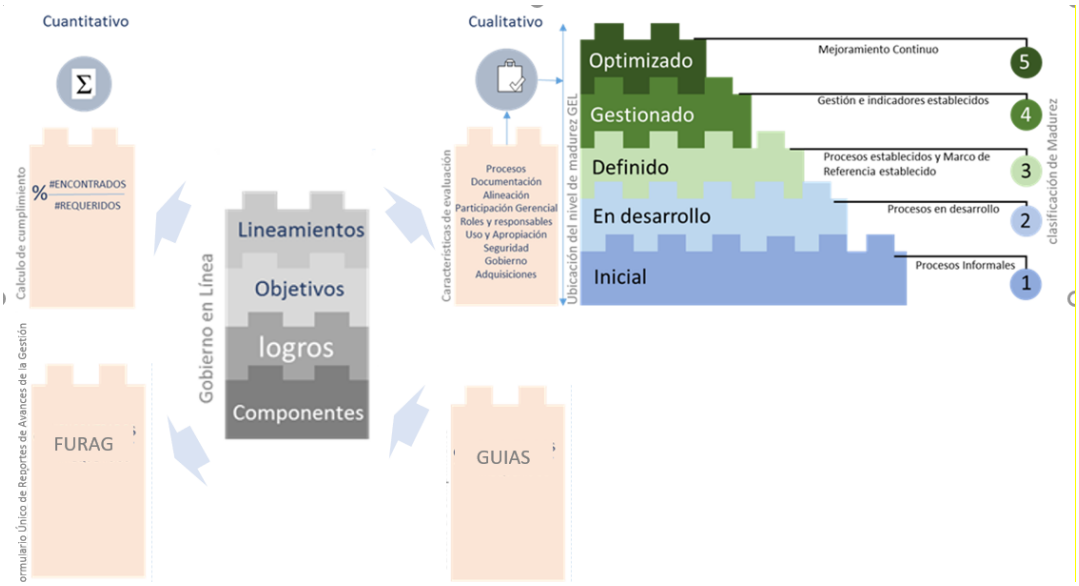
Las actividades aplicadas para la etapa de evaluación de cada uno de los componentes de Gobierno en Línea se han enmarcado dentro de las mejores prácticas de arquitectura empresarial y utilizando diferentes instrumentos sugeridos por los marcos más utilizados. Para este caso, se ha utilizado el marco de referencia del Open Group, The Open Group Architecture Framework, en su versión 9.1 (TOGAF 9.1), que en su base de recursos respecto a los niveles de madurez, hace referencia a diferentes modelos de evaluación, como las del Instituto de Ingeniería conocido por su nombre en inglés como “Software Engineering Institute” (SEI) , el cual orienta las evaluaciones a los productos de software por medio del Modelo de Madurez de Capacidad de Software SW-CMM. De otro lado se cita en el mismo marco el modelo el Modelo de madurez de integración o Capability Maturity Model Integration por sus siglas en inglés (CMMI), adaptación del modelo generado por el SEI Institute.

Dentro de las adaptaciones mencionadas el departamento de comercio de los Estados Unidos (DoC), ha desarrollado un modelo de madurez de capacidad de arquitectura, (ACCM) el cual contempla tres aspectos de evaluación como son: el modelo de madurez de la arquitectura de IT, las características de unidades operativas de procesos, y un modelo de medición de la capacidad de arquitectura.

Por lo anterior la metodología aplicada toma como base el modelo de madurez de capacidad de arquitectura empresarial del departamento de comercio de los Estados Unidos, aplicada sobre el Marco de Referencia para la Gestión de TI del Gobierno Colombiano, principal habilitador de la Estrategia de Gobierno en Línea.

Se realizó la evaluación de la Estrategia de Gobierno en Línea con cada componente y sus divisiones, teniendo en cuenta siete criterios y ubicando cada uno de estos sobre un nivel de madurez de cinco niveles.

La siguiente gráfica muestra la metodología aplicada al capítulo de diagnóstico donde explica que basado en el cumplimiento de los lineamientos de Gobierno en línea sus guías y el Furag, se realiza una evaluación cuantitativa y cualitativa de la CRC con respecto a su cumplimiento.



Gráfica 8 - Metodología diagnóstico Gobierno en Línea CRC

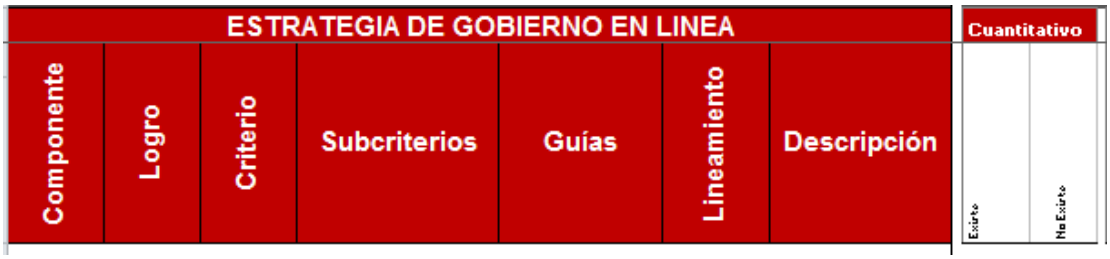
con la aplicación de esta metodología, se realiza el estimado sobre el nivel de madurez correcto en una evaluación holística de las siguientes siete características: Procesos, documentación y estándares, alineación con la estrategia, participación gerencial, definición de roles y responsabilidades, uso y apropiación, e incorporación componente de seguridad.

3.1.2 Metodología aplicada, evaluación cuantitativa y cualitativa.

La metodología aplicada se hace teniendo en cuenta una evaluación cuantitativa y una evaluación cualitativa que se definen dentro de los siguientes aspectos:

a) La evaluación cuantitativa de cumplimiento a nivel de lineamientos se realiza contra los requisitos de Gobierno en Línea (GEL) y sus guías, la cual independiente del grado de calidad de las características inherentes a cada lineamiento, define el nivel de cumplimiento. Corresponde al número de lineamientos cumplidos respecto a los

requeridos por Gobierno en Línea el cual nos permite calcular el "índice de cumplimiento cuantitativo", de acuerdo con la información entregada por la Entidad. Ver gráfica:



Gráfica 9 - Plantilla para la evaluación cuantitativa

b) La evaluación cualitativa que contiene el resultado del avance de la madurez y se obtiene de la revisión de los insumos descritos en el presente informe, contra lo requerido por los lineamientos de GEL y las guías para la evaluación cualitativa se realiza lo siguiente:

   i. Calificación individual de los lineamientos sobre las siete (7) características de evaluación, asignando el nivel de madurez del uno (1) al (5). Para las características de evaluación que no apliquen se determinará un valor de 5 con el fin de no afectar la calificación final.

   ii. Cálculo promedio de la calificación otorgada, determinando así el nivel de madurez en el que se encuentra el lineamiento que van desde inicial (1), en desarrollo (2), definido (3), Gestionado (4) y optimizado (5).

   iii. Con los resultados se calcula el cumplimiento porcentual cualitativo para cada lineamiento, y para cada componente, esto es para el objetivo, criterio, y el logro.

   iv. Los resultados determinarán la brecha porcentual como base para determinar las actividades necesarias para cubrir estas brechas. (Ver Gráfica)

Gráfica 10- Plantilla para la evaluación cualitativa

c) Obtenidas las evaluaciones cuantitativas y cualitativas, se describe la evaluación por logro especificado y se determinan las brechas individuales encontradas respecto a lo requerido por Gobierno en Línea (GEL), teniendo en cuenta las actividades relacionadas en el contrato que permite mejorar el cumplimiento de los indicadores de Gobierno en línea.

d) Las brechas se consolidan y se describen al final de la evaluación, las cuales representarán las bases del desarrollo de la siguiente fase, para aplicar los ejercicios que describirán la transformación y determinarán las hojas de ruta de implementación.

