1. OBJETO Y CAMPO DE APLICACIÓN

Este documento establece las prácticas para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en la Corporación para el Desarrollo Sostenible del Urabá – CORPOURABA. Estas prácticas se enmarcan en los Planes Estratégicos de Tecnologías de la Información (PETI) y de Seguridad de la Información (PESI), así como en el Modelo de Seguridad y Privacidad de la Información (MSPI), y abarcan la seguridad funcional, la coordinación, la documentación, la capacitación, la administración de configuraciones de sistemas y de seguridad informática, y la gestión de riesgos.

La aplicación de estas prácticas es periódica, según lo definido en el numeral "3.3. Actividades de Administración y Seguridad Informática", con el fin de:

Definir las responsabilidades en la gestión de la seguridad de la información en la Corporación.

- Servir como guía y lista de verificación para la ejecución de actividades.
- Establecer la estructura del área de informática de la Corporación.
- Estructurar la valoración y el tratamiento de los riesgos de seguridad de la información, adaptándolos a las necesidades de la Corporación.

2. NORMATIVIDAD

- LEY 1712 DE 2014, *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."*
- LEY ESTATUTARIA 1581 DE 2012, *"Por la cual se dictan disposiciones generales para la protección de datos personales".*
- LEY 1273 DE 2009, *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*
- LEY ESTATUTARIA 1266 DE 2008, *"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".*
- LEY 734 DE 2002, *"Por la cual se expide el Código Disciplinario Único".*
- Decreto 1078 de 2015, *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".*
- CONPES 3854 DE 2016, Política Nacional de *Seguridad Digital*
- Decreto 620 de 2020*, "Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo*

45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales".

- Resolución 1126 de 2021 *"Por la cual se modifica la Resolución 2710 de 2017, por la cual se establecen lineamientos para la adopción del protocolo IPv6"*
- Resolución 1519 del 2020 *"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"*
- Resolución 00500 de marzo 10 de 2021 *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"*

3. TÉRMINOS Y DEFINICIONES[1]

- **Acceso Controlado:** Mecanismos para asegurar que el acceso a los activos de información esté autorizado y restringido según las necesidades operativas y los requisitos de seguridad.
- **Ataque**: Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo de información.
- **Autenticación**: Proceso de verificar la identidad de una entidad o usuario.
- **Disponibilidad**: Característica de la información de estar accesible y utilizable cuando un usuario autorizado la requiere.
- **Competencia**: Capacidad demostrada para aplicar conocimientos y habilidades y alcanzar los resultados esperados.
- **Confidencialidad**: Propiedad de la información de no ser divulgada o puesta a disposición de personas, entidades o procesos no autorizados.
- **Control**: Medida implementada para modificar un riesgo.
- **Evento**: Suceso o cambio en un conjunto de circunstancias.
- **Gobernanza de la Seguridad de la Información:** Conjunto de políticas, procedimientos y responsabilidades que dirigen y controlan las actividades de seguridad de la información de la organización.
- **Necesidad de Información:** Requisito de conocimiento para la gestión de objetivos, riesgos y problemas.
- **Instalaciones de Procesamiento de Información:** Cualquier sistema, servicio o infraestructura de procesamiento de información, incluyendo las ubicaciones físicas que los albergan.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Continuidad de la Seguridad de la Información:** Procesos y procedimientos establecidos para asegurar la continuidad de las operaciones de seguridad de la información ante interrupciones.
- **Incidente de Seguridad de la Información:** Evento o serie de eventos no deseados o inesperados que tienen una alta probabilidad de comprometer las operaciones de la organización y amenazar la seguridad de la información.
- **Sistema de Información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información y otros componentes para la gestión de la información.

[1] Extractado de https://normaiso27001.es/referencias-normativas-iso-27000/#def31

- **Estándar de Implementación de Seguridad:** Documento que especifica los métodos autorizados para implementar la seguridad.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema o a la organización.

4. CONTEXTO DE LA ORGANIZACIÓN

CORPOURABA interactúa con las siguientes entidades del gobierno nacional en temas de seguridad informática:

- COLCERT: Grupo de Respuestas a Emergencias Cibernéticas de Colombia.
- CCP: Centro Cibernético de la Policía Nacional.
- CSIRT: Equipo de Respuesta ante Incidencias de Seguridad Informáticas.
- Grupo de transformación digital del SIAC: adscrito al Ministerio de Ambiente y Desarrollo Sostenible.

