PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFROMACION DE LA CORPORACION SOCIAL DE CUNDINAMARCA

Tabla de Contenido

1. INTRODUCCION

Los lineamientos de a nivel de seguridad y privacidad de la información establecidos por el gobierno nacional en cabeza del Ministerio de tecnologías de información y las comunicaciones – MINTIC para las entidades públicas que involucran las tecnologías de la Información son de carácter globalizador, llevando a que muchas instituciones desarrollen políticas para el uso adecuado de las tecnologías y recomendaciones para aprovechar los recursos disponibles, evitando de esta manera un uso indebido. Es de gran importancia el desarrollo y evolución de sistemas y políticas que generen seguridad en el manejo, control y gestión de la información de la Corporación Social de Cundinamarca, ya que es su activo más valioso y está definido en la legislación colombiana.

La Oficina de Tic, realiza y hace seguimiento al manual de seguridad y privacidad para preservar la confidencialidad, integridad y disponibilidad de los activos de información de la Corporación Social de Cundinamarca, garantizando su buen uso y la privacidad de los datos. Este habilitante Comprende las acciones a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada, además orientado en los lineamientos establecidos en el sistema de gestión de calidad, como un instrumento que concientice a los funcionarios, de la importancia y sensibilidad del manejo de la información, del control de los riesgos asociados, la superación de fallas y debilidades relacionadas, de tal forma que permitan a la Corporación cumplir con su misión y visión.

2. OBJETIVO GENERAL

Especificar las actividades que se desarrollarán como parte del plan de Seguridad y Privacidad de la Información, que permitan implementar las políticas de gobierno digital y los requisitos legales vigentes, y además buscar el aprovechamiento de los servicios tecnológicos y de comunicaciones brindando confiabilidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso con el fin de asegurar su correcta funcionalidad, ofreciendo un nivel de seguridad óptimo que contribuyan al cumplimiento misional de la Corporación Social de Cundinamarca.

3. TERMINOS Y DEFINICIONES

termino	Definición
AJAX	acrónimo de Asynchronous JavaScript And XML (JavaScript asíncrono y XML), es una técnica de desarrollo web para crear aplicaciones interactivas o RIA (Rich Internet Applications). Estas aplicaciones se ejecutan en el cliente, es decir, en el navegador de los usuarios mientras se mantiene la comunicación asíncrona con el servidor en segundo plano. De esta forma es posible realizar cambios sobre las páginas sin necesidad de recargarlas, mejorando la interactividad, velocidad y usabilidad en las aplicaciones.
Base de datos SQL	(por sus siglas en inglés Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar, de forma sencilla, información de bases de datos, así como hacer cambios en ellas.
Bitvise	Es un cliente para administrar y modificar código fuente en programas web.
Copia de seguridad:	Una copia de seguridad, copia de respaldo o backup (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales.
DATADOC	Software desarrollado para el control, la administración y la gestión documental de una entidad.
Direccionamiento IP	Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado

	ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP).
Directorio Activo	Es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red. Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.
Firewall – Trunk	Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. La opción “trunk” – “baúl” canaliza ciertas amenazas a un sitio seguro para después ser analizadas.
Firewall Fortinet	Es un producto que ofrece soluciones de servicios a nivel de seguridad informática con mecanismos de software y hardware. Solución adquirida por la Corporación Social de Cundinamarca.
ISOLUCION	Compañía de tecnología relacionada con el diseño, desarrollo, implementación y soporte de soluciones tecnológicas para los sistemas integrados de gestión y los sistemas de gestión de la Calidad, basados en modelos normativos ISO y sus complementarios.
Lenguaje PHP	Es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico. Fue uno de los primeros lenguajes de programación del lado del servidor que se podían incorporar directamente en el documento HTML en lugar de llamar a un archivo externo que procese los datos. El código es interpretado por un servidor web con un módulo de procesador de PHP que genera la página Web resultante. Puede ser usado en la mayoría de los servidores web al igual que en casi todos los sistemas operativos y plataformas. PHP se considera uno de los lenguajes más flexibles, potentes y de alto rendimiento conocidos hasta el día de hoy.
LITISOFT	Es un sistema que controla los procesos judiciales, desde la presentación de la demanda hasta la terminación del proceso judicial. Tiene parametrizados todos los tipos de proceso y sus