3.2 Fase 2: PLANIFICACIÓN

3.2.1 Establecimiento de la situación actual con base en un análisis de riesgos - Actividades Seguridad y Privacidad de la Información

Criterio	Alcance	Actividades
Seguridad y Privacidad de la Información	Documentar el nivel de madurez de ipv6 y road map de las fases de transición, realizando el inventario de hardware y software, la identificación de la topología actual de la red, relacionar los equipos de computación y de comunicaciones que soportan ipv6 y considerando las recomendaciones de las guías de adopción y aseguramiento emitidas por MINTIC	Establecer los elementos de hardware y software de la Entidad para determinar el grado de compatibilidad de la plataforma tecnológica actual con el protocolo IPv6. Identificar la topología actual de la red de la Entidad para determinar el grado de compatibilidad de la plataforma tecnológica actual con el protocolo IPv6. Establecer la relación de los equipos de computación y de comunicaciones que soportan IPv6 (IPv6-ready o IPv6-web) de la Entidad para determinar el grado de compatibilidad de la plataforma tecnológica actual con el protocolo IPv6. Realizar una evaluación de nivel de madurez de los servicios de operación con respecto a la compatibilidad de la plataforma tecnológica actual con el protocolo IPv6. Generar plan de migración de la infraestructura tecnológica de la CRC al protocolo IPv6
	Levantamiento de activos para los procesos seleccionados. Actualización de la matriz de riesgos de la CRC para los procesos seleccionados.	Inventario de activos: Entrevistas y documentación existente de los procesos de Servicios Tecnológicos y de Sistemas de Información: inventarios de activos, levantamiento de información de los activos actuales, su criticidad, valoración y clasificación. Áreas usuarias de los servicios tecnológicos y de sistemas de información (Planeación Estratégica, Atención al cliente y Relacionamiento con agentes, Gestión administrativa y financiera, Asesoría Jurídica y Solución de Controversias, Diseño Regulatorio y Capital Humano): Información manejada en cada sistema de información, valoración y clasificación del activo de información.
	Levantamiento de activos para los procesos seleccionados. Actualización de la matriz de riesgos de la CRC para los procesos seleccionados.	Actualización de la matriz de riesgos: Entrevistas y documentación existente de la Coordinación Sistema de Gestión Integrado: Matriz de riesgos existente en la entidad. Entrevistas y documentación existente de los procesos de Servicios Tecnológicos y de Sistemas de Información: Riesgos de seguridad en los procesos de Servicios Tecnológicos y de Sistemas de Información. Imágenes del módulo de riesgos de la herramienta de sistema de gestión integrado - Global Suite. Verificación de los riesgos de seguridad identificados, análisis y valoración (controles y acciones preventivas).

Criterio	Alcance	Actividades Realizadas
Definición del Marco de Seguridad Y Privacidad de la Entidad	Diagnóstico de seguridad y privacidad Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la CRC. Identificar el nivel de madurez de seguridad y privacidad de la información en la CRC.	Recolección y validación de la información para SGSI de la CRC, en la Coordinación de Tecnología y Sistemas de Información, en los Procesos: Sistemas de Información, Servicios Tecnológicos, y Estrategia Gobierno – Seguridad GEL/Controller, esta fase se desarrolló en sesiones de trabajo, sensibilización a los funcionarios y elaboración de encuestas. Se construyó una matriz en la cual se evidencia los cuatro marcos de referencia: MSPI, ISO 27001, FURAG y la NIST y en qué estado se encuentra toda la documentación necesaria para la implementación de un SGSI: Requisito, política, guía, plan, metodología, procedimientos entre otros, teniendo en cuenta las dependencias, responsables, cargo, para así poder llevar un control de la implementación del SGSI en la CRC, siendo uno de insumos para el diligenciamiento y análisis de la herramienta de diagnóstico del MINTIC y del método de diagnóstico por lineamientos, para conocer la estado actual e identificación del nivel de madurez de SPI de la CRC.

Tabla 1 - Planeación de SPI

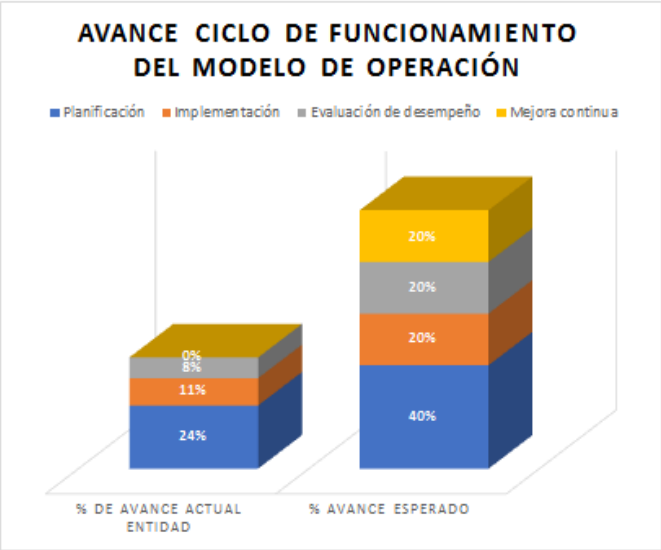
3.2.2 Diagnostico Seguridad y Privacidad de la Información.

A continuación, se presenta el diagnóstico del componente de Seguridad y Privacidad de la Información teniendo como base la metodología mencionada en la Fase 1 y por lineamientos del marco de referencia de Arquitectura de TI de MinTic.

Presentación de resultados del documento diagnóstico de MinTIC del Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo representa el avance anual del ciclo PHVA del componente de seguridad y privacidad de la información decreto 1078 de 2015 que específica, el cumplimiento que deben tener las entidades nacionales y territoriales como se evidencia en la siguiente gráfica.

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	24%	40%
2016	Implementación	11%	20%
2017	Evaluación de desempeño	8%	20%
2018	Mejora continua	0%	20%
TOTAL		43%	100%

Gráfica 11 - Modelo MSPI de MinTIC.



Gráfica 12- Resultado de avance Ciclo de Funcionamiento del Modelo de Operación (PHVA) del MSPI en la CRC.

Componente de Seguridad y Privacidad de la Información	**Análisis instrumento diagnóstico**
Objetivo 1: Planear SGSI	**PHVA**
	24%
EVALUCIÓN	
La CRC ha realizado avances en la implementación del Componente de Seguridad de la Información, políticas, procesos y procedimientos de TI, de igual forma se efectuó el diagnóstico del estado actual de la CRC, frente a la fase de planeación con un avance del 24 %., referentes al ciclo PHVA con la herramienta oficial del MSPI. Fase inicial de la implementación de SGSI. La CRC debe gestionar las políticas complementaras del SGSI.	
BRECHAS IDENTIFICADAS	
ID	**Descripción brecha identificada**
01	El inicio y desarrollo de la implementación del SGSI al ser de toda la CRC es un trabajo conjunto, por lo que se necesita que la alta dirección este apoyando, acompañando y avalando este proceso y los compromisos de las coordinaciones, dependencias, funcionarios y contratistas.
02	Se debe realzar levantamiento de información, procedimiento, ejecución y resultado de pruebas de efectividad. y análisis de vulnerabilidad de los Sistemas de Información de la CRC.
04	Priorizar e Implementar políticas complementarias del SGSI de la CRC con sus respectivos procedimientos.
08	Todo sistema de gestión de seguridad requiere jornadas de capacitación y concientización.
09	Se debe integrar el MSPI con el SGD

19	Documento análisis y evaluación de riesgos SGSI de la CRC.
22	Se debe tener un documento del plan de implementación del sistema de gestión de seguridad de la información, guía paso a paso del desarrollo del SGSI de la CRC.
23	Se debe crear la Política teniendo en cuenta competencias, privilegios de los usuarios de la red de la CRC.
29	Elaborar documento Nomograma legal de cumplimiento de SGSI de la CRC.
33	Política de control de acceso

Tabla 2 - Resultado Detallado - Planear

Componente de Seguridad y Privacidad de la Información	**Análisis instrumento diagnóstico**
Objetivo 2: Hacer	**PHVA**
	11 %

EVALUCIÓN

La CRC debe seguir construyendo los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de los activos de la información de conformidad con su valoración y clasificación, para su formalización, estos se recomiendan que se alineen con políticas complementarias, efectuando el ciclo que se debe realizar para su aprobación.

