CORANTIOQUIA - Subdirección Administrativa y Financiera Medellín
RESOLUCIÓN
CORPORACIÓN AUTÓNOMA REGIONAL DEL
Fecha: 26-jul-2023 05:13 PM Pág: 2
Anexos: 96 PÁGINAS
Archivar en:
Radicado por: Claudia María Gómez Londoño

040-RES2307-3653
Favor citar este número al responder

Por la cual se adopta el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2023 de la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA-

La Directora General de la Corporación Autónoma Regional del Centro de Antioquia, en uso de sus facultades legales y estatutarias y en especial las que le confieren el artículo 29 de la Ley 99 de 1993 y el Decreto 1768 de 1994 y,

CONSIDERANDO

Que el Decreto 1008 de 2018 establece los lineamientos generales de la Política de Gobierno Digital que deberán adoptar las entidades pertenecientes a la administración pública, encaminados hacia la transformación digital y el mejoramiento de las capacidades TIC, para el desarrollo del habilitador transversal “Seguridad de la Información” de la Política de Gobierno Digital.

Que el Decreto 1499 de 2017 determina el cumplimiento institucional de las Políticas de Gobierno y Seguridad Digital en relación con el habilitador “Seguridad de la Información” conforme a la Resolución 500 de 2021 (MinTIC) y la Política de Seguridad Digital acorde con los lineamientos de los documentos CONPES 3701 de 2011 Lineamiento de Políticas de Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad Digital, CONPES 3975 de 2019 Política Nacional para la Transformación Digital e Inteligencia Digital, CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital.

Que el Plan de Acción 2020 – 2023 “+ Sostenibilidad + Vida, Integrando la Naturaleza con el Desarrollo”, en concordancia con el Plan de Gestión Ambienta Regional 2020 – 2031 “Un Plan Intergeneracional”, la Resolución 040-RES2112-9432 del 30 de diciembre de 2021 donde se adopta en la Corporación Autónoma Regional del Centro de Antioquia (Corantioquia) el “Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2022 – 2023” y la Resolución 040-RES2010-5756 - Política General de Tecnología, de Seguridad y Privacidad de la Información que se constituyen en instrumentos de planificación que orientan la ruta de acción en materia de inversiones y proyectos TIC encaminados hacia la transformación digital, modernización tecnológica de la entidad y seguridad y privacidad de la Información corporativa.

Código Dependencia-

Que, por las consideraciones antes expuestas, la Directora General de la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA- en mérito de lo expuesto,

RESUELVE

Artículo 1º. Objeto: Adoptar en la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA-, el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2023.

Artículo 2°. Implementación: La Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA- deberá implementar el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2023, adoptada a través del presente acto administrativo, conforme a sus responsabilidades y competencias.

Artículo 3º. Seguimiento y Revisión: La Subdirección Administrativa y Financiera o la dependencia encargada de liderar los procesos tecnológicos de la Corporación le hará seguimiento a su implementación. El Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información serán revisados anualmente, o antes si existiesen modificaciones que así lo requieran, para que se mantenga oportuno, suficiente y eficaz.

Artículo 4º. Vigencia: La presente Resolución rige a partir de la fecha de su expedición y deja sin efecto cualquiera otra contraria a estas disposiciones.

Dado en Medellín, el 26 de Julio 2023

PUBLÍQUESE Y CUMPLASE

ANA LIGIA MORA MARTÍNEZ
Directora General

Anexo: Plan de Seguridad y Privacidad de La Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2023.

Asignación: N/A
Elaboró: Ambrosio Caicedo Celis
Revisó: Carlos Alberto Velásquez López, Glenys Danith Oviedo Castro

Fecha de elaboración: 2023-07-26

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

GRUPO INTERNO DE TRABAJO TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA

CORPORACIÓN AUTÓNOMA REGIONAL DEL CENTRO DE ANTIOQUIA - CORANTIOQUIA

MEDELLÍN
JULIO 2023

CONTROL DE VERSIONES

Fecha	Autor (es)	Versión	Referencia del Cambio
26/07/2023	• Ambrosio Caicedo Celis • Ferney Andrés Valdés Tabares • Marleny Vélez Cárdenas • Jorge Andrés Gallego Londoño	1.0	Versión inicial

TABLA DE CONTENIDO

Introducción

La Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA dando alcance al cumplimiento del Decreto 1008 de 2018 que establece los lineamientos generales de la Política de Gobierno Digital que deberán adoptar las entidades pertenecientes a la administración pública, encaminados hacia la transformación digital y el mejoramiento de las capacidades TIC, para el desarrollo del habilitador transversal "Seguridad de la Información" de la Política de Gobierno Digital; así mismo el Decreto 1499 de 2017 determina el cumplimiento institucional de las Políticas de Gobierno y Seguridad Digital en relación con el habilitador "Seguridad de la Información" conforme a la Resolución 500 de 2021 (MinTIC) y la Política de Seguridad Digital acorde con los lineamientos de los documentos CONPES 3701 de 2011 Lineamiento de Políticas de Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad Digital, CONPES 3975 de 2019 Política Nacional para la Transformación Digital e Inteligencia Digital, CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital.

Por otra parte, La Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA ha implementado el tratamiento y protección de los datos personales conforme a las disposiciones de la Resolución 1519 de 2020 de MinTIC que define los estándares y directrices para publicar la información institucional atendiendo los lineamientos de la Ley 1712 de 2014; y acoge en sus procesos el marco normativo y regulatorio de la entidad relacionada con la Seguridad y Privacidad de la Información (SPI).

De acuerdo con lo anterior, se define el Plan de Seguridad y Privacidad de la Información – Plan SPI para la vigencia 2023, en el marco del Plan de Acción 2020 – 2023 "+ Sostenibilidad + Vida, Integrando la Naturaleza con el Desarrollo", en concordancia con el Plan de Gestión Ambiental Regional 2020 – 2031 "Un Plan Intergeneracional", la Resolución 040-RES2112-9432 del 30 de diciembre de 2021 donde se adopta en la Corporación Autónoma Regional del Centro de Antioquia (Corantioquia) el "Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2022 – 2023" y la Resolución 040-RES2010-5756 - Política General de Tecnología, de Seguridad y Privacidad de la Información que se constituyen en instrumentos de planificación que orientan la ruta de acción en materia de inversiones y proyectos TIC encaminados hacia la transformación digital y modernización tecnológica de la entidad.

Objetivo

Definir las medidas, actividades y controles necesarios para adelantar la gestión de la seguridad y privacidad de la información (SPI) de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información, la norma ISO NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad de la operación de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA para asegurar la confidencialidad, integridad y disponibilidad de la información.

Alcance

La gestión de la seguridad y privacidad de la información aplica a todos los procesos institucionales de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA y demás partes interesadas que comparten, utilicen, recolecten, procesen, intercambien o consulten cualquier tipo de información, ya sea interna o externa, así como las actividades pertinentes que se consideren fundamentales para determinar la estrategia de implementación de los controles de seguridad requeridos para el adecuado funcionamiento del proceso Gestión de TIC del Sistema de Gestión Integral de la Corporación.

Inicia con la definición del Plan de Seguridad y Privacidad de la Información, continua con la ejecución y finaliza con el seguimiento y evaluación de la gestión realizada.

Aplica a toda información creada, procesada o utilizada sin importar el medio, formato o presentación y lugar en el cual se encuentre.

Definiciones

Activos de información: Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensibles o críticos para el cumplimiento de los objetivos de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

CIGD: Sigla Comité Institucional de Gestión y Desempeño.

Confidencialidad: Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

Control: Medida que modifica y mitiga el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: Acceso a la información cuando se requiere, teniendo en cuenta la privacidad.

GIT: Sigla Grupo Interno de Trabajo.

Incidente de seguridad de la información: Un incidente de seguridad de la Información está indicado por un único evento o una serie de eventos de Seguridad de la Información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y de amenazar la seguridad de la información.