	respectivos trámites por cada jurisdicción: civil, administrativa, penal, laboral y constitucional. Está compuesto por los módulos de: Información jurídica y financiera, control de términos y módulo de reportes.
Modo batch	Se conoce como sistema por lotes (en inglés batch processing), o modo batch, a la ejecución de un programa sin el control o supervisión directa del usuario (que se denomina procesamiento interactivo). Este tipo de programas se caracterizan porque su ejecución no precisa ningún tipo de interacción con el usuario.
Permisos SQL server	Asignar por parte de un administrador de la base de datos, derechos de acceso o restricción a las opciones o información contenida en las tablas de almacenamiento, administración y estructura de los datos contenidos en los servidores de información de la Organización
Segmento DMZ	Llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.
Segmentos de red	Es un conjunto de equipos (computadoras y periféricos) conectados en red. Una red de una organización puede estar compuesta por varios segmentos de red conectados a la LAN principal llamada backbone, que existe para comunicar los segmentos entre sí.
Servidor DHCP	(siglas en inglés de Dynamic Host Configuration Protocol, en español «protocolo de configuración dinámica de host») es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después. Los servidores DHCP administran de forma centralizada direcciones IP e información relacionada y la ofrecen a los clientes automáticamente. Esto permite configurar la red de cliente en un servidor en lugar de hacerlo en cada equipo cliente.
Servidor DNS:	Domain Name System o DNS (en español «Sistema de Nombres de Dominio») es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. El servidor

	DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.
Servidor NTP	Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable. Una solución completa para sincronizar redes de gran tamaño. El servidor de hora combina un reloj de radio basado en GPS con un ordenador de estado sólido Linux incorporado y ofrece una configuración y administración sencillas a través de una interfaz de navegador.
Sistema Operativo Linux	Es un sistema operativo, una gran pieza de software que controla un computador. Es parecido a Microsoft Windows, pero completamente libre. El nombre correcto es GNU/Linux pero "Linux" se usa más. Linux no es el producto de una sola compañía, es el resultado de la contribución de un gran número de compañías y grupos de personas. De hecho, el sistema GNU/Linux es un componente central, el cual se transforma en muchos productos diferentes: las llamadas distribuciones.
Software:	Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación. Se considera que el software es el equipamiento lógico e intangible de un ordenador. En otras palabras, el concepto de software abarca a todas las aplicaciones informáticas, como los procesadores de textos, las planillas de cálculo y los editores de imágenes.
SQL Server Management Studio (SSMS):	Es una aplicación de software de Microsoft que se utiliza para configurar, gestionar y administrar todos los componentes dentro de Microsoft SQL Server. La herramienta incluye tanto los editores de scripts y herramientas de gráficos que trabajan con objetos y características del servidor. Una característica central de SSMS es el explorador de objetos, lo que permite al usuario navegar, seleccionar y actuar sobre alguno de los objetos dentro del servidor.
Switch:	Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de

	un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta. Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Al igual que los puentes, dado que funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local (LAN).
Tiempo real	Un sistema en tiempo real (STR) es aquel sistema digital que interactúa activamente con un entorno con dinámica conocida en relación con sus entradas, salidas y restricciones temporales, para darle un correcto funcionamiento de acuerdo con los conceptos de predictibilidad, estabilidad, controlabilidad y alcanzabilidad. La palabra tiempo significa que el correcto funcionamiento de un sistema depende no sólo del resultado lógico que devuelve la computadora, también depende del tiempo en que se produce ese resultado. La palabra real quiere decir que la reacción de un sistema a eventos externos debe ocurrir durante su evolución. Como una consecuencia, el tiempo del sistema (tiempo interno) debe ser medido usando la misma escala con que se mide el tiempo del ambiente controlado (tiempo externo).
Topología de red	Se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma. En algunos casos, se puede usar la palabra arquitectura en un sentido relajado para hablar a la vez de la disposición física del cableado y de cómo el protocolo considera dicho cableado. Así, en un anillo con un concentrador (unidad de acceso a múltiples estaciones, MAU) podemos decir que tenemos una topología en anillo, o de que se trata de un anillo con topología en estrella. La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.
Usuarios de dominio	Es una cuenta compuesta por nombre y contraseña con el fin de acceder a los diferentes servicios de un servidor o grupo de servidores, redes, carpetas, archivos, información y recursos compartidos para compartir, editar o transferir la gestión digital de la Organización. La cuenta de un usuario del dominio registra toda la información necesaria para su definición, los grupos a los que pertenece el usuario, los derechos y permisos que tiene el

	usuario para utilizar el equipo y la red, así como para tener acceso a sus recursos. En los controladores de dominio de Windows Server, las cuentas de usuario se administran con usuarios y equipos de Active Directory.
VLAN	Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local (los departamentos de una empresa, por ejemplo) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un conmutador de capa 3 y 4). Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.
ZIMBRA:	La suite de colaboración Zimbra (en inglés Zimbra Collaboration Suite o ZCS) es un programa informático colaborativo o Groupware que consta de un servicio de correo electrónico creado por Zimbra Inc. compañía ubicada en San Mateo, California. Posee tanto el componente de servidor como su respectivo cliente.
Información pública	Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.
Internet:	Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.
Intranet:	Es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.
Vulnerabilidad o riesgo de seguridad de la información	Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

4. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

En la Corporación social de Cundinamarca mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada ciudadano y con la necesidad de gestionar la seguridad y privacidad de la información se requiere crear, documentar y socializar las siguientes políticas:

- **Política de seguridad de la información:** Documento en el cual se establecen las indicaciones generales para el manejo de la seguridad de la información dentro de la administración central e institutos centralizados dependientes.
- **Política de privacidad y protección de datos personales:** Documento por el cual se da cumplimiento a la ley 1581 de 2012 y el decreto reglamentario 1377 de 2013 para el manejo de datos personales en la Entidad.

4.1. OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

- Minimizar los riesgos de pérdida, integridad, disponibilidad y confidencialidad de la información y garantizar la continuidad de la información.
- Realizar campaña de cultura en seguridad y privacidad de la información en el año 2021 para los funcionarios, contratistas, terceros, aprendices, practicantes y proveedores de la Entidad.
- Realizar seguimiento al cumplimiento de la política de seguridad, privacidad de información y la protección de datos.
- Mantener un seguimiento al plan de manejo y acceso a la información de la atención al ciudadano.

- Capacitar y socializar los controles de política de seguridad, privacidad de información y la protección de datos.
- Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital de manera integral.
- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información de la corporación
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

5. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Gestión	Actividades	Tareas	Responsables	Programación de tareas (trimestral)			
				1er	2do	3er	4to
Transformación Digital	Identificar los riesgos de seguridad digital y Diseñar los controles de seguridad necesarios para garantizar la seguridad y la protección de los datos personales en el marco de los acuerdos de intercambio de información de la entidad con otros.	Realizar una matriz de riesgos de seguridad de la información para los convenios suscritos por la Entidad cargada en Sistema de Gestión Institucional	**Oficina de Tic**				
	Acompañar a la Entidad en el diseño de lineamientos y controles de seguridad de la información que fortalezcan la implementación de la estrategia de racionalización de trámites y estrategia cero papeles.	Lineamientos de seguridad para la estrategia de cero papeles. Informe de resultados de prueba piloto de seguridad de la información para la estrategia cero papeles. Acompañarla implementación de los controles de seguridad para la estrategia cero papeles.	**Oficina de Tic**				
	Documentar el manual de seguridad de la información para la protección de los datos personales en sistemas de información que realicen tratamiento de datos personales	Actualizar el manual de protección de datos personales para sistemas de información con información de carácter personal	**Oficina de Tic**				
Gestión de Riesgos	Actualización de panorama de riesgos de seguridad digital	Realizar de tratamiento de riesgos de seguridad Digital, cargados en sistema de gestión institucional					
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Realimentación, revisión y verificación de los riesgos identificados (Ajustes)					

	Sensibilización	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación					
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento					
	Mejoramiento	Identificación y actualización de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales.					
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores					
Activos de información	Definir lineamientos para el levantamiento de activos de información	Elaboración metodología e instrumento de levantamiento de activos de información	**Oficina de Tic**				
	Levantamiento Activos de Información	Socializar la guía de activos de Información. Validar activos de información en el instrumento levantado en la vigencia anterior. Identificar nuevos activos de información en cada dependencia. Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	**Oficina de Tic**				

		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información. Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.					
	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación por cada líder de proceso. Consolidar el instrumento de activos de Información. Publicar los instrumentos de activos de información consolidado.	**Oficina de Tic**				
Plan de Cambio y Cultura de Seguridad y Privacidad de la	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI.	**Oficina de Tic**				