Se Finalizó la identificación, valoración, clasificación, análisis de riesgos de los dos procesos de la Coordinación de Tecnología de la Información, Sistemas de Información, Servicios Tecnológico, se debe realizar en Gobierno de TI, para completar esta Coordinación.
Este proceso de SPI se debe tener en cuenta para realizarse en todos los procesos de la CRC.
Se debe Imprentar, comunicar, sensibilizar y formalizar procedimientos documentos, como el de atención a incidentes de Seguridad de la Información, devolución de activos, medios removibles, anexo técnico ISO 27001, documento con la metodología de análisis y evaluación de riesgos. Entre otros.

BRECHAS IDENTIFICADAS

ID	**Descripción brecha identificada**
05	Continuar realizando la identificación valoración y clasificación de los activos en función a seguridad de la información de la CRC.
07	Se debe crear un procedimiento de manejo de seguridad con la colaboración del área de comunicación.
10	Imprentar y formalizar el procedimiento de atención a incidentes de Seguridad de la Información
11	Implementar y formalizar el Procedimiento de asignación y devolución de activos a funcionarios, contratistas y/o terceros

12	Es necesario formalizar acuerdo de confidencialidad funcionarios, contratistas personas naturales y jurídicas
13	Se deben construir Procedimientos para el manejo, procesamiento, almacenamiento y comunicación de los activos de información de conformidad con su valoración y clasificación.
14	Procedimiento para la gestión de medios removibles.
15	Procedimiento de Borrado Seguro.
16	Continuar con el proceso de implementación del SGSI, en la Coordinación de Tecnología y Sistemas de Información y seguir con los otros procesos de la CRC.
17	Elaborar plan de implementación de IPv6 en la CRC, aprobado por la Coordinación de Tecnología y Sistemas de Información.
18	Documento con la metodología de análisis y evaluación de riesgos.
19	Documento con el análisis y evaluación de riesgos del SGSI de la CRC.
21	Documento con la declaración de aplicabilidad de la CRC.
29	Documento Nomograma legal de cumplimiento de SGSI de la CRC.
30	Procedimiento legal propiedad intelectual de la información de la CRC.
31	Procedimiento Privacidad de los datos personales y privacidad de la información ley 1581 1377 de la CRC.
32	Procedimiento Acuerdo de Niveles de Servicio para contratistas proveedores SLA, de la CRC.
34	Control de acceso a códigos fuente de programas de la CRC.
36	Implementar Políticas y procedimientos del Anexo técnico de la ISO 27001

Tabla 3- Resultado Detallado - Hacer

Componente de Seguridad y Privacidad de la Información	**Análisis instrumento diagnóstico**
Objetivo 3: VERIFICAR	**PHVA**
	8 %
EVALUCIÓN	
La CRC debe realizar la revisión y verificación de los procedimientos que se están formalizados: Política y Manual de Seguridad de la información, activos de información, y todos los procedimientos del anexo técnico de desarrollo. Construir e implementar el documento: Definición de indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI de la CRC es eficiente, eficaz y efectiva.	
BRECHAS IDENTIFICADAS	

ID	Descripción brecha identificada
03	Revisar y evaluar la Política y Manual de Seguridad de la Información de la CRC de forma periódica.
06	Efectuar revisión y monitoreo de los activos de información
24	Documento Definición de indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI de la CRC es eficiente, eficaz y efectiva.

Tabla 4- Resultado Detallado - Verificar.

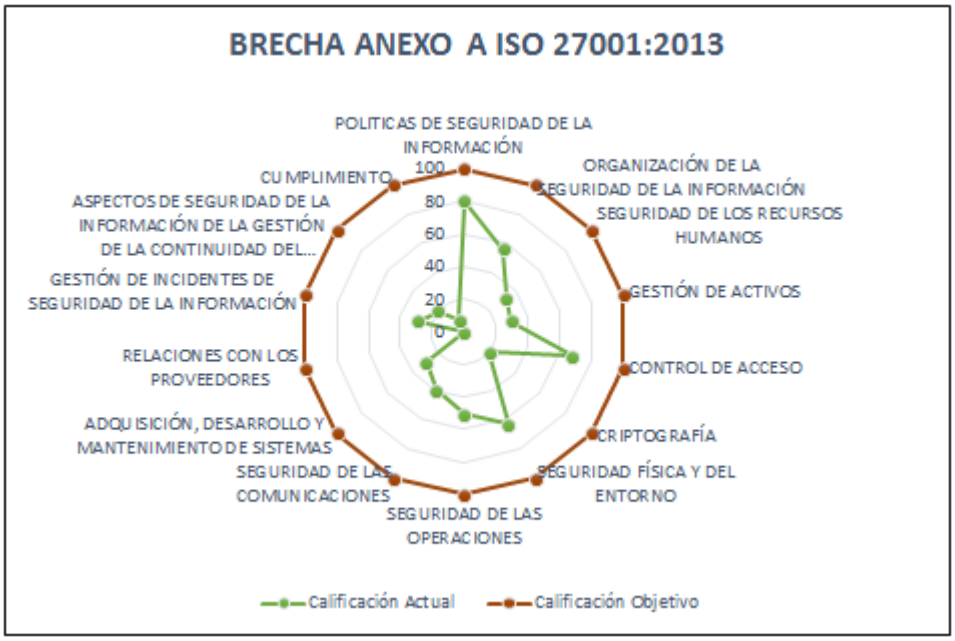
Componente de Seguridad y Privacidad de la Información	Análisis instrumento diagnóstico
Objetivo 4: ACTUAR	**PHVA**
	0 %
EVALUCIÓN	
La CRC debe en su proceso de implementación del SGSI elaborar el plan de ejecución de auditorías y revisiones independientes al MSPI revisado y aprobado por la Alta Dirección, plan de mejora continua, Plan de Continuidad de Negocio BCP y el Análisis de Impacto de Negocio BIA de la CRC.	
BRECHAS IDENTIFICADAS	
ID	**Descripción brecha identificada**
25	Elaborar el plan ejecución de auditorías y revisiones independientes al MSPI revisado y aprobado por la Alta Dirección.
26	Elaborar plan de mejora continua, revisados y aprobados por la Alta Dirección de la entidad de la CRC.
27	Elaborar Plan de Continuidad de Negocio BCP de la CRC.
28	Elaborar documento Análisis de Impacto de Negocio BIA de la CRC.

Tabla 5 - Resultado Detallado - Actuar.