Además, CORPOURABA se relaciona con todos sus funcionarios y contratistas, según su organigrama.

5. LIDERAZGO

5.1. LIDERAZGO Y COMPROMISO

Los roles de liderazgo en la gestión de TI y seguridad de la información son:

- **Dirección General:** Responsable de la aprobación de las actividades de TI y la ordenación del gasto.
- **Subdirección de Planeación y Ordenamiento Territorial:** El Subdirector de Planeación y Ordenamiento Territorial ejerce como Jefe de TI.

5.2. Política del Sistema de Gestión de Seguridad de la Información

La Dirección General de CORPOURABA, reconociendo la importancia de la gestión adecuada de la información, se compromete con la implementación de un SGSI para establecer un marco de confianza en el cumplimiento de sus responsabilidades con el Estado y los ciudadanos. Este compromiso se alinea con las leyes aplicables, la misión y visión de la Corporación, y las políticas de Calidad y del Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST).

CORPOURABA busca, a través de la protección de la información, minimizar el impacto de los riesgos identificados sobre sus activos, manteniendo un nivel de exposición aceptable que garantice la integridad, confidencialidad y disponibilidad de la información, en concordancia con las necesidades de los grupos de interés.

Esta política aplica a toda la Corporación, incluyendo funcionarios, contratistas, aprendices, practicantes, proveedores y la ciudadanía, y se fundamenta en los siguientes principios:

- Minimizar el riesgo en las funciones críticas de la entidad.

- Cumplir con los principios de seguridad de la información y de la función administrativa.
- Mantener la confianza de los usuarios, entes de control y empleados.
- Apoyar la innovación tecnológica y proteger los activos tecnológicos.
- Establecer políticas, procedimientos e instructivos de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en CORPOURABA.
- Garantizar la continuidad de la Corporación ante incidentes.
- CORPOURABA se compromete a definir, implementar, operar y mejorar continuamente el SGSI, basándose en lineamientos claros, alineados con las necesidades de la Corporación y los requisitos regulatorios aplicables.

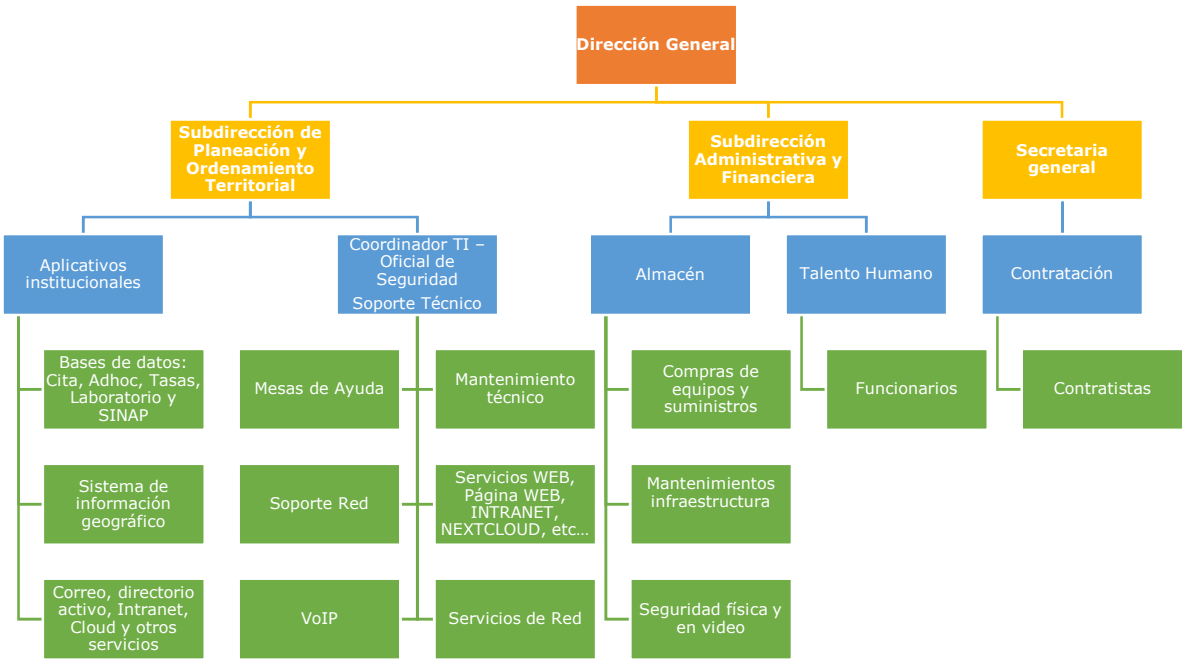
5.3. políticas de Seguridad de la Información