Información, Seguridad Digital y continuidad de la operación		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos.					
	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI.	**Oficina de Tic**				
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI.	**Oficina de Tic**				
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	**Oficina de Tic**				
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	**Oficina de Tic**				
Sistema integrado de planeación y gestión	Realizar la actualización del documento de contexto de seguridad de la información institucional	Documento actualizado de contexto de la seguridad de la información	**Oficina de Tic**				
	Diseñar estrategias y controles que permitan la implementación de las políticas de seguridad de la información en los procesos institucionales	Documento de controles de seguridad que soporten las políticas de seguridad de la información institucional. Implementación de controles que soportan las políticas de seguridad institucionales.	**Oficina de Tic**				
	Apoyar el diseño de lineamientos y controles que mejoren los niveles de seguridad de los repositorios de información	Propuesta de estructura de tabla de retención de documentos del sistema de gestión de seguridad de la información.	**Oficina de Tic**				

		Implementación de los ajustes al sistema de gestión documental en la TRD del repositorio documental, una vez aprobados por el Archivo General de la Nación.					
	Elaborar y actualizar los documentos del sistema de gestión de seguridad de la información requeridos por la Norma ISO 27001 y el modelo de seguridad y privacidad de la Información recomendado por el Ministerio de las Tecnologías de la Información y las Comunicaciones	Procedimientos del sistema de gestión de seguridad de la información actualizados	**Oficina de Tic**				
	Realizar la evaluación de la efectividad de los controles de seguridad de la información adoptados por la Entidad para el tratamiento de los riesgos de seguridad Digital	Informe de desempeño de los controles de seguridad de la información	**Oficina de Tic**				
	Recolectar la información necesaria para realizar al cálculo de los indicadores del sistema de gestión de seguridad de la información y realizar el cálculo de dichos indicadores	Ficha de indicadores de seguridad de la información diligenciada	**Oficina de Tic**				
	Apoyar técnicamente la elaboración de una directriz con alcance a todas las entidades del estado para la adopción del rol de oficial de seguridad de la información	Borrador de lineamiento para adopción del rol de oficial de seguridad de la información a nivel de las entidades del estado	**Oficina de Tic**				
Vulnerabilidades	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pentest (Prueba de test de seguridad)	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	**Oficina de Tic**				

	Contratar Análisis de Vulnerabilidades y Pentest	Definir estudios previos y procesos de contratación para realizar el pentest y análisis de vulnerabilidades teniendo en cuenta el alcance y mitología	**Oficina de Tic**				
	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance y la metodología establecida	**Oficina de Tic**				
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis de vulnerabilidades y pentest	**Oficina de Tic**				
Seguridad operativa	Apoyar el diseño e implementación de lineamientos y controles que mejoren los niveles de seguridad de sistemas de información institucionales como Furag III, Sigep II, Suite SIE	Análisis de seguridad para los sistemas de información misionales y recomendaciones.	**Oficina de Tic**				
	Apoyar el diseño y adopción de procedimientos de protección de datos personales para los procesos institucionales y sistemas de información misionales que realicen tratamiento de datos personales.	Procedimientos de seguridad de la información para la protección de información personal gestionada por los sistemas de información institucionales Implementación de controles de seguridad para bases de datos en el registro nacional de bases de datos.	**Oficina de Tic**				
	apoyar las actividades de identificación, mejoramiento e implementación de roles de	Ajuste al procedimiento de administración de usuarios para	**Oficina de Tic**				

	seguridad para los servicios de información de la corporación	roles y privilegios en sistemas de información. Análisis del esquema de roles y privilegios para los sistemas de información y bases de datos gestionadas por la Entidad.					
	Documentar los controles de seguridad de la información que permiten el cumplimento de los requisitos legales en materia de seguridad de la información obligatorios para la Entidad	Plan de implementación de controles de seguridad que soportan los requisitos del Registro Nacional de Bases de datos.	**Oficina de Tic**				
	Identificar vulnerabilidades sobre los sitios web institucionales y formular planes de mejoramiento para realizar su tratamiento.	Realizar la aplicación de Ethical Hacking al portal y micrositios y dar recomendaciones.	**Oficina de Tic**				
	Diseñar y apoyar la adopción de controles y lineamientos de seguridad de la información para la estrategia institucional de teletrabajo.	Lineamientos de seguridad para la estrategia de teletrabajo institucional.	**Oficina de Tic**				
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC	**Oficina de Tic**				
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	**Oficina de Tic**				
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el	**Oficina de Tic**				

		levantamiento de activos de información					

6. BIBLIOGRAFIA

- https://www.mintic.gov.co/portal/inicio/
- https://www.mineducacion.gov.co/1759/w3-article-371073.html?_noredirect=1
- http://csc.gov.co/
- https://www.mintic.gov.co/portal/inicio/74903:Decreto-1008-del-14-de-junio-de-2018
- https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85742