3.2.3 Resultados Evaluación de Efectividad de Controles - ISO 27001:2013.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	56	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	33	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	30	100	REPETIBLE
A.9	CONTROL DE ACCESO	68	100	GESTIONADO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	63	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	51	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	40	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	30	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	29	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
A.18	CUMPLIMIENTO	7,5	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		38	100	REPETIBLE

Gráfica 13- Evaluación de Efectividad de Controles - ISO 27001:2013



Gráfica 14 - Evaluación de Efectividad de Controles gráfica - Anexo a ISO 2001:2013 del MSPI.

Componente de Seguridad y Privacidad de la Información	Análisis instrumento diagnóstico MSPI
Objetivo 4: Brecha Anexo A ISO 27001:2013	**ISO 27001**
	38%
EVALUCIÓN	
La CRC ha realizado gestiones relacionadas con los procesos y procedimientos de Seguridad de la Información, frente a la Brecha anexo ISO 27001:2013, se encuentra en un estado inicial del 38% debido a que se encuentra en el proceso de implementación del SGSI en la Entidad.	

Los Anexos: A5 Política de Seguridad de la Información 80 - 100 A9 Control de acceso 68 – 100 A11 Seguridad Física y del Entorno 63 – 100 En la evaluación efectiva del control se encuentra en un nivel de administración Gestionado. **Los Anexos:** A10 Criptografía 20 - 100 Inicial A17 Aspectos de Seguridad de la Información de la gestión de Continuidad de Negocio 20 -100 Inicial A18 Cumplimiento 7,5 -100 Inicial *Estos anexos se encuentran en una fase inicial los que significa que han realizado acciones, pero hay que seguir gestionándolas.* **Los Anexos:** A7 Seguridad de Recursos Humanos 33 -100 Repetible A8 Gestión de Activos 30 - 100 Repetible A13 Seguridad de las Comunicaciones 40 -100 Repetible A14 Adquisición, desarrollo y Mantenimiento de Sistemas 30-100 Repetible A16 Gestión de Incidentes de Seguridad de la Información 29 -100 Repetible *Estos anexos se encuentran en una fase con un nivel de gestión repetible en la que hay que impulsar y reforzar para seguir gestionándolos.* **El Anexo:** A6 Organización de La seguridad de la Información 56 - 100 Efectivo A12 Seguridad de las operaciones 51 – 100 Efectivo *Este anexo se encuentra en una fase con un nivel de gestión efectivo lo que quiere decir que se están Administrando.* **El Anexo:** A15 Relación con los proveedores 0 – 100 Inexistente *Este anexo se encuentra en una fase con un nivel de gestión inexistente - sin gestión.*
BRECHAS IDENTIFICADAS
ID | **Descripción brecha identificada**
01-02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
En este se encuentran incluidos todas brechas que contribuirán al cumplimiento de Anexo A de la ISO 27001:2013.

Tabla 6- Análisis - Brecha Anexo A ISO 27001:2013

3.2.4 Nivel de Madurez Modelo Seguridad y Privacidad de la Información.

Gráfica 15- Nivel de Madurez MSPI

Componente de Seguridad y Privacidad de la Información		**Análisis instrumento diagnóstico MSPI**	
Objetivo 5: NIVEL DE MADUREZ MSPI		**Inicial**	**Repetible**
		SUFICIENTE	**INTERMEDIO**
EVALUCIÓN			
La CRC en el Nivel de Madurez del MSPI se encuentra en el nivel inicial **SUFICIENTE** Del 71 al 100%, significa que ya está en el proceso de levantamiento de activos de información identificados y valorados, con análisis de riesgo teniendo en cuenta la triada de la seguridad de la información confidencialidad, integridad y disponibilidad. La CRC está ubicada en el Nivel Repetible **INTERMEDIO** del 36 al 70% donde existen procesos básicos de gestión de seguridad de la información, aplicando controles que permiten minimizar los riesgos y se está iniciando el proceso de planificación en la implementación del MSPI de la Entidad, caracterizando los procesos y los sistemas de información.			
BRECHAS IDENTIFICADAS			
ID	**Descripción brecha identificada**		
01-02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36			
En este se encuentran incluidas todas brechas que aportaran al avance y desarrollo del Nivel de Madurez del MSPI de la CRC.			

Tabla 7- Análisis del Nivel de madurez MSPI

3.2.5 Calificación Frente a las Mejores Prácticas de Ciberseguridad (NIST) del MSPI.

A continuación, se relaciona la tabla de calificación frente a las mejores prácticas de ciberseguridad (NIST) del MSPI

CALIFICACIÓN FRENTE A LAS MEJORES PRÁCTICAS DE CIBERSEGURIDAD (NIST) DEL MSPI.	

• **Identificar**
  • Gestión de activos
  • Ambiente de negocios
  • Evaluación de riesgos
  • Estrategia de gestión de riesgos
	

• **Proteger**
  • Control de acceso
  • Capacitación y sensibilización
  • Seguridad datos
  • Protección información y procedimientos
  • Mantenimiento
  • Tecnología de protección
	

• **Detectar**
  • Anomalías y eventos
  • Monitoreo continuo de la seguridad
  • Proceso de detección
	

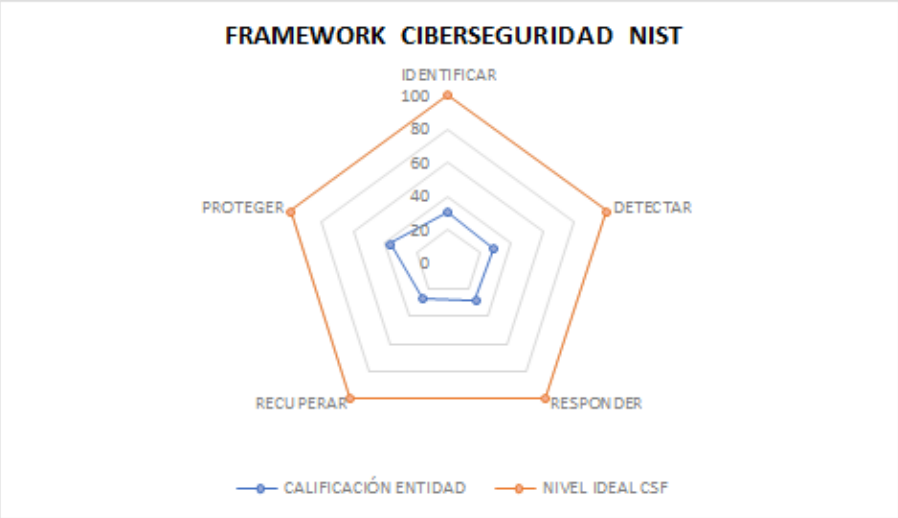
• **Responder**
  • Planes de respuesta
  • Comunicaciones
  • Análisis
  • Mitigación
  • Mejoras
	

• **Recuperarse**
  • Planes de recuperación
  • Mejoras
  • Comunicaciones
	

Tabla 8- Resultado calificación de Ciberseguridad

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	31	100
DETECTAR	29	100
RESPONDER	28	100
RECUPERAR	27	100
PROTEGER	37	100

Gráfica 16 - Calificación - Modelo Framework Ciberseguridad NIST Instrumento Diagnóstico MSPI.



Gráfica 17 . Resultados - Modelo Framework Ciberseguridad NIST Instrumento Diagnóstico MSPI.