El Sistema de Gestión de Seguridad del a Información (SGSI) de CORPOURABA se soporta en las siguientes 12 políticas de seguridad:

1. CORPOURABA definirá, implementará, operará y mejorará continuamente un Sistema de Gestión de Seguridad de la Información, basado en los lineamientos del gobierno nacional, las necesidades de los procesos y los requisitos regulatorios pertinentes.
2. Las responsabilidades en materia de seguridad de la información serán definidas, comunicadas, publicadas y aceptadas por todos los funcionarios, contratistas y terceros.
3. CORPOURABA protegerá la información generada, procesada o custodiada por los procesos misionales y los activos de información asociados.
4. CORPOURABA protegerá la información creada, procesada, transmitida o custodiada por sus procesos, con el fin de minimizar los impactos financieros, operativos o legales derivados de su uso incorrecto.
5. La aplicación de los controles aprobados, de acuerdo con la clasificación de la información propia o en custodia de la Corporación, es fundamental.
6. CORPOURABA protegerá su información de las amenazas originadas por los servidores públicos.
7. CORPOURABA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soportan sus procesos críticos.
8. CORPOURABA controlará la operación de sus procesos, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
9. CORPOURABA implementará controles de acceso a la información, los sistemas y los recursos de red.
10. CORPOURABA garantizará que la seguridad sea un componente integral del ciclo de vida de los sistemas de información.
11. CORPOURABA garantizará la mejora continua de su modelo de seguridad a través de una gestión eficaz de los eventos de seguridad y las vulnerabilidades asociadas a los sistemas de información.
12. CORPOURABA garantizará la disponibilidad de sus procesos y la continuidad de sus operaciones, considerando el impacto potencial de los eventos.

CORPOURABA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales aplicables

6. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA CORPORACIÓN



La asignación de responsabilidades en el área de sistemas de la Corporación se distribuye entre funcionarios y personal externo de la siguiente manera:

6.1. Funcionarios de la Corporación

- **Dirección General:**
  - Ordena los gastos relacionados con TI.
  - Aprueba las actividades del área de TI.
- **Subdirección de Planeación y Ordenamiento Territorial (SPOT):**
  - El Subdirector de Planeación y Ordenamiento Territorial ejerce el rol de Jefe de TI, siendo responsable de la dirección estratégica y operativa del área.
  - Un Profesional Universitario, designado por el Jefe de TI, actúa como Coordinador de TI, apoyando en la gestión de proyectos y procesos del área.
  - Un Contratista o quien sea designado por el Jefe de TI, actúa como Oficial de Seguridad, encargado de la seguridad informática de la Corporación.
- **Subdirección Administrativa y Financiera:**
  - El Almacenista conjuntamente con la SPOT coordina las compras de equipos y suministros de TI, así como el mantenimiento de la infraestructura tecnológica y los sistemas de seguridad física y video.
- **Administradores de los Sistemas:**
  - A cada sistema de información se le asigna un administrador, quien debe asegurar el cumplimiento de los procedimientos establecidos por el Jefe de TI para mantener un nivel adecuado de seguridad de la información.

6.2. Soporte Tecnológico Tercerizado

El soporte tecnológico en sistemas se proporciona a través de un servicio externo:

- **Director y/o Coordinador del Área de Soporte (o quien haga sus veces):**
  - Un Ingeniero de Telecomunicaciones, Sistemas, Electrónico y/o afín es responsable del seguimiento del soporte tecnológico proporcionado y de la identificación de oportunidades de mejora en el servicio.

- **Personal In Situ:**

  - Uno o varios Tecnólogos en Telecomunicaciones, Sistemas, Electrónico y/o afín es responsable de brindar soporte técnico al usuario final en las instalaciones de la Corporación.

6.3. Manejo de Aplicativos

El desarrollo y mantenimiento de aplicativos se gestiona mediante contratos externos, que pueden incluir mesas de ayuda y/o nuevos desarrollos. La supervisión o interventoría de estos contratos es definida por el Subdirector de Planeación y Ordenamiento Territorial y/o la Directora General.

6.4. Roles de Usuario Final

Además de los roles específicos del área de sistemas, se definen roles y responsabilidades para los usuarios finales de los servicios de TI.