Integridad: Es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (impacto). (ISO/IEC 27000).

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

SGI: Sigla Sistema de Gestión Integral.

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

Condiciones Generales

La Dirección General de la Corporación promueve la seguridad y privacidad de la información (SPI), a través del cumplimiento de la Política General de Tecnología, de Seguridad y Privacidad de la Información, adoptada mediante la Resolución 040-RES2010-5756 y del cumplimiento de la política de Protección de Datos Personales adoptada mediante la Resolución 040-RES1904-1730; la implementación del proceso Gestión de TIC y su articulación con los procesos corporativos, con la que se determinan los cambios a incorporar en el presente documento.

De igual forma, para llevar a cabo la preparación de plan de seguridad y privacidad de la información de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA se siguieron los lineamientos contenidos en el Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en Entidades Públicas – Anexo Técnico No. 4 – DAFP expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones, la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la Información, Diseño de Controles en Entidades Pública, emitida por el Departamento Administrativo de la Función Pública – DAFP.

Plan de Seguridad y Privacidad de la Información

La Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA, mediante la implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el proceso Gestión de TIC del Sistema de Gestión Integral de la Corporación, protege, preserva y gestiona la confidencialidad, integridad, disponibilidad de la información, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales reduciendo la probabilidad de ocurrencia de incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua.

Para lograr el cumplimiento del Plan se definen las siguientes estrategias:

1. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en los lineamientos de la Seguridad y Privacidad de la Información.
2. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad de la información de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA.
3. Gestionar los riesgos de SPI, Seguridad Digital de manera integral.
4. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
5. Generar la concientización para el uso y apropiación de la Seguridad y Privacidad de la Información como eje transversal de la Corporación.
6. 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.

Roles y Responsabilidades

Rol		Responsabilidad
Rol Estratégico	Comité Institucional de Gestión y Desempeño.	Aprobar el Plan SPI. Tomar decisiones sobre los asuntos de la seguridad de la información.
Rol Táctico	Oficial de Seguridad o quien haga sus veces.	Preparar y presentar el Plan SPI. Asegurar la implementación de las políticas que se desarrollan para garantizar la confidencialidad, disponibilidad e integridad de la información en el marco del proceso Gestión de TIC del Sistema de Gestión Integral de la Corporación, la seguridad y privacidad la información y seguridad digital.
Rol Funcional	GIT Tecnologías de la Información y las Comunicaciones	Ejecutar y hacer seguimiento al desarrollo del Plan SPI. Informar sobre la gestión de la SPI.
	Líderes de Procesos	Integrar los procesos institucionales a la gestión de la SPI. Ejecutar los controles a nivel de proceso para la seguridad y protección de los activos de información. Promover las buenas prácticas de SPI.

Funciones

Comité de seguridad de la información

Las funciones del comité de Seguridad de la Información son asumidas por el Comité Institucional de Gestión y Desempeño – CIGD.

Dirección General

- Aprobar y/o revisar anualmente o cuando se requiera la Política de Seguridad de la Información de la Corporación.
- Aprobar los objetivos de seguridad de la información, los cuales estarán alineados con los objetivos estratégicos de la entidad.

- Gestionar el presupuesto necesario para el normal funcionamiento del Plan de Seguridad y Privacidad de la Información.
- Promover activamente una cultura de seguridad y privacidad de la información basada en la mitigación de los riesgos para la entidad.

Oficial de seguridad o quien haga sus veces

El rol del Oficial de seguridad o Coordinador del proceso Gestión de TIC o quien haga sus veces, es el responsable de:

- Realizar seguimiento al cumplimiento de los lineamientos y políticas del proceso Gestión de TIC.
- Revisar y proponer las políticas, planes, programas, procedimientos en materia de seguridad de la información para la aplicación de controles en el sistema.
- Realizar revisiones periódicas al proceso Gestión de TIC y definir acciones conducentes a la mejora continua.
- Asegurar el cumplimiento de las políticas, normas, procedimientos, y demás lineamientos en materia de seguridad de la información.

Líderes de procesos

El rol de los líderes de procesos en la ejecución del plan de revisión y seguimiento al proceso Gestión de TIC, es fundamental dado que es el responsable de:

- Seguimiento a la ejecución de los planes de tratamiento de riesgos en seguridad de la información.
- Actualización de activos de información.
- Revisión y cumplimiento de los procedimientos, controles y políticas del proceso Gestión de TIC.

Coordinador del GIT TIC

El GIT de apoyo informático y sus profesionales serán los responsables de los controles técnicos de seguridad de la información:

- Cierre de vulnerabilidades técnicas.
- Seguimiento al cierre de vulnerabilidades técnicas.
- Seguimiento de indicadores.
- Seguimiento al cierre de eventos e incidentes de seguridad de la información.
- Seguimiento del plan de tratamiento de riesgos de seguridad de la información del proceso Gestión TICs.
- Establecer controles de seguridad de la información con el fin de mitigar los riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y/o servicios que presta el GIT de apoyo informático.

Funcionarios y Contratistas

- Implementar las normas, políticas y procedimientos definidos para el sostenimiento del proceso Gestión de TIC.
- Mantener y garantizar la confidencialidad e integridad de la información que reciben, generan y procesan en la Corporación.
- Hacer buen uso de los activos de información de la entidad.
- Respetar la legislación y regulación vigente.
- Notificar a la cuenta de correo electrónico seguridadinformatica@corantioquia.gov.co los eventos o incidentes de seguridad de información, así como cualquier eventualidad sospechosa que pueda poner en riesgo la continuidad de las operaciones de la Corporación.

Plan de implementación de la seguridad y privacidad de la información

El Plan de implementación de Seguridad y Privacidad de la Información de la Corporación tiene como propósito definir las actividades para la operación, evaluación y mejora de la Seguridad y Privacidad de la Información (SPI) con énfasis en la gestión de activos de información, riesgos, toma de conciencia, protección de datos y seguridad digital institucional.

El seguimiento de la gestión del Plan SPI 2023 se presenta periódicamente al Comité Institucional de Gestión y Desempeño – CIGD, y documenta según los productos definidos.

Las iniciativas en materia de Seguridad y Privacidad de la Información de la Corporación se encuentran enmarcadas en el "Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2022 – 2023" adoptado mediante la Resolución 040-RES2112-9432 del 30 de diciembre de 2021, las cuales se relacionan a continuación:

INICIATIVAS DE OPERACIÓN

FICHA DE PROYECTO				
Id del Proyecto	INI_OPE_04			
Nombre del Proyecto	Portal Web Corporativo, Intranet y Datos Abiertos.			
Objetivos del Proyecto	Actualizar la página web e intranet de la Corporación según la norma técnica NTC 5854 y lineamientos del MINTIC.			
Vigencia de Ejecución	2022	**Costo Aproximado de Implementación**	$36.397.500	
Prioridad de la Implementación	**Alta**	Media	Baja	

Responsables	Subdirección Administrativa y Financiera
Descripción / Alcance	
Rediseño y optimización del sitio web e intranet de Corantioquia www.corantioquia.gov.co con la migración de plataforma, SEO, ciberseguridad y cumplimiento de normativa de Gobierno Digital, FURAG, ITA, NTC5854, MIPG y Resolución MINTIC 1519 de 2020 en sus anexos 1,2 y 3.	

Adicionalmente, con base en el ejercicio de identificación de los conjuntos de datos corporativos que se determinaron mediante los talleres de Datos Abiertos realizados, y teniendo en consideración la obligatoriedad de las entidades públicas de "divulgar datos abiertos" según lo establecido en la Ley 1712 de 2014, artículo 11, literal k), se han realizado las siguientes actividades:

- Identificación de los conjuntos de datos corporativos.
- Priorización de los conjuntos de datos.
- Definición de metadatos.
- Consolidación y estructuración de los conjuntos de datos para publicarlos como Datos Abiertos.
- Cargue y publicación de los conjuntos de datos en la plataforma de Datos Abiertos https://www.datos.gov.co/.
- Fortalecimiento continuo de la estrategia.