Componente de Seguridad y Privacidad de la Información	**Análisis instrumento diagnóstico MSPI**
Objetivo 6: Resultados Calificación Frente a las Mejores Prácticas de Ciberseguridad (NIST) del MSPI, relacionados en la gráfica.	**Promedio**
	30%
EVALUCIÓN	
La CRC en el Modelo Framework Ciberseguridad NIST del MSPI tiene un promedio del 30% teniendo en cuenta los criterios evaluados (identificar, detectar, responder, recuperar y proteger) con respecto al 100% requerido lo que significa que se encuentra en la etapa inicial. En la fase de PROTEGER se encuentra en una posición superior a las otras de 37% es decir; existen acciones actuales que garantizan la protección de la información y de los sistemas de información de la CRC. La meta debe ser, aumentar el crecimiento proporcional de cada una de las fases, y se recomienda la importancia de tener en cuenta la fase de **detectar** como prevención a la materialización de riesgos de la Entidad.	
BRECHAS IDENTIFICADAS	
ID	**Descripción brecha identificada**

01-02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
En este se encuentran también incluidas todas brechas que deben tener las Mejores Prácticas de Ciberseguridad (NIST), que contribuirán a la implementación de MSPI de la CRC.

Tabla 9 - Análisis del MSPI

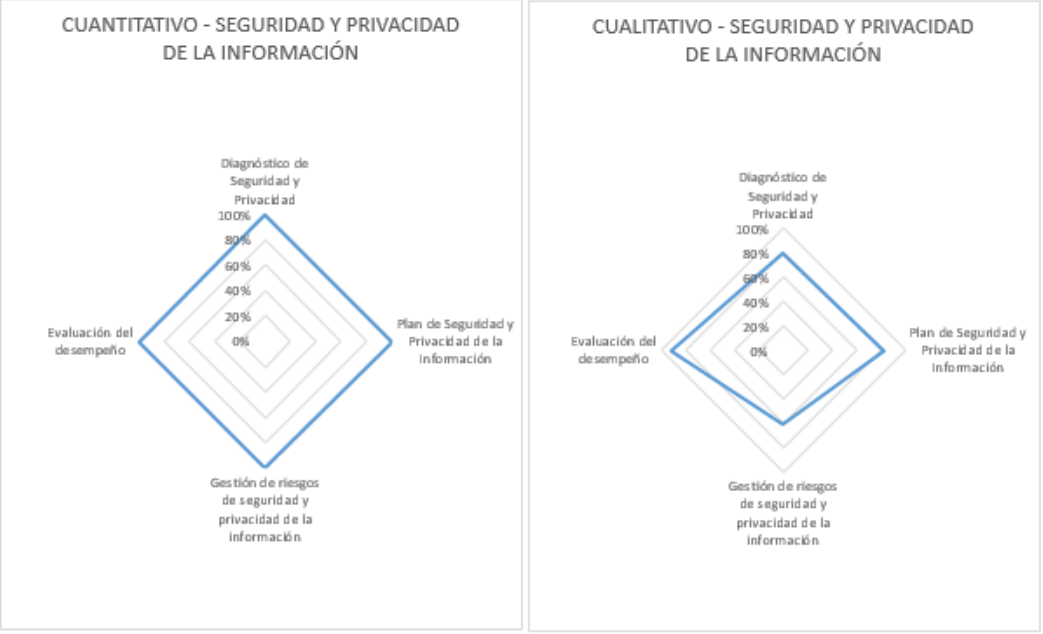
3.2.6 Resultado del Análisis del Componente de Seguridad y Privacidad de la información por Lineamientos

Criterio	Análisis Cuantitativo					Análisis Cualitativo	
	N.L	N.E.	F	% E	% F	% C	% X.C
Diagnóstico de Seguridad y Privacidad	5	5	0	100%	0%	80%	20%
Plan de Seguridad y Privacidad de la Información	7	7	0	100%	0%	83%	17%
Gestión de riesgos de seguridad y privacidad de la información	2	2	0	100%	0%	60%	40%
Evaluación del desempeño	4	4	0	100%	0%	91%	9%
Cumplimiento de Seguridad y Privacidad de la Información	**18**	**18**	**0**	100%	**0%**	**79%**	**21%**

Tabla 10 - Seguridad y Privacidad de la Información

3.2.7 Resultados cuantitativos y cualitativos por criterios del Análisis del Componente de Seguridad y Privacidad de la información por Lineamientos.

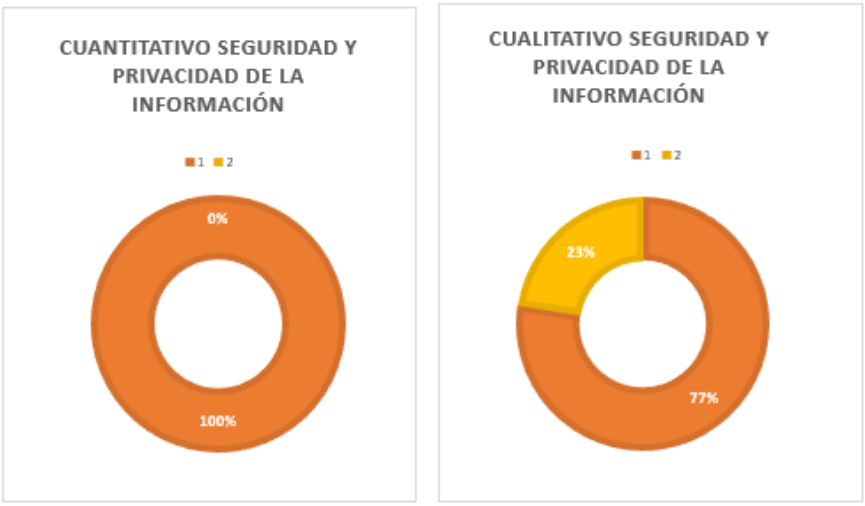
Los resultados individuales por criterio se ilustran en las siguientes gráficas.



Gráfica 18- CUMPLIMIENTO LOGROS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.2.8 Resultados consolidados del Análisis del Componente de Seguridad y Privacidad de la información por Lineamientos.

Los resultados consolidados a nivel de porcentaje del *Análisis del Componente de Seguridad y Privacidad de la información por Lineamientos*.



Gráfica 19- Resultados cuantitativos y cualitativos del Análisis del Componente de Seguridad y Privacidad de la información por Lineamientos

3.2.9 Resultados detallados del Análisis del Componente de Seguridad y Privacidad de la información por Lineamientos.

Los resultados generales están soportados en el diagnóstico individual de los objetivos. El resultado para cada uno de los objetivos para el logro de uso y apropiación, se describe en las siguientes tablas.

Componente de Seguridad y Privacidad de la Información	**Análisis Diagnóstico por Lineamientos GEL**	
Objetivo 5: ANALISIS DEL COMPONENTE DE SEGURIDAD Y PRIVACIDA DE LA INFORMACIÒN POR LINEAMIENTOS DE GEL	**Cuantitativo**	**Cualitativo**
	100%	**77%**
EVALUCIÓN		
La CRC en el Análisis del Componente de Seguridad y Privacidad de la Información, teniendo en cuenta los lineamientos del Marco de Referencia de Arquitectura de TI, valorados por cada uno de sus componentes, ya que SPI no posee lineamientos propios debido a que es un componente transversal.		

De la tabla anterior se concluye que la Entidad tiene un nivel de madurez de SPI cualitativo del 77% resultado de las acciones que se adelantan a partir de los lineamientos que hacen parte de la Estrategia de Gobierno Digital. del total del 100% porcentaje cuantitativo. Para llegar al cumplimiento del 100%, se debe continuar con la implementación el SGSI, a todos los Procesos de la CRC, ya que por parte de la implementación MSPI la Entidad se encuentra en un 43%, esto garantizará la reducción de los riesgos de SPI a que está expuesta la información de crítica de la Entidad, tomando como referencia el Modelo de Seguridad y Privacidad de Información de MINTIC, para esto se debe cerrar todas las brechas identificadas en el diagnóstico, como línea base, para la implementación del ciclo de funcionamiento del modelo de operación del MSPI, (Diagnóstico, Planificación, Implementación Evaluación de Desempeño y Mejora Continua). Se evidencio un incremento del 54% al 77% de la evaluación inicial realizada por la CRC, lo que concluye un avance significativo en el Marco de Referencia de Arquitectura de TI de GEL.
BRECHAS IDENTIFICADAS
ID — **Descripción brecha identificada**
01-02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
En este se encuentran incluidas todas las brechas que aportaran a la implementación del MSPI del MSPI de la CRC.