6.5. Usuarios y Servicios en las Oficinas de Trabajo

- Se consideran usuarios de CORPOURABA a todos los funcionarios (vinculados) y contratistas (terceros) activos en la Corporación.
- Los nuevos funcionarios, terceros y contratistas que requieran utilizar los servicios de TI deben ser registrados por su área correspondiente ante el área de sistemas, mediante el diligenciamiento del formato "R-RI-80: ROLES Y ACUERDO DE RESPONSABILIDADES USUARIOS TI".

7. PLANIFICACIÓN

7.1. ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES

CORPOURABA ha establecido el procedimiento "P-MJ-11 ADMINISTRACIÓN DEL RIESGO" para definir los lineamientos que rigen el diligenciamiento del formato "R-MJ-10 MAPA DE RIESGOS". Este procedimiento permite identificar, valorar y definir el tratamiento de los riesgos relacionados con la seguridad de la información, así como de otros riesgos que puedan afectar a la organización.

7.2. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS

CORPOURABA se compromete a alcanzar los siguientes objetivos de seguridad de la información, para lo cual se establecen los planes y acciones necesarios:

- Implementar, operar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).
- Proteger la información generada, procesada o resguardada por los procesos de la organización (directivos, evaluativos, misionales y de apoyo) y los activos de información asociados. Esto incluye controlar la operación de los procesos para garantizar la seguridad de los recursos tecnológicos y las redes de datos.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos de la organización.
- Garantizar la disponibilidad de los procesos y la continuidad de las operaciones, considerando el impacto potencial de los eventos que puedan afectarlos.
- Garantizar el cumplimiento de todas las obligaciones legales, regulatorias y contractuales aplicables a la organización en materia de seguridad de la información.

8. SOPORTE

8.1. RECURSOS

CORPOURABA asegura que las actividades relacionadas con la seguridad de la información y otras actividades de TI se financien con los recursos asignados en el Plan Operativo Anual de Inversiones, en consonancia con el cumplimiento de las metas establecidas en el Plan de Acción Cuatrienal.

8.2. COMPETENCIA

CORPOURABA define los requisitos de competencia para sus funcionarios en el "*Manual Específico de Funciones y Competencias Laborales de la Corporación para el Desarrollo Sostenible del Urabá -CORPOURABA"*. Los requisitos de competencia para los contratistas se establecen en los procesos de contratación.

8.3. TOMA DE CONCIENCIA

CORPOURABA imparte formación a los nuevos funcionarios en seguridad de la información y manejo de los servicios de TI, a través de los procesos de inducción, capacitación en el cargo y otros programas de capacitación. Además, se realizan procesos anuales de reinducción para todo el personal.

8.4. COMUNICACIÓN

CORPOURABA establece y mantiene mecanismos de comunicación interna y externa relevantes para el Sistema de Gestión de Seguridad de la Información (SGSI).

8.5. INFORMACIÓN DOCUMENTADA

Los lineamientos para la gestión de la información documentada de los sistemas de gestión de la Corporación se definen en el procedimiento "P-MJ-01 CONTROL DOCUMENTOS Y REGISTROS".

9. OPERACIÓN

9.1. PLANIFICACIÓN Y CONTROL OPERACIONAL

CORPOURABA define mediante los siguientes planes:

- "R-RI-81 PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN: PETI"
- "R-RI-82 PLAN ESTRATÉGICO DE SEGURIDAD DE LA IINFORMACIÓN Y MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN".

El seguimiento de estos planes está a cargo de la Subdirección de Planeación y Ordenamiento Territorial.

A continuación, se presentan las actividades realizadas con el fin de dar cumplimiento a los objetivos de control y controles que se enumeran en la "Table A.1. Objetivos de control y controles", relacionada en la norma ISO/IEC 27001:2013, la cual se toma como base para la implementación del SGSI.

A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

A.5.1.1 Políticas para la seguridad de la información

Las políticas de seguridad de la información de la Corporación se detallan en el numeral 5.2 de este documento.

La aprobación de estas políticas se realiza mediante resolución emitida por la Dirección General, basada en la elaboración del Coordinador del SGC. Su divulgación a funcionarios y contratistas se efectúa a través de la INTRANET, correo corporativo y los espacios del lunes técnico, mientras que a las partes externas se comunica mediante su inclusión en los procesos de contratación pertinentes. Las políticas de seguridad de la información de la Corporación se detallan en el numeral 5.2 de este documento.