FICHA DE PROYECTO			
Id del Proyecto	INI_OPE_10		
Nombre del Proyecto	Infraestructura Tecnológica.		
Objetivos del Proyecto	Prestar los servicios especializados que garanticen el buen funcionamiento de la Infraestructura Informática y de Telecomunicaciones de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA, que incluya el servicio de Mesa de Ayuda para mejorar la prestación de los servicios tecnológicos de la Corporación.		
Vigencia de Ejecución	2022-2023	**Costo Aproximado de Implementación**	$631.636.955
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción / Alcance			
Realización de las operaciones técnicas necesarias para garantizar el correcto funcionamiento del centro de cómputo y los servicios informáticos y de telecomunicaciones de la Corporación Autónoma Regional del Centro de Antioquia, de conformidad con los Acuerdos de Nivel de Servicio (ANS), con un porcentaje de disponibilidad de la plataforma tecnológica de La Corporación, superior a 99,4%.			

FICHA DE PROYECTO			
Id del Proyecto	INI_OPE_12		
Nombre del Proyecto	Licenciamiento de Productos de Software.		
Objetivos del Proyecto	Contar con el licenciamiento necesario para el correcto funcionamiento y disponibilidad de las aplicaciones corporativas.		
Vigencia de Ejecución	2022-2023	**Costo Aproximado de Implementación**	$3.447.823.376
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción / Alcance			

Contratar la suscripción de licencias de los productos Office 365, Adobe, Oracle y Avaya. Este servicio deberá incorporar un esquema de uso y apropiación de las plataformas que permita a los usuarios de la Entidad hacer un uso eficiente de la totalidad de las herramientas incluidas en la suscripción.

Es de resaltar, que se ha venido migrando la información corporativa a servicios de nube mediante la sensibilización y configuración de la aplicación OneDrive a todos los usuarios con el objeto de brindar seguridad a la información de la entidad.

INICIATIVAS DE TRANSFORMACIÓN DIGITAL Y MODERNIZACIÓN TECNOLÓGICA

FICHA DE PROYECTO			
Id del Proyecto	INI_TMOD_01		
Nombre del Proyecto	Adquisición, instalación, configuración y migración de un Sistema de Información Administrativo, Financiero, Contable, y Fiscal ERP (Enterprise Resource Planning – Planificación de Recursos Empresariales) integral para la Corporación Autónoma Regional del Centro de Antioquia - Corantioquia.		
Objetivos del Proyecto	Implementar un Sistema de Gestión Administrativa y Financiera que cumpla con los requerimientos técnicos, funcionales y no funcionales definidos por la normatividad presupuestal, contable, financiera, manejo de activos fijos, inventarios, inmuebles, talento humano, gestión de proyectos, control y seguimiento al PGAR y PAI (incluye Software como Servicio).		
Vigencia de Ejecución	2023	**Costo Aproximado de implementación**	$1.075.693.702
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción / Alcance			

La plataforma tecnológica deberá cumplir como mínimo con las características funcionales, técnicas y tecnológicas, tanto en el diseño como en la versatilidad de sus aplicaciones, de acuerdo con los siguientes requerimientos:

- Hosting y/o alojamiento.
- Soporte técnico, mantenimiento y actualización de la solución.
- Especialistas por módulo.
- Transferencia de conocimiento.
- Documentación.

FICHA DE PROYECTO			
Id del Proyecto	INI_TMOD_02		
Nombre del Proyecto	Renovación de la Infraestructura Tecnológica.		
Objetivos del Proyecto	Renovar la Infraestructura Tecnológica de la Corporación a sistemas de almacenamiento en la nube e híbrida, incluyendo servicios de respaldo alterno (backup) según los lineamientos del MINTIC y la Directiva Presidencial 03 de 2021.		
Vigencia de Ejecución	2023	**Costo Aproximado de Implementación**	$797.981.999
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción / Alcance			
Migración de la Infraestructura Tecnológica actual a la nube e híbrida, lo que permitirá centralizar toda la información de la Corporación en un espacio virtual que puede ser de forma pública o privada, es decir, puede permitir que sea consultada por muchos usuarios o bien decidir que solo tengan acceso un determinado número de usuarios; además, estas características hacen posible que los usuarios internos y externos puedan acceder a datos de interés desde cualquier lugar y reducir así los tradicionales procesos para compartir datos que solían gastar más tiempo.			

FICHA DE PROYECTO			
Id del Proyecto	INI_TMOD_03		
Nombre del Proyecto	Renovación de Equipos Tecnológicos y Periféricos.		
Objetivos del Proyecto	Adquirir y renovar equipos tecnológicos de última generación de acuerdo con las necesidades de los procesos.		
Vigencia de Ejecución	2022-2023	**Costo Aproximado de Implementación**	$1.441.376.291
Prioridad de la Implementación	Alta	**Media**	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción / Alcance			

Adquisición de recursos tecnológicos, entre los cuales se encuentran: Servidores, almacenamiento, redes, equipos de escritorio, tabletas, portátiles, dispositivos electrónicos, periféricos, entre otros, para la prestación de los servicios que apoyan y soportan la operación, desarrollo y crecimiento de la Corporación.

FICHA DE PROYECTO			
Id del Proyecto	INI_TMOD_12		
Nombre del Proyecto	Migración de IPv4 a IPv6.		
Objetivos del Proyecto	Migrar del protocolo IPv4 a IPv6, que incluya las fases de: Diagnóstico, Planeación, Ejecución, Piloto de Pruebas, Transferencia de Conocimiento, Implementación, Pruebas de Funcionalidad y Monitoreo.		
Vigencia de Ejecución	2023	**Costo Aproximado de Implementación**	$349.962.740
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción / Alcance			
Construcción del plan de migración del protocolo IPv4 a IPv6, y aunar esfuerzos para realizar el acompañamiento y brindar asistencia mediante herramientas técnicas y el personal especializado en la realización del diagnóstico, el plan de implementación, la transferencia de conocimiento, la implementación y el desarrollo de pruebas de funcionalidad (monitoreo) del protocolo IPv6.			

FICHA DE PROYECTO			
Id del Proyecto	INI_TMOD_14		
Nombre del Proyecto	Actualización del licenciamiento y acuerdo de soporte de la solución de firewall de la Corporación.		
Objetivos del Proyecto	Realizar la adquisición de equipo, renovación del licenciamiento y acuerdo de soporte de la solución firewall de la Corporación por tres (3) años.		
Vigencia de Ejecución	2022-2023	**Costo Aproximado de Implementación**	$97.000.000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción / Alcance			
Suministro del licenciamiento que permita el uso y soporte de la solución firewall para la Corporación, incluyendo renovación y servicios profesionales con personal certificado por el fabricante para la actualización de los firewall, con el fin de garantizar la protección de los servicios tecnológicos y usuarios en la navegación web, entre otros.			

FICHA DE PROYECTO	
Id del Proyecto	INI_TMOD_16

Nombre del Proyecto	Firma Electrónica y Digital.		
Objetivos del Proyecto	Realizar la adquisición, instalación, configuración, pruebas, puesta en funcionamiento y soporte de una solución web para firma digital de documentos, con certificados de firma digital y sus respectivos tokens.		
Vigencia de Ejecución	2022-2023	**Costo Aproximado de Implementación**	$ 98.392.532
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción / Alcance			
Se cuente con estándares de seguridad robustos que permitan realizar el proceso de gestión documental de la Entidad y permitir a la Corporación estar a la vanguardia en últimas tecnologías aumentando la productividad y buen desempeño de sus Servidores Públicos, sus procesos misionales, planes, programas, proyectos metodologías y estrategias, contribuyendo a fortalecer y mejorar los servicios tecnológicos que presta la Corporación a los usuarios internos y externos.			