Tabla 11- Resultados detallados de Seguridad y Privacidad de la Información

3.3 Fase 3: Análisis de la brecha existente entre la situación actual y la de referencia

Se determinan acciones requeridas, recursos y costos.

ID	Brecha	Descripción (cambio)	Solución	Interesado Sugerido
1	Se debe generar compromiso, apoyo por parte de la alta Dirección, coordinaciones, dependencias, funcionarios y contratistas en el inicio y desarrollo de la implementación del SGSI de la CRC.	El inicio y desarrollo de la implementación del SGSI al ser de todo CRC es un trabajo conjunto, por lo que se necesita que la alta dirección este apoye, acompañe y avale este proceso y los compromisos de las coordinaciones, dependencias, funcionarios y contratistas.	Generar un documento firmado por la alta Dirección o Coordinación administrativa, en la que se establezcan los compromisos de la alta dirección, coordinaciones, dependencias, funcionarios y contratistas en el inicio y desarrollo de la implementación del SGSI de la CRC.	Coordinación de Tecnología y Sistemas de Información. Oficial de Seguridad de la Información. Comité de Seguridad de la Información. Dirección. Coordinaciones. Dependencias. Funcionarios Contratistas
2	Se debe realizar pruebas de efectividad y análisis de vulnerabilidad de los Sistemas de Información de forma periódica, formulando sus acciones correctivas.	Se debe realzar levantamiento de información, procedimiento, ejecución y resultado de pruebas de efectividad. y análisis de vulnerabilidad de los Sistemas de Información de la CRC.	Documento levantamiento de información, procedimiento, ejecución y resultado de Pruebas de Efectividad. Documento y procedimiento de análisis de Vulnerabilidades de la entidad.	Coordinación de Tecnología y Sistemas de Información. Oficial de Seguridad de la Información. Comité de Seguridad de la Información.

ID	Brecha	Descripción (cambio)	Solución	Interesado Sugerido
3	Revisar y evaluar la Política y Manual de Seguridad de la Información de la CRC de forma periódica y continua.	Revisar y evaluar la Política y Manual de Seguridad de la Información de la CRC de forma periódica.	Documento con la revisión y evaluación de la Política y Manual de Seguridad de la Información de la CRC de forma periódica, teniendo en cuenta los procesos para manejar las desviaciones y las excepciones, realizando las modificaciones correspondientes.	Coordinación de Tecnología y Sistemas de Información. Oficial de Seguridad de la Información. Comité de Seguridad de la Información.
4	Es necesario priorizar e implementar las políticas complementarias del SGSI de la CRC con sus respectivos procedimientos.	Priorizar e Implementar políticas complementarias del SGSI de la CRC con sus respectivos procedimientos.	Políticas y Procedimientos, debidamente documentados, socializados y aprobados por el Comité de Seguridad de la Información y la Dirección de la CRC.	Coordinación de Tecnología y Sistemas de Información. Oficial de Seguridad de la Información. Comité de Seguridad de la Información.
5	Seguir realizando la identificación valoración y clasificación de los activos en función a seguridad de la información de la CRC.	Identificación valoración y clasificación de activos de seguridad de la información en todos los procesos de la CRC.	Continuar con el proceso de implementación del SGSI en todos los procesos de la CRC. Identificación valoración y clasificación de activos de seguridad de la información de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
6	Revisión y monitoreo de los activos de información	Realizar seguimiento y monitoreo de los activos de Información	Se debe realizar la revisión periódica de los activos de información esto ayudará a monitorear y actualizar los cambios que de los activos de información de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
7	Creación de normativa de manejo de seguridad con la colaboración del área de comunicación.	Para las labores de divulgación de los avances en implementación del SGSI dentro de la CRC, debe existir una metodología de transformación de la información desde el área de seguridad de la información, con el fin de garantizar la más pronta atención y transferencia de conocimiento en materia de protección a la información.	Crear una normativa con carácter de cumplimiento obligatorio en el que cada reforma en el área de seguridad de la información se debe comunicar por medio de los canales con los que cuenta la CRC	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
8	Es importante diseñar un plan de capacitación actualizado para la enseñanza de seguridad de la información.	Todo sistema de gestión de seguridad requiere jornadas de capacitación y concientización de los involucrados. Para generar una adherencia adecuada entre los funcionarios y directivos, esto propenderá a generar conciencia y colaboración en el manejo de políticas, procedimientos, incidentes y recursos que minimice la	Crear un plan de capacitaciones enfocadas a la implementación y sostenimiento del SGSI de la entidad.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.

ID	Brecha	Descripción (cambio)	Solución	Interesado Sugerido
		pérdida de información o activos.		
9	Se recomienda Integrar el MSPI, con el sistema de gestión documental de la entidad.	Se debe integrar el MSPI con el SGD	Se debe realizar un trabajo en conjunto para la integración de MSPI con el sistema de gestión documental de la CRC	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
10	Formalizar e implementar el procedimiento de atención a incidentes de Seguridad de la Información	Se está construyendo el procedimiento ahora se debe sensibilizar, comunicar y formalizar en la CRC	Continuar con el proceso de formalización de este procedimiento.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
11	Imprentar y formalizar el Procedimiento de asignación y devolución de activos a funcionarios, contratistas y/o terceros	Debe ser integrado este procedimiento con el de ingreso de personal de Talento Humano	Procedimiento integrado implementado y documentado de ingreso de personal con la asignación y devolución de activos.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
12	Se establece la necesidad de formalizar acuerdo de confidencialidad funcionarios, contratistas personas naturales y jurídicas	Los acuerdos de confidencialidad de la información se encuentran dentro del contrato del personal.	Implementación de un acuerdo de confidencialidad específico para cada uno de los funcionarios y contratistas de la CRC; existe para personas jurídicas en TI, se debe formalizar para todos los funcionarios, contratistas y personas jurídicas contratistas de la entidad	Talento Humano Oficial de Seguridad de la Información.
13	Se deben construir Procedimientos para el manejo, procesamiento, almacenamiento y comunicación de los activos de información de conformidad con su valoración y clasificación.	Se deben construir Procedimientos para el manejo, procesamiento, almacenamiento y comunicación de los activos de información de conformidad con su valoración y clasificación.	Elaboración y construcción de procedimiento para el manejo, procesamiento, almacenamiento y comunicación de los activos de información	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información Toda la entidad
14	Procedimiento para la gestión de medios removibles.	Se debe construir Procedimiento para gestión de medios removibles.	Elaboración y construcción Procedimiento para gestión de medios removibles.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información Toda la entidad