La aprobación de estas políticas se realiza mediante resolución emitida por la Dirección General, basada en la elaboración del Coordinador del SGC. Su divulgación a funcionarios y contratistas se efectúa a través de la INTRANET, correo corporativo y los espacios del lunes técnico, mientras que a las partes externas se comunica mediante su inclusión en los procesos de contratación pertinentes

A.5.1.2 Revisión de las políticas para la seguridad de la información

Las políticas se revisan anualmente según programación del SGC, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

En el numeral 5.3 de este documento se encuentran Roles, Responsabilidades Y Autoridades En La Corporación.

Estos roles incluyen tanto la estructura de la Corporación definida en el manual de funciones, la estructura de TI que se encuentra en este documento, las relaciones con proveedores y contratistas y las relaciones con entes territoriales, entes de control y otros entes gubernamentales.

A.6.1 Organización interna

A.6.1.1 Roles y responsabilidades para la seguridad de la Información:

Busca establecer el marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la Corporación

A.6.1.2 Separación de deberes:

Tabla de responsabilidades en SI: Se presentan y asignan las responsabilidades de los funcionarios y contratistas en materia de la seguridad de la información.

Rol	Responsabilidad
Dirección General	Ordenador de gasto y líder del SGSI
Subdirector de Planeación y Ordenamiento Territorial	Director de TI
Coordinador TI –	Realizar seguimiento a los contratos de TI, administrar el presupuesto asociado y supervisar su ejecución.
Oficial de Seguridad	Brindar los servicios de seguridad en la corporación, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la corporación
Soporte Técnico	Prestar asesoría y soporte tecnológico en redes, equipos y software y atender al usuario final
Almacén	Control de los equipos, infraestructura y software de propiedad de la Corporación
Talento Humano	Realizar contratación de personal que esté directa o indirectamente involucrado con TI, garantizar su formación y propiciar la capacitación en temas de TI
Contratación	Realizar procesos de contratación que estén directa o indirectamente involucrado con TI.
Responsables de Aplicativos	Coordinar y/o supervisar los contratos de actualización, establecer línea directa con el proveedor y verificar el funcionamiento del aplicativo,
Dueños de la información	Definir la clasificación de la información, determinar los niveles de acceso a la información y asignar permisos.

Funcionarios	Acatar las indicaciones sobre el manejo del software, Hardware y la infraestructura de TI, asistir a las capacitaciones programados y reportar los incidentes.
Contratistas	Acatar las indicaciones sobre el manejo del software, Hardware y la infraestructura de TI, cumplir las recomendaciones impartidas en esta materia y reportar los incidentes.

A.6.1.3 Contacto con las autoridades:

Tabla contactos autoridades pertinentes.

Autoridad	Grupo
Policía Nacional	Grupo de respuesta a emergencias cibernéticas (COLCERT)
	Centro Cibernético Policial (CCP)
	CSIRT
Contraloría	Contraloría General de la Nación
Procuraduría	Procuraduría General de la Nación
Fiscalía	Fiscalía General de la Nación

A.6.1.4 Contacto con grupos de interés especial

Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

Foro o Grupo	Contacto	Observaciones
Transform_Digital SIAC	300 4069787 - Fernando Bolívar - MADS	Transformación Digital Sector Ambiente
Iccn sector	316 8069934 – Renato MADS	Seguridad digital

A.6.1.5 Seguridad de la información en la gestión de proyectos:

La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. Para ello en todos los contratos que involucran TI una cláusula sobre seguridad de la información.

A.6.2 Dispositivos móviles y teletrabajo:

A.6.2.1 Política para dispositivos móviles

Se adopta la política y se establecen medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

- Control de acceso a todos los dispositivos de la Corporación.
- Responsabilidad de los usuarios para el manejo de la información
- Seguimiento a las instalaciones y actualizaciones de los antivirus.
- Suspensión por periodos de inactividad
- Copias de seguridad en la nube o dispositivos de la corporación

- Revisión y/o registro ante la oficina de TI de todos los equipos de cómputo portátiles que utilizan la red corporativa principal y/o los discos corporativos
- Los usuarios deben evitar conectarse a redes inseguras
- Los usuarios no deben modificar las condiciones de seguridad ni instalar software no permitido

A.6.2.2 Teletrabajo Control

Se implementan políticas y medidas de seguridad y de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el teletrabajo.