Valor Total estimado: $7.976.265.095

A continuación, se presenta la programación de actividades que conforman el Plan SPI:

Nro.	Control	Actividades Por Ejecutar	Producto	Fecha inicial estimada	Fecha final estimada	Responsable
1	Diagnóstico MSPI	Realizar la actualización de la Matriz del MPSI	Matriz diagnóstico diligenciada	Agos de 2023	Agos de 2023	GIT TIC
2	Política general de seguridad de la información	Revisar, ajustar y aprobar la Política de Seguridad de la información	Política de Seguridad de la Información Actualizada	Sept de 2023	Sept de 2023	Dirección General Subdirección de Planeación GIT TIC
3	Manual de seguridad de la información	Revisar, ajustar y aprobar el Manual de Seguridad de la Información.	Manual de Seguridad de la Información Actualizado	Sept de 2023	Sept de 2023	GIT TIC Subdirección de Planeación
4	Estrategia de Seguridad Digital	Revisar, ajustar y aprobar la Estrategia de Seguridad Digital	Estrategia de Seguridad Digital Actualizada	Oct de 2023	Oct de 2023	GIT TIC Subdirección de Planeación
		Realizar actividades para el fortalecimiento de capacidades a través de acuerdos con otras Entidades Nacionales en temas de Defensa y Seguridad Digital.	Actas de reuniones y/o acuerdos	Oct de 2023	Dic de 2023	GIT TIC Subdirección de Planeación, funcionarios de la Corporación

5	Documentos del proceso Gestión de TIC – Procedimiento	Revisar y ajustar los documentos de proceso Gestión de TIC implementado en la	formatos, instructivos,	Agos de 2023	Dic de 2023	GIT TIC Subdirección de Planeación

	de seguridad de la información y otros	Corporación, de acuerdo con las actualizaciones definidas y aprobadas por el CIGD	políticas y flujogramas actualizados			Todos los procesos del alcance del proceso Gestión de TIC
6	Gestión de activos de Información	Validar, verificar, actualizar y aprobar el inventario de Activos de Información. Verificar, actualizar y aprobar el inventario de activos críticos, infraestructuras críticas y servicios esenciales.	Matriz de activos actualizada y aprobada	Agos 2023	Dic de 2023	GIT TIC Subdirección de Planeación Todos los procesos del alcance del proceso Gestión de TIC
7	Gestión de vulnerabilidades	Definir lineamientos para ejecutar las pruebas de vulnerabilidades Ejecución de pruebas de seguridad (análisis de vulnerabilidades) al menos una vez al año. Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades	Documentación gestión de vulnerabilidades y resultados de pruebas de vulnerabilidades	Agos 2023	Dic de 2023	GIT TIC

		Realizar seguimiento al cierre de vulnerabilidad técnicas de acuerdo con su nivel de criticidad				

		Verificar la ejecución del re- test de pruebas de seguridad Documentar las actualizaciones cuando ocurra un cambio importante en los activos de información producto del retest.				
8	Indicadores de seguridad de la información	Revisar, ajustar o formular, implementar y medir los indicadores del proceso Gestión de TIC.	Matriz con indicadores actualizados según periodicidad e informe del cumplimiento de las acciones correctivas en caso de que aplique	Agos 2023	Dic de 2023	Subdirección de Planeación GIT TIC
9	Gestión de riesgos (Identificación, Análisis y Evaluación de Riesgos)	Realizar la identificación, análisis y evaluación de riesgos de los activos de información	Matriz con la evaluación de riesgos incluidos los riesgos de los activos de información y seguridad digital.	Agos 2023	Dic de 2023	Subdirección de Planeación GIT TIC
		Realizar la identificación, análisis y evaluación de riesgos de los activos críticos, infraestructura crítica y servicios esenciales (entorno digital)		Agos 2023	Dic de 2023	
		Realizar seguimiento trimestral al Mapa o Plan de Tratamiento	Mapa o Plan de Tratamiento de Riesgos actualizado con soportes	Nov 2023	Dic de 2023	

		de Riesgos de la Corporación				

		Realizar valoración trimestral del riesgo residual para establecer las variaciones y/o ajustes de cada periodo cuando corresponda		Nov 2023	Dic de 2023	Líderes de los procesos misionales de la Corporación GIT TIC
		Como parte del seguimiento se realiza la revisión y preparación de evidencias que respaldan la ejecución de las actividades de control establecidas en el Plan de Tratamiento de Riesgos		Nov 2023	Dic de 2023	Subdirección de Planeación GIT TIC
10	Plan de Continuidad de Negocio de TI y los Planes de Contingencia	Revisar, ajustar y aprobar el Plan de Continuidad de Negocio, sus Anexos y los Planes de Contingencia	Plan de Continuidad de Negocio de TI – Anexos y Plan de Contingencia actualizados	Agos 2023	Dic de 2023	GIT TIC
		Validar, verificar, actualizar la identificación y/o valoración de Riesgos de interrupción de la operación de la entidad	Documentación de las	Agos 2023	Dic de 2023	

		según corresponda	pruebas realizadas			
		Realizar seguimiento y revisión de la ejecución de las pruebas del plan según Cronograma				

		Realizar seguimiento a la documentación y lecciones aprendidas de los resultados de las pruebas del Plan				
		Revisión de las acciones de mejora Identificadas en las pruebas del Plan				
11	Plan de comunicación, socialización y sensibilización	Elaborar y ejecutar el Plan de comunicación en temas relacionados con la seguridad de la información como complemento al Plan Institucional de Capacitación de la Corporación	Plan de Sensibilización y toma de conciencia en temas relacionados con seguridad de la Información y Seguridad Digital	Nov 2023	Dic de 2023	GIT TIC
		Desarrollar un Plan de sensibilización y toma de conciencia sobre ciberseguridad para ejercer control y protección sobre los entornos digitales Realizar mínimo 2 sesiones de		Nov 2023	Dic de 2023	GIT TIC Líderes de los procesos de la Corporación, Talento humano, GIT TIC

		sensibilización en seguridad de la información en las jornadas de inducción y reinducción		Nov 2023	Dic de 2023	(Nota: Los lideres podrán realizar socializaciones internas de seguridad de la información

						cuando sea pertinente mas no es obligatorio)
		Hacer seguimiento a las evidencias de socialización del proceso Gestión de TIC.	Evidencias de socialización y sensibilización	Agos 2023	Dic de 2023	Subdirección de Planeación
12	Auditoria (Internas y/o Externas)	Realizar auditorías internas y/o externas de la norma ISO 27001:2013	Informe de auditoría y Plan de Mejoramiento	Agos 2023	Nov de 2023	Subdirección de Planeación
		Realizar seguimiento al cierre de las no conformidades producto de las auditorías internas y externas al proceso Gestión de TIC.				Todos los líderes de los procesos incluyendo al líder del GIT TIC.
		Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso				
		Gestionar los incidentes de Seguridad de la Información identificados	Formatos Registro de Incidentes y/o Eventos de Seguridad de la Información y Soportes gestión	Agos 2023	Dic de 2023	

13	Gestión de incidentes de seguridad	Socializar el procedimiento de respuesta de gestión de incidentes al GIT de Apoyo Informático Realizar el seguimiento a la gestión de incidentes de seguridad de la	Presentación al GIT TIC Presentación con los resultados de los incidentes ocurridos en tema de	Agos 2023 Agos 2023	Dic de 2023 Dic de 2023	GIT TIC

		información incluyendo cierre	seguridad y privacidad de la información			
		Realizar seguimiento a las lecciones aprendidas producto de la gestión del incidente				
		Realizar seguimiento de los reportes de eventos de seguridad de la información y tomar acciones.				
		Capacitar a los usuarios internos y partes interesadas sobre los boletines de CSIRT.	Evidencias de sensibilización	Oct 2023	Dic de 2023	
14	Declaración de aplicabilidad – Anexo A	Revisión de los controles de la norma ISO 27001:2013	Declaración de aplicabilidad actualizada	Nov 2023	Dic de 2023	GIT TIC
		Actualizar declaración aplicando acciones y controles para la implementación del control				
		Seguimiento a la aplicación de los controles				

Nota: En todo caso, se podrán presentar modificaciones a este cronograma pero sin afectar la implementación de este Plan.

SEGUIMIENTO, MEDICIÓN Y EVALUACIÓN

El seguimiento y evaluación al Plan de Seguridad y Privacidad de la Información, se realizará conforme al cumplimiento de las actividades definidas en este plan.

Así pues, el proceso de seguimiento y evaluación permite contar con información objetiva y oportuna de utilidad para: tomar acciones que permitan mejorar la Seguridad y Privacidad de la Información orientada a la consecución de resultados.

El avance del Plan de Seguridad y Privacidad de la Información se evaluará semestralmente.

El resultado del avance de la implementación del Plan de Seguridad y Privacidad de la Información, se interpretará de conformidad con los siguientes rangos de evaluación:

Nivel de ejecución (N.E) deficiente	Nivel de ejecución (N.E) aceptable	Nivel de ejecución (N.E) sobresaliente
N.E < 75 %	75 % ≤ N.E ≤ 90 %	90 % < N.E ≤ 100 %

Nro.	RIESGO	ACTIVOS	TIPO
1	Pérdida de Confidencialidad	TALENTO HUMANO	Seguridad de la Información

2	Pérdida de Confidencialidad	TALENTO HUMANO INFORMACIÓN	Seguridad de la Información
3	Pérdida de Disponibilidad	INFORMACIÓN	Seguridad de la Información

4	Pérdida de Disponibilidad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información

5	Perdida de Integridad	HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información
6	Perdida de Integridad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información

7	Pérdida de Disponibilidad	INFORMACIÓN TALENTO HUMANO	Seguridad de la Información
8	Pérdida de Disponibilidad	INFORMACIÓN TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información

9	Pérdida de Integridad	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información
10	Pérdida de Disponibilidad	HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información
11	Pérdida de Confidencialidad	INFORMACIÓN TALENTO HUMANO	Seguridad de la Información

12	Pérdida de Confidencialidad	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información
13	Pérdida de Confidencialidad	INFORMACIÓN TALENTO HUMANO	Seguridad de la Información
14	Pérdida de Confidencialidad	INFORMACIÓN	Seguridad de la Información

		HARDWARE SOFTWARE Y SERVICIOS	
15	Pérdida de Confidencialidad	INFORMACIÓN	Seguridad de la Información
16	Pérdida de Disponibilidad	INFORMACIÓN TALENTO HUMANO	Seguridad de la Información

17	Pérdida de la confidencialidad, integridad	INFORMACIÓN	Seguridad de la Información
18	Pérdida de Disponibilidad	INFORMACIÓN	Seguridad de la Información

19	Pérdida de Disponibilidad	HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información
20	Pérdida de la confidencialidad, integridad	INFORMACIÓN	Seguridad de la Información
21	Pérdida de la confidencialidad, integridad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información

22	Pérdida de Integridad	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información

1	Asesoría y documentación brindada por Entidades del Estado en temas de seguridad de la información, por ejemplo guías que provee MinTIC, DAFP, Archivo General de la Nación	TALENTO HUMANO INFORMACIÓN	Seguridad de la Información

AMENAZA
Usuarios mal intencionados o por desconocimiento de la seguridad de la información ocasionan pérdida parcial o total de la información.

Acciones indebidas de los funcionarios o contratistas con privilegios de acceso (Usuarios mal intencionados o con desconocimiento de los procesos, procedimientos y/o políticas de la Entidad)
Fuga de información Divulgación de procedimientos o información catalogada como reservada o clasificada Configuración por default de componentes tecnologicos

Incendio, inundación, terremoto, polvo
Funcionarios con acceso a Datacenter, inconformes y/o sin conocimientos en seguridad de la información
Códigos maliciosos
Proveedores tecnológicos
Ciberdelincuentes
Ataques terroristas
Disturbios civiles
Interrupción de los servicios de la entidad y página web
Indisponibilidad de la plataforma tecnológica

Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso
Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso

Funcionarios/contratistas, Proveedores externos, Ciberataques, servicios de suministro, amenazas naturales
Afectación en la disponibilidad del respaldo de la información Insuficiencia de espacio o almacenamiento para el aseguramiento de la información Pérdida o corrupción de los datos Corrupción de las cintas en el momento de las copias y las restauración del Backup Inexistencia de Backup de la información misional
Indisponibilidad de los servicios y/o página web Administradores de tecnología sin conocimientos técnicos de seguridad de la información. Fuga y/o pérdida de información generada por código malicioso

Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la plataforma tecnológica Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso
Falla en el suministro de energía, servicios ofrecidos por el proveedor
Usuarios sin conocimiento de las políticas, manual y procedimientos de seguridad de la información

Red sin protección, sin las herramientas o equipos tecnológicos de comunicación que aseguren al usuarios su correcto funcionamiento Fuga de información debido al acceso de usuarios no autorizados a la infraestructura de red de la entidad. Indisponibilidad del servicio de la red inalámbrica debido a ataques de denegación de servicios (DoS). Suplantación de identidad para acceder a los aplicativos tecnológicos de la entidad que se encuentran disponibles a través de la red de datos. Funcionarios descontentos pueden hacer uso de usuarios y contraseñas de personal que ya no labora en la entidad para visualizar y/o sustraer información confidencial de la entidad.
Fuga y/o pérdida de información Divulgación no autorizada de información debido a acceso de terceros Secuestro de información generado por una aplicación ramsomware.
Usuarios mal intencionados, Atacantes, Códigos maliciosos

Funcionarios y/o Contratistas inconformes Atacantes externos,
Funcionarios con desconocimiento en temas de contratación de personal Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la Corporación Insuficiente protección y privacidad de información personal

Robo o hurto de información catalogada como sensible por falta de implementación de herramientas que aseguren el transporte de la información por la red Acceso a información privada, reservada o sensible sin la debida autorización.
Funcionarios con roles de seguridad de la información sin conocimiento Interrupción completa en la continuidad del negocio (Daño en Data Center, Servicios Tecnológicos y pérdida de la Información) Los usuarios realizan trabajo en casa, manipulan información, acceden a los sistemas de información desde las conexiones establecidas en el hogar Practicas inapropiada que afecten la disponibilidad de la información y la plataforma tecnológica

Ausencia de revisiones periódicas por parte de los administradores de los recursos de la infraestructura tecnológica
Filtración y manipulación de la información para beneficio de un tercero
Proveedores de sistemas de información, funcionarios con roles de desarrollo que no cumplen las políticas y requerimientos en seguridad Manipulación intencionada interna o externa de las fuentes de información ocasionando pérdida parcial y/o total del código fuente Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. Indisponibilidad de acceso a los repositorios de información o herramienta donde se resguarda el código fuente

Usuarios y administradores sin conocimiento de las políticas y procedimientos de seguridad de la información

No Aplica

MAPA Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURID

CAUSA / VULNERABILIDAD	P PROBABILIDAD
Desconocimiento de los lineamientos sobre la seguridad de la información institucionales Desactualización de la Política y Manual de seguridad de la información Uso y apropiación insuficiente de las políticas, manual y procedimientos de seguridad de la información Falta de competencias del personal a cargo del cumplimiento de las responsabilidades de la seguridad de la información asignadas Falta o insuficiente descripción de los roles y responsabilidades sobre seguridad de la información en los documentos de contratación	CASI SEGURO

Ausencia de implementación de procedimientos en la gestión de usuarios que incluya registro de usuarios, cancelación de usuarios, asignación y anulación de derechos de acceso. Ausencia de gestión sobre las vulnerabilidades técnicas	RARA VEZ
Falta de implementación de procedimientos o políticas adecuadas en seguridad de la información en las actividades, servicios o procesos aplicadas a los proveedores y/o contratistas en la labor contratada	RARA VEZ

Ausencia de planes de emergencia y pruebas al mismo. Ausencia de redes contra incendio, condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física Acciones fortuitas o malintencionados en el centro de computo, ocasionando pérdida parcial o total de la información alojada en los equipos. Conexión de equipos a corriente no regulada Debilidad en la infraestructura tecnológica, ausencia de un sistema de control de acceso. Falta de mantenimiento a equipos de usuarios y a la plataforma tecnológica Hardware y software obsoletos y sin garantía Encargado del componente no se encuentra disponible y no existe un rol de respaldo de éste. Gestión inadecuada de la capacidad de los equipos, falla en las UPS o aires acondicionados. Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) Ausencia de redundancias para los servicios críticos No se registra un monitoreo constante de los eventos y registro de logs que permitan detectar posibles intrusiones y/o debilidades de seguridad. El antivirus instalado en los servidores no se encuentra activo o desactualizado	RARA VEZ

Ausencia de políticas y controles restrictivos para la instalación de software no autorizado Uso e instalación de software con vulnerabilidades Perfiles y privilegios no asignados Descarga de virus informáticos maliciosos (Spiware, troyanos, virus, gusanos)	RARA VEZ
Base de datos de antivirus desactualizada. Usuarios con privilegios de uso de medios removibles Equipos informaticos sin licencia o con software desactualizados	IMPROBABLE

Manipulación, transporte y almacenamiento inadecuado a las cintas de Backup. Ausencia de pruebas regulares a las copias de respaldo. Incumplimiento al acuerdo de confidencialidad Manipulación inadecuada de la documentación recepcionada por el personal de la Entidad. Falta de valores y compromiso con la Entidad Intereses a favor de terceros Incumplimiento de los Roles y Responsabilidades para la seguridad de la Información.	IMPROBABLE
Ausencia de medidas para evitar la pérdida de datos, por ejemplo copias de respaldo. Falta de pruebas regulares a las copias de respaldo. Ausencia de manuales para la administración de las herramientas de aplicaciones. Administrador de servidores sin conocimiento de las políticas de seguridad de la información. El respaldo de Backup está ubicado en los mismos servidores a los cuáles se les realiza las copias de respaldo	RARA VEZ
Vulnerabilidades técnicas sin conocer, uso de software desactualizado Intrusión de personal no autorizado a la plataforma tecnológica Acceso sin autorización locales, remotos y a los centros de cableado o de la UPS	

Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) Falta de políticas, controles de seguridad, no existen procedimientos establecidos para la restricción de acceso a la infraestructura física de la organización Falta de socialización acerca de las diferentes modalidades de ciberataques	RARA VEZ
Ausencia de canal de respaldo, acuerdos de nivel de servicio con el proveedor sin establecer. Falta de respaldo de los servicios de suministro (aire, energía, entre otros).	POSIBLE
Ausencia de políticas para la gestión y uso de contraseñas Falta de sensibilización y capacitación en el manejo y uso de contraseñas Personal inconforme al interior de la Entidad o poco compromiso ante las políticas de Seguridad de la Información. Robo o usurpación de contraseñas	IMPROBABLE

Ausencia de controles que protejan la información transferida y las instalaciones de procesamiento de información de soporte No hay un proceso establecido para la administración y gestión de usuarios al interior de la entidad. Ausencia de procesos que establezcan los procedimientos para habilitar o deshabilitar las cuentas de usuario. No existe un registro actualizado de los usuarios que tienen acceso a los aplicativos y servicios ni se identifica su estado (Activo, Bloqueado, Deshabilitado). Deficiencias en las configuraciones de seguridad de la red, incluida la inalámbrica, empleando un cifrado débil. Ausencia de un administrador de red que configure, administre y gestione la red bajo criterios de seguridad de la información. No se aplican políticas de seguridad de la información.	RARA VEZ
Controles de acceso al correo electrónico inadecuados, uso de contraseñas débiles, uso de cifrados débiles	RARA VEZ
Ausencia de controles adecuados para la transferencia de información Cifrados débiles	RARA VEZ

Ausencia de herramientas que permitan asegurar el transporte de la información	
Accesos lógicos sin retirar, novedades de funcionarios y/o contratistas sin reportar, ausencia de acuerdos de confidencialidad Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) y/o ataque informático interno por parte de un funcionario o contratista con acceso, a la plataforma tecnológica Incumplimiento del procedimiento de clasificación y etiquetado documental Ausencia de implementación de procesos, procedimiento y políticas que permitan preservar y mantener los pilares referentes a Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad)	RARA VEZ
Desconocimiento de la legislación Colombiana y de los procedimientos internos de la Entidad Incomprensión de las nuevas leyes y reglamentos y la identificación de la legislación aplicable Procedimientos inadecuados de contratación de personal. Procedimiento insuficiente para el cumplimiento de los requisitos de propiedad intelectual	RARA VEZ

Uso de controles criptográficos débiles, protección inadecuada a llaves criptográficas, ausencia de políticas para asegurar el uso apropiado de controles criptográficos Protocolos de certificación para paginas seguras sin licencia o vencidos Desconocimiento de Políticas sobre teletrabajo y trabajo remoto Falta de Monitoreo de tráfico de red a través de la VPN. Falta de parches de seguridad del sistema operativo del equipo conectado. Falta de actualización de firmas del software antivirus	POSIBLE
Exclusión de la seguridad de la información en la planificación de la continuidad del negocio Obsolescencia Tecnológica Plan de contingencia y guías desactualizadas Eventos catastróficos: inundaciones, incendios, terremotos, ataques terroristas, disturbios civiles pandemia La entidad no tiene el control sobre las medidas de protección utilizadas por el usuario para salvaguardar los datos y evitar perdida de integridad y confidencialidad de la información a la que accede desde trabajo en casa.	IMPROBABLE

Falta de identificación de rangos críticos Saturación de capacidad de almacenamiento. Falta de reporte de alarmas en los arreglos de discos	POSIBLE
No se realiza una valoración de los riesgos de seguridad de la información en una etapa temprana del proyecto con el fin de identificar los controles necesarios . Falta de integración de la seguridad de la información en la gestión de proyectos. Inadecuada gestión de estudio de mercado, viabilidad o especificación técnica del producto o servicio que permita dar cumplimiento del requerimiento	RARA VEZ
Falta de políticas que exijan la inclusión de requisitos de seguridad de la información para la adquisición, desarrollo y mantenimiento de sistemas Ausencia de una metodología de desarrollo de software seguro. No se realiza la gestión documental y/o actualización de control de versión para el desarrollo de nuevas funcionalidades del software permaneciendo de manera local en el equipo del desarrollador y no en el repositorio documental No se encuentra documentado los lineamientos de seguridad implementados en el desarrollo de software	RARA VEZ

Ausencia de procedimientos formales para el control de cambios. Ausencia de políticas para el control de cambios en los sistemas. Ausencia de transferencia de conocimiento y falta de capacitación técnica	POSIBLE

OPC

No Aplica	No Aplica

)AD Y PRIVACIDAD DE LA INFORMACIÓN 2023 -

RIESGO RESIDUAL		OPCION DE TRATAMIENTO
CALIFICACIÓN		
IMPACTO	EVALUACIÓN	
MODERADO	EXTREMO	Reducir el riesgo

MENOR	BAJO	Reducir el riesgo
MODERADO	MODERADO	Reducir el riesgo

MODERADO	MODERADO	Reducir el riesgo

MODERADO	MODERADO	Reducir el riesgo
MENOR	BAJO	Reducir el riesgo

MAYOR	ALTO	Reducir el riesgo
MENOR	BAJO	Reducir el riesgo

MODERADO	MODERADO	Reducir el riesgo
MODERADO	ALTO	Reducir el riesgo
MODERADO	MODERADO	Reducir el riesgo

MENOR	BAJO	Reducir el riesgo
INSIGNIFICANTE	BAJO	Reducir el riesgo
MENOR	BAJO	Reducir el riesgo

MENOR	BAJO	Reducir el riesgo
MENOR	BAJO	Reducir el riesgo

MODERADO	MODERADO	Reducir el riesgo
MAYOR	ALTO	Reducir el riesgo

MAYOR	ALTO	Reducir el riesgo
MODERADO	MODERADO	Reducir el riesgo
MODERADO	MODERADO	Reducir el riesgo

INSIGNIFICANTE	BAJO	Reducir el riesgo

ORTUNIDADES

No Aplica		No Aplica

CORANTIOQUIA

ACCIONES	ACTIVIDAD DE CONTROL
Revisiones periódicas y actualización de la política general y el manual de políticas de seguridad de la información cuando aplique.	Políticas para la seguridad de la información Revisión de la política
Dar cumplimiento con el diligenciamiento del acuerdos de confidencialidad para todos los funcionarios públicos de la Entidad	
Validar el cumplimiento de la política general y el manual de las políticas especificas de seguridad de la información.	
Definir y diligenciar el plan anual de capacitación, educación (formal y no formal). Formación en seguridad de la información (formal y no formal).	Toma de conciencia, educación y formación en la seguridad de la información
Socializar la política general y manual de seguridad de la información aprobada por la alta dirección, por medio de: Correo electrónico, Intranet, Pagina Web, Sensibilizaciones. (Dejar evidencia documentada)	

Hacer seguimiento a la implementación de las políticas de control de acceso lógico	Gestión de derechos de acceso privilegiado
Hacer seguimiento de las políticas de suministro de acceso formal de usuarios para asignar o revocar derechos de acceso	
Revisión periódica de la política de los derechos de acceso	Política de control de acceso
Revisión y seguimiento a la solución de las vulnerabilidades de cada componente.	
Seguimiento y control a los proveedores en la aplicación de los requisitos de seguridad en los sistemas de información, dando cumplimiento a la norma. Realizar seguimiento a las conexiones de los proveedores de acuerdo al objeto contractual (Validación de servidores, recursos, VPNs, etc)	Política de seguridad de la información para las relaciones con proveedores
	Tratamiento de la seguridad dentro de los acuerdos con proveedores
las que se encuentren en uso en los equipos. Controlar y asegurar que no se exceda el numero de licencias asignadas a usuarios. Adquirir software de fuentes conocidas y confiables para asegurar que no se violen los derechos de autor.	Derechos de propiedad intelectual

Actualizar plan de continuidad del negocio	Protección contra amenazas externas y ambientales
Verificar el cumplimiento del control de acceso al centro de datos	Ubicación y protección de los equipos
Establecer plan de mantenimientos preventivos a los equipos de la infraestructura tecnológica para el periodo	
Realizar inspecciones periódicas de los equipos tecnológicos y de respaldo (servidores, UPS, planta eléctrica) para verificar su funcionamiento y ejecutar las correcciones necesarias	Servicios de suministro
Validar y poner a prueba sistemas de redundancia suficiente para los servicios y arquitectura crítica usados para el procesamiento de información	Implementación de la continuidad de la seguridad de la información Disponibilidad de instalaciones de procesamiento de información.

Verificar el cumplimiento de las políticas de teletrabajo y trabajo remoto establecidos por la Corporación	Teletrabajo Gestión de derechos de acceso privilegiado Restricciones sobre la instalación de software
Verificar el cumplimiento de las políticas para la gestión de vulnerabilidades técnicas y para la restricción de instalación de software en sistemas operativos	
Verificar la aplicación del procedimiento para la restricción de la instalación de software en sistemas operativos	
Verificar la pertinencia y aplicación de las reglas para el manejo de la gestión de los medios removibles.	Controles contra códigos maliciosos
Cumplimiento de las políticas para la protección contra código malicioso en servidores y equipos de cómputo.	

Realizar pruebas de restauración de las copias de respaldo de la información, software e imágenes de los sistemas para este periodo. Verificar el almacenamiento adecuado de las copias de respaldo. Monitores y seguimiento de la ejecución de las copias de respaldo con el fin de asegurar el correcto procedimiento (Completitud de los datos y registros) durante la gestión.	Respaldo de información
Validar los requisitos de seguridad en la custodia de cintas al proveedor (Transporte, instalaciones, manipulación, etc.).	Cadena de suministro de tecnología de información y comunicación
Dar cumplimiento con la política y procedimientos para la realización de backups a software, imágenes de los sistemas operativos, e información crítica Verificación de las copias de respaldo por medio de pruebas de restauración	Respaldo de información
Establecer contacto con grupos de interés, especializados en seguridad de la información	

Desarrollar pruebas de vulnerabilidades periódicas	Contacto con grupos de interés especial Gestión de las vulnerabilidades técnicas
Instalación de nuevas versiones de software	
Establecer redundancia en los servicios críticos de la Entidad	Seguridad de los servicios de red Disponibilidad de instalaciones de procesamiento de información
Solicitar al proveedor principal activación de una comunidad SNMP para monitoreo interno.	
Seguimiento a los acuerdos de nivel de servicio con los Proveedores de los servicios críticos.	
Dar cumplimiento a las políticas de seguridad de la información relacionadas con el uso adecuado de contraseñas por parte de los usuarios.	Sistema de gestión de contraseñas
Validar el cumplimiento de las políticas de asignación de contraseñas temporales seguras cuando se crean usuarios	
Verificar el cumplimiento de la política de cambio de contraseña de cuentas de administración genéricas cada vez que expire el tiempo de acceso concedido a un funcionario, exfuncionario, contratista y/o proveedor.	
Validar el funcionamiento de la herramienta para gestión de contraseñas	

Incluir en el plan de sensibilización y capacitación temas asociados al uso adecuado de contraseñas para este periodo.	
Verificar que a nivel de Switch se deshabilitan los puertos que no están en uso	Controles de redes Seguridad de los servicios de red Separación en las redes
Verificar el funcionamiento de la autenticación en redes Wi-Fi mediante los protocolos seguros (WPA2)	
Verificar el uso de protocolos de comunicación seguros (HTTPS)	
Hacer seguimiento a la implementación de servicios y/o equipos que brinden seguridad perimetral	
Verificar la separación de la red de la entidad mediante VLANS	
Socialización a los usuarios en medios de comunicación sobre los riesgos a los cuales están expuestos por medio del correo electrónico para este periodo	Protección de transacciones de los servicios de las aplicaciones
Validar o realizar mantenimiento a los procedimientos y controles para la transferencia de información durante el transito de la misma, además de los niveles aceptables de control de acceso.	Política de desarrollo seguro
	Procedimientos de control

Establecer acuerdos para intercambio de información con entes de control	Procedimientos de control de cambios en sistemas
Verificar el control y seguimiento a la gestión de usuarios	Teletrabajo Terminación o cambio de responsabilidades de empleo
Verificar el cumplimiento de las políticas de teletrabajo y trabajo remoto establecidos por la Corporación	
Dar cumplimiento con el diligenciamiento del acuerdos de confidencialidad para todos los funcionarios públicos de la Entidad	
Verificación del procedimiento en el proceso de cambio o terminación de empleo	
Verificar la aplicación de protocolos de verificación sobre los antecedentes de los funcionarios que estén acorde a las funciones u obligaciones laborales	Selección Términos y condiciones del empleo Proceso disciplinario Terminación o cambio de responsabilidades de empleo
Validar procedimiento de vinculación y retiro laboral desde las áreas pertinentes (Gestión administrativa y Talento humano).	

Hacer seguimiento a la Implementación de controles criptográficos y gestión de llaves criptográficas para este periodo Divulgación de Políticas sobre teletrabajo y trabajo remoto	Teletrabajo Política sobre el uso de controles criptográficos
Realizar seguimiento periódico del plan de continuidad del negocio para asegurar e incorporar los aspectos derivados de la gestión de Seguridad de Información.	Planificación de la continuidad de la seguridad de la información Implementación de la continuidad de la seguridad de la información Verificación, revisión y evaluación de la continuidad de la seguridad de la información
Monitoreo de conexiones de red o Análisis de tráfico de red Firewall para protegerse ante amenazas y minimizar los riesgos que comprometan la información Conexiones seguras a través de la VPN	

Seguimiento y monitoreo periódico de los componentes de la plataforma tecnológica	Gestión de capacidad
Validar la aplicabilidad de la metodología de proyectos y la inclusión de requisitos sobre la seguridad de la información.	Seguridad de la información en la gestión de proyectos
Aplicar la valoración de riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios.	
Realizar seguimiento a los riesgos identificados y a los controles implementados para tratar los riesgos durante las fases del proyecto.	
Establecer e implementar políticas para la protección de ambientes de desarrollo.	Seguridad en los procesos de desarrollo y de soporte Ambiente de desarrollo seguro
Verificar la aplicación de las metodologías en desarrollo seguro.	
Implementación de herramientas actualizadas a la última versión estable.	

Verificar la pertinente o actualización de los procedimientos de gestión de cambios adoptados	Procedimientos de control de cambios en sistemas

Asistencia a capacitaciones ofrecidas por el Min Tic. Revisión de documentación generada por el Min Tic y relacionada con seguridad de la información. Asesoría en seguridad de la información dada por personal de Min Tic. Implementación de guías generadas por el Min Tic-MSPI.	No Aplica

SOPORTE	INDICADOR
Política general de seguridad de la información aprobada por la alta dirección	Evidencia de seguimiento
Cláusula de confidencialidad en los contratos de prestación de servicios Acuerdos de confidencialidad firmados	Evidencia de seguimiento
Manual de políticas especificas de seguridad de la información aprobado por el Comité Directivo.	Cumplimiento de políticas y manual de seguridad de la información **# Políticas satisfactorias / # Políticas medibles**
Plan anual de capacitación de la entidad Invitaciones y asistencia a foros, talleres y charlas relacionadas con seguridad de la información	Evidencia de seguimiento
Plan de medios de comunicación de seguridad de la información (Información, tips, recomendación y temas generales en seguridad)	

Perfiles y privilegios de administración asignados para ciertos administradores de las plataformas	Evidencia de seguimiento
Política para el control de acceso definida	
Archivo de seguimiento a la remediación de las vulnerabilidades	
Se establecerá que el proveedor debe cumplir con las políticas de seguridad de la información de la entidad.	Evidencia de seguimiento
Clausula de confidencialidad en los contratos suscritos con proveedores y contratistas Acuerdo de confidencialidad para proveedores	
Clausula de derechos de propiedad intelectual en los contratos suscritos con proveedores y contratistas.	Evidencia de seguimiento

Sistema de detección y prevención de incendios. Plan de continuidad del negocio para montar servicios en centro de datos alterno.	Evidencia de seguimiento
Bitácora de acceso al Datacenter	
Mantenimientos a aire acondicionado, switches, cuchillas, servidores, etc.	
Sistema de Alimentación Ininterrumpida (UPS) con autonomía de 16 minutos. Planta Eléctrica con autonomía de 10 horas	Evidencia de seguimiento
Pruebas realizadas a los planes de contingencia de los servicios críticos	

Cumplimiento de la política general de seguridad de la información aprobada por la alta dirección y el Manual de Políticas de Seguridad de la Información.	Monitoreo de logs Evidencia de seguimiento
Formato -Administración de cambios a TI	Detección de vulnerabilidades # Test ejecutados / # Total test programados
Perfiles y privilegios de administración asignados para ciertos usuarios	Evidencia de seguimiento
Se monitorea con la consola de antivirus Sophos.	Evidencia de seguimiento
Al conectar dispositivos USB el antivirus automáticamente realiza un escaneo el cual no se puede cancelar por parte del usuario.	Evidencia de seguimiento
Se controlan desde la consola las actualizaciones de las bases de datos de virus.	

Restauración de copias de respaldo de información	Evidencia de seguimiento
Protocolos y procedimientos de seguridad de la información del proveedor	
Evidencia de respaldo y restauración Diligenciamiento del formato -Seguimiento y control de seguridad de la información	Cumplimiento de la política de copias de respaldo a servidores **# Reportes ejecutados / # Reportes programados**
Cierre de puertos. Monitoreo de Logs	Evidencia de seguimiento

Pruebas de vulnerabilidad periódicas	Detección de vulnerabilidades **# Test ejecutados / # Total test programados**
Actualización de software para mitigar riesgos de seguridad.	
Software de monitoreo. Eventos y alarmas de los componentes de infraestructura tecnológica Línea de soporte del proveedor de internet para reporte de indisponibilidad del servicio.	Evidencia de seguimiento
Políticas de control de contraseñas en el servidor de dominio.	Evidencia de seguimiento
Configuración en el servidor de dominio para cambio de contraseñas	
Se realizan sensibilizaciones por medio de los Tips de seguridad de la información a través de Corantioquia al día.	

A nivel de Switch se deshabilitan los puertos que no están en uso	Evidencia de seguimiento
Autenticación a la Wifi a través del directorio activo para la red inalámbrica corporativa	Evidencia de Seguimiento
En la red de invitados se cuenta con seguridad (WPA2)	Evidencia de Seguimiento
	Evidencia de Seguimiento
Envío de mensajería electrónica mediante HTTPS Encriptación estándar (TLS)	Evidencia de Seguimiento
Uso de certificados digitales para servicios críticos	Evidencia de Seguimiento
Uso de protocolos de comunicación SFTP	

Uso de VPN con certificados y autenticación	Evidencia de Seguimiento
Cada usuario de la VPN tiene asignadas reglas de conexión dentro del firewall	
Diligenciamiento de cada uno de los formatos de gestión de acceso, de acuerdo a los diferentes sistemas de información de la Entidad.	Evidencia de seguimiento
Cumplimiento de la política general de seguridad de la información aprobada por la alta dirección y el Manual de Políticas de Seguridad de la Información.	
Acuerdo de confidencialidad firmado por todos los funcionarios públicos. Cláusula de confidencialidad en los contratos de prestación de servicios	
Procedimiento de novedades	
Normograma y demás lineamientos que aplican	Evidencia de seguimiento
Manual de contratación, Ley 80 y sus decretos	
Procedimiento de vinculación y retiro laboral	Evidencia de seguimiento

Cumplimiento de la política general de seguridad de la información aprobada por la alta dirección y el Manual de Políticas de Seguridad de la Información. Monitoreo de Logs Implementación de sistema de autenticación de doble factor (tokens) y certificados SSL	Evidencia de seguimiento
Backup de las aplicaciones y bases de datos de las aplicaciones misionales Plan de Contingencia de la Entidad Plan de continuidad del negocio Centro de datos ubicado en sitio alterno	Evidencia de seguimiento
Reporte de amenazas Reporte de VPN Reporte de usuarios conectado	Evidencia de seguimiento

Implementación de scripts para el monitoreo a los recursos de los servidores y notificación por correo electrónico del estado al administrador	Evidencia de seguimiento
En el formato de ESPECIFICACIONES TECNICAS se establece un ítem de requerimientos mínimos obligatorios de ESPECIFICACIONES DE SEGURIDAD INFORMÁTICA DE PRODUCTO Y/O SERVICIO	Evidencia de seguimiento
Formato Orden de cambio Formato -Documento de especificación	Evidencia de seguimiento

Formato Administración de cambios a TI	Evidencia de seguimiento

	No Aplica