ID	Brecha	Descripción (cambio)	Solución	Interesado Sugerido
15	Procedimiento de Borrado Seguro.	Se debe construir procedimiento de Borrado Seguro.	Elaboración y construcción Procedimiento Borrado Seguro.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información Toda la entidad
16	Continuar con el proceso de implementación del SGSI, en la Coordinación de Tecnología y Sistemas de Información y seguir con los otros procesos de la CRC.	Esto teniendo en cuenta el cumplimiento del decreto 2573 de 2014 de MINTIC.	Continuar la Implementación del SGSI Teniendo en cuenta que para el 2018 las entidades nacionales deben estar el cumplimiento en un 100%	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información Toda la entidad.
17	Elaborar plan de implementación de IPv6 en la CRC, aprobado por la Coordinación de Tecnología y Sistemas de Información.	Se realizó el diagnóstico para la transición de IPv4 a IPv6, ahora hay que elaborar el plan de implementación IPv6.	Proyectar el plan de implementación de ipIPv6 en la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información Toda la entidad.
18	Documento con la metodología de análisis y evaluación de riesgos.	Documento donde se explica la metodología del análisis y evaluación de riesgos.	Continuar la Implementación del SGSI en la CRC. Documento donde se explica la metodología del análisis y evaluación de riesgos.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información Toda la entidad.
19	Documento con el análisis y evaluación de riesgos del SGSI de la CRC.	Documento análisis y evaluación de riesgos SGSI de la CRC.	Continuar la Implementación del SGSI en la CRC. Documento análisis y evaluación de riesgos SGSI de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
20	Documento con el plan de tratamiento de riesgos de la CRC.	El plan de tratamiento de riesgos debe ser revisado en intervalos iguales de tiempo para verificar la adaptabilidad a los procesos de la CRC.	Continuar la Implementación del SGSI. Documento con el plan de tratamiento de riesgos de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información Toda la entidad.
21	Documento con la declaración de aplicabilidad de la CRC.	Elaborar la declaración de aplicabilidad en función del levantamiento de activos de información por procesos documentando la omisión de controles y las referencias de documentos de aceptación de riesgos de la CRC.	Continuar la Implementación del SGSI. Documento con la declaración de aplicabilidad de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
22	Plan de implementación del sistema de gestión de seguridad de la información de la CRC.	Se debe tener un documento del plan de implementación del sistema de gestión de seguridad de la información,	Creación del documento plan de implementación del sistema de gestión de	Coordinación de Tecnología y Sistemas de Información.

ID	Brecha	Descripción (cambio)	Solución	Interesado Sugerido
		guía paso a paso del desarrollo del SGSI de la CRC.	seguridad y privacidad de la información de la CRC.	Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
23	Política para administración de usuarios dentro de la red de la CRC.	Se debe crear la Política teniendo en cuenta competencias, privilegios de los usuarios de la red de la CRC.	Crear política de administración de usuarios de la red de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
24	Documento definición de indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI de la CRC es eficiente, eficaz y efectiva.	Definición de indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI.	Documento Definición de indicadores de gestión y cumplimiento que permitan identificar si la implementación del MSPI de la CRC es eficiente, eficaz y efectiva.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
25	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI de la CRC.	Elaborar el plan ejecución de auditorías y revisiones independientes al MSPI revisado y aprobado por la Alta Dirección.	Continuar la Implementación del SGSI. Plan ejecución de auditorías y revisiones independientes al MSPI revisado y aprobado por la Alta Dirección.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
26	Plan de mejora continua, revisado y aprobado por la Alta Dirección de la entidad de la CRC.	Elaborar plan de mejora continua, revisados y aprobados por la Alta Dirección de la entidad de la CRC.	Seguir con la Implementación del SGSI. Plan de mejora continua, revisado y aprobado por la Alta Dirección de la entidad de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
27	Plan de Continuidad de Negocio BCP de la CRC.	Elaborar Plan de Continuidad de Negocio BCP de la CRC.	Continuar la Implementación del SGSI. Plan de Continuidad de Negocio BCP de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
28	Documento Análisis de Impacto de Negocio BIA de la CRC.	Elaborar documento Análisis de Impacto de Negocio BIA de la CRC.	Continuar la Implementación del SGSI. Documento Análisis de Impacto de Negocio BIA de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.

ID	Brecha	Descripción (cambio)	Solución	Interesado Sugerido
29	Documento Normograma legal de cumplimiento de SGSI de la CRC.	Elaborar documento Normograma legal de cumplimiento de SGSI de la CRC.	Continuar la Implementación del SGSI. Documento Normograma legal de cumplimiento de SGSI de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
30	Procedimiento legal propiedad intelectual de la información de la CRC.	Elaborar procedimiento legal propiedad intelectual de la información de la CRC.	Continuar la Implementación del SGSI. Procedimiento legal propiedad intelectual de la información de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
31	Procedimiento Privacidad de los datos personales y privacidad de la información ley 1581 1377 de la CRC.	Procedimiento Privacidad de los datos personales y privacidad de la información ley 1581 1377.	Continuar la Implementación del SGSI. Procedimiento Privacidad de los datos personales y privacidad de la información ley 1581 1377.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
32	Procedimiento Acuerdo de Niveles de Servicio para contratistas proveedores SLA, de la CRC.	Elaborar procedimiento Acuerdo de Niveles de Servicio para contratistas proveedores SLA, de la CRC.	Implementación del SGSI. Procedimiento Acuerdo de Niveles de Servicio para contratistas proveedores SLA, de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
33	Política de control de acceso del SGSI de la CRC.	Política de control de acceso Revisión, Control y Monitoreo Política de control de acceso Uso de programas utilitarios privilegiados. Política de Registro, Privilegios y Cancelación de Usuarios y Contraseñas. Revisión, Control y Monitoreo Política de Registro, Privilegios y Cancelación de Usuarios y Contraseñas. Política y procedimientos acceso a carpetas compartidas. Revisión, Control y Monitoreo Política y procedimiento acceso a carpetas compartidas. Uso de programas utilitarios privilegiados.	Se debe construir las políticas correspondientes a control de acceso monitoreo, uso de programas, usuarios, contraseñas, acceso a carpetas compartidas, a programas privilegiados con sus respectivas revisiones SGSI de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
34	Control de acceso a códigos fuente de programas de la CRC.	Control de acceso a códigos fuente de programas Política sobre el uso de controles criptográficos	Elaborar la política control de acceso de fuentes de programa, uso de controles criptográficos, protección y	Coordinación de Tecnología y Sistemas de Información.

ID	Brecha	Descripción (cambio)	Solución	Interesado Sugerido
		Política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	tiempo de vida de las llaves criptografías de la CRC.	Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
35	Política de seguridad física de la CRC.	Política Perímetro de seguridad física Revisar control físico de acceso con sus directrices Seguridad de oficinas, recintos e instalaciones	Construir, revisa y optimizar los procesos de seguridad física de la CRC.	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.
36	Implementar Políticas y procedimientos del Anexo técnico de la ISO 27001	Principios de construcción de sistemas seguros Ambiente de desarrollo seguro Desarrollo contratado externamente Pruebas de seguridad de sistemas Prueba de aceptación de sistemas Protección de datos de prueba Responsabilidades y procedimientos Reporte de eventos de seguridad de la información Reporte de debilidades de seguridad de la información Evaluación de eventos de seguridad de la información y decisiones sobre ellos Respuesta a incidentes de seguridad de la información Aprendizaje obtenido de los incidentes de seguridad de la información Recolección de evidencia	Implementar Políticas y procedimientos del Anexo técnico de la ISO 27001 Priorizando procedimientos críticos de la entidad	Coordinación de Tecnología y Sistemas de Información. Comité de Seguridad de la Información. Oficial de Seguridad de la Información. Toda la entidad.

Tabla 12- Análisis de Brechas de Seguridad y Privacidad de la Información.

3.4 Fase 4: Elaboración del plan de implantación de la arquitectura de referencia considerando recursos, prioridades e indicadores de control.