- Uso de VPN autorizada por la oficina de TI y con controles de acceso duplicados, el usuario no puede compartir esta información.
- Identificación del usuario que tiene acceso y lugar (o equipo portátil) desde donde se conecta.
- Cumplir con las recomendaciones de MINTIC y Mintrabajo sobre el tema.
- Realizar periódicamente evaluaciones del cumplimiento de estas recomendaciones.

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

A.7.1 Antes de asumir el empleo

Busca asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

A.7.1.1 Selección

La oficina de Talento Humano realiza las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos, siguiendo lo contemplado en el procedimiento *"P-TH-01: VINCULACIÓN DE SERVIDORES PÚBLICOS"* y la oficina de contratación verifica el cumplimiento de los requisitos del contratista siguiendo el procedimiento "*P-RI-04 CONTRATACION*"

A.7.1.2 Términos y condiciones del empleo

Todos los funcionarios y contratistas deben acoger y acatar estos termino al firmar el formato "*R-RI-80 ROLES Y RESPONSABILIDADES TI*" antes de su ingreso a laborar, al conocerlos se procede a darle las credenciales requeridas.

A.7.2 Durante la ejecución del empleo

Se debe asegurar de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan, para ello se realizan charlas periódicas de reinducción.

A.7.2.1 Responsabilidades de la dirección

Todos los funcionarios y contratistas deben acoger y acatar estos termino al firmar el formato "*R-RI-80 ROLES Y RESPONSABILIDADES TI*" antes de su ingreso a laborar, al conocerlos se procede a darle las credenciales requeridas.

.

A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Todos los funcionarios de la Corporación, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la Corporación pertinentes para su cargo, para ello la oficina de Talento Humano sigue el procedimiento "P-TH-03 FORMACIÓN, CAPACITACIÓN Y BIENESTAR".

Actividades diarias
Socialización de correos sospechosos de portar malware o phishing.
Bloqueo de IP´s sospechosos de portar malware, virus o phishing.

Actividades Trimestrales
Charlas o capacitaciones sobre seguridad de la información.

Actividades Anuales
Capacitar en nuevas tecnologías al personal administrativo de la red

A.7.2.3 Proceso disciplinario

Las entidades del estado se rigen por lo establecido en el Código Único Disciplinario Ley 734 de 2002 o la que la reemplace o modifique, el cual se comunica según lo contemplado en el plan de capacitación, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

A.7.3 Terminación y cambio de empleo

Busca proteger los intereses de la Corporación como parte del proceso de cambio o terminación de empleo.

A.7.3.1 Terminación o cambio de responsabilidades de empleo

Cuando se termina el vínculo laboral se sigue el procedimiento "*P-TH-08 RETIRO DEL SERVID PUBLICO*" y lo contemplado en el procedimiento "*P-RI-04 CONTRATACION*".

A.8 GESTIÓN DE ACTIVOS

A.8.1 Responsabilidad por los activos

Busca identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

A.8.1.1 Inventario de activos

El director, Coordinador, responsables de la información, Archivo y los contratistas de TI deben realizar el inventario de activos de información y mantenerlo actualizado.

El almacenista debe mantener el inventario de activos físicos y software de la Corporación.

A.8.1.2 Propiedad de los activos

Los activos mantenidos en el inventario deben tener un propietario designado por los funcionarios de los roles directivos de TI.

A.8.1.3 Uso aceptable de los activos

Toda la información y activos asociados con información e instalaciones de procesamiento de información deben ser usados para cumplir con el propósito para el cual fueron diseñados e implementados en la entidad, como lo determina el código único disciplinario.

Cualquier falla en los equipos y/o el software deben ser reportados a la oficina de TI.

La pérdida o robo de algunos de estos ítems debe informarse al almacén quien lo reportará a la oficina de Ti.

USO DEL CENTRO DE CÓMPUTO, DE LOS EQUIPOS DE CÓMPUTO Y DE LOS SERVICIOS DE TI.

I. Reglas Generales

- Los equipos de cómputo son herramienta de trabajo, los cuales benefician el logro de los objetivos de La Corporación para el desarrollo sostenible del Urabá CORPOURABA.
- El área de centro de cómputo es la parte esencial de la plataforma tecnológica, donde se encuentra el corazón de la red corporativa y desde este punto se reparte los servicios informáticos a los diferentes nodos de la misma.
- Es necesario integrar bancos de información, tanto en el aspecto bibliográfico, documental, informático y audiovisual, suficientes en cantidad y calidad, que