La elaboración de este plan facilita la implantación de un Sistema de Gestión de Seguridad de la información (SGSI), ya que basa su desarrollo en el modelo de protección de la información, el mismo que está alineado con el estándar ISO-17799 que describe las mejores prácticas para la Gestión de Seguridad de la Información e ISO-27001 que describe especificaciones para un Sistema de Gestión de Seguridad de la Información (SGSI).

Dicho modelo tiene su centro en la clasificación de la información, la gestión de riesgos y los tres ejes definidos en la arquitectura de seguridad:

- Normativa (Política de seguridad institucional)
- Estructura organizativa (personal capacitado y consciente)
- Infraestructura tecnológica (tecnología controlada)

3.4.1 Hoja de Ruta

Se presenta la hoja de ruta elaborada a partir de brechas agrupadas en paquetes de trabajo que generan la misma capacidad a la Entidad.

PAQUETES DE TRABAJO- SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
ID	**Paquete de Trabajo (nombre unificado de las soluciones)**	**Descripción General**	**Capacidad Entregada**	**Brechas Cubiertas**
01	Documentos de Gestión y Manejo del SGSI de la CRC.	Actas, Normativas, Políticas, planes de auditoria	Gobierno de la Gestión	01 03 04 07 08 20 22 23 25 26 27 33 34 35 36
02	Insumos Manejo de Seguridad de la información del SGSI de la CRC.	Activos, procesos, subprocesos, procedimientos, metodologías, Estándares	Gestión de Seguridad	02 05 06 10 11 12 13 14 15 16 17 18 19 21 24 28 29 30 31 32 34 36
03	Cumplimiento de Normativa Legal Asociada(GEL) del SGSI de la CRC.	Clasificación, Presentación de información a Externos	Cumplimiento Legal	07 16 17 22 29 30 31
04	Instrumentos para gestión de Seguridad de la Información del SGSI de la CRC.	Formatos para documentación de tareas en seguridad	Gobierno de Sistemas de Información	02 05 06 08 10 11 12 13 14 15 16 19 20 21 22 23 24 25 30 31 32 33 35 36

Tabla 13- Paquetes de trabajo de Seguridad y Privacidad de la Información

	ANO 2018		Capacidad
Hoja de Ruta año 2018	Seguridad y Privacidad de la Información	Paquete 01	Gobierno de la Gestión
		Paquete 02	Gestión de seguridad
		Paquete 03	Cumplimiento legal

	ANO 2018		Capacidad
		Paquete 04	Gobierno de sistemas de información

Tabla 14- Implementación 2018

4 CONCLUSIONES

a. Se aplicó la metodología propuesta por el MINTIC para la entidad gubernamental CRC, se realizó el diagnóstico sobre el estado actual iniciando con los Procesos de Sistemas de Información y Servicios Tecnológicos pertenecientes a la Coordinación de Tecnología y Sistemas de Información con respecto a la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, luego de lo cual se plantearon las medidas necesarias, para seguir efectuando la implementación del MSPI en la Entidad.
b. De acuerdo al análisis realizado se encontraron 36 brechas de seguridad y se determinó el plan de implementación.
c. Se diseñaron paquetes de trabajo para el tratamiento de las brechas y se elaboró una hoja de ruta como parte de la implementación de acuerdo a la metodología establecida.

5 RECOMENDACIONES

a. Se recomienda definir e implementar los planes correspondientes para asegurar la calidad de los componentes de información gestionados en la Entidad.
   Crear un esquema de gestión de los componentes de información en la Entidad, que contribuyan a alcanzar los niveles requeridos de seguridad, privacidad y trazabilidad de los componentes de información.

   Definir los procedimientos para la planeación y gestión de los sistemas de información, donde se apliquen las buenas prácticas para la adquisición y/o desarrollo de sistemas de información.

   Implementar mecanismos que contribuyan a la gestión de los derechos y requisitos legales en materia de derechos de autor de la información gestionada a través de los sistemas de información habilitados por la Entidad

b. La CRC debe elaborar un acto administrativo a nivel directivo en el cual, se formalice y se comunique a todos: Directores, coordinadores, funcionarios, contratistas y terceros del proceso que se está efectuando en la CRC, para su conocimiento, disposición y disponibilidad del proceso crítico e importante la Implementación del Sistema de Seguridad y Privacidad de la Información.

c. La CRC debe realizar un plan de concientización, sensibilización y apropiación a toda la Entidad de Seguridad y Privacidad de la Información, en el proceso de implementación que se está realizando a todo nivel: Directivo, coordinaciones, funcionarios, contratitas y terceros, teniendo en cuenta el rol y responsabilidad que tiene cada uno en este proceso integral de la Entidad, esto ayudará a ser más práctico y eficiente el SGSI.
d. La CRC debe realizar una revisión, ajuste y mejora al procedimiento de control de acceso del personal visitante y funcionarios a las instalaciones de la CRC, debido a que se presentan fallas de seguridad de la información; tomando las medidas respectivas, para que a futuro se minimice el riesgo de un incidente de seguridad.
e. Se debe realizar una revisión, ajuste y mejora al procedimiento que tiene la CRC para desarrollo, teniendo en cuenta el MSPI y el anexo técnico y administrativo de la ISO 27001:2013.
f. Se debe efectuar todas las adecuaciones físicas y técnicas con cumplimiento a las normas técnicas vigentes del centro de cómputo y de cableado, se evidencia un riesgo alto de seguridad de la información para la CRC.

6 REFERENCIAS

[1] J. KILLMEYER, Information Security Architecture.

[2] B. IYER y R. GOTTLIEB, The Four-Domain Architecture: An approach to support enterprise architecture design, 2004.

[3] Networking and Security Institute - SANS, Information Systems Security Architecture: A Novel Approach to Layered Protection, Estados Unidos, 2004.

[4] Ministerio de Tecnologías de la Informacion y las Comunicaciones, «Modelo de Seguridad y Privacidad de la Información,» 2016.

[5] Colciencias, «Modelo de Medición de Grupos, de Investigacion, Desarrollo Tecnológico o de Innovación y reconocimiento de investigadores del Sistema Nacional de Ciencia, tecnología e Innovación 2014,» Colciencias, 2014. [En línea]. Available: http://www.colciencias.gov.co/sites/default/files/ckeditor_files/files/DOCUMENTO MEDICI%C3%93N GRUPOS - INVESTIGADORES VERSI%C3%93N FINAL 15 10 2014 (1).pdf. [Último acceso: 01 2015].

7 BIBLIOGRAFIA

[1] J. Killmeyer Tudor, Information Security Architecture. An Integrated Approach to Security in the Organization, CRC Press LLC, 2001.

[2] B. IYER y R. GOTTLIEB, The Four-Domain Architecture: An approach to support enterprise architecture design, 2004.

[3] Networking and Security Institute - SANS, Information Systems Security Architecture: A Novel Approach to Layered Protection, Estados Unidos, 2004.

[4] Ministerio de Tecnologías de la Informacion y las Comunicaciones, «Modelo de Seguridad y Privacidad de la Información,» 2016.

[5] Colciencias, «Modelo de Medición de Grupos, de Investigacion, Desarrollo Tecnológico o de Innovación y reconocimiento de investigadores del Sistema Nacional de Ciencia, tecnología e Innovación 2014,» Colciencias, 2014. [En línea]. Available: http://www.colciencias.gov.co/sites/default/files/ckeditor_files/files/DOCUMENTO MEDICI%C3%93N GRUPOS - INVESTIGADORES VERSI%C3%93N FINAL 15 10 2014 (1).pdf. [Último acceso: 01 2015].

[6] G. Kreizman, «An Introduction to Information Security,» de *Gartner The Future of IT Conference*, Mexico City, Mexico, 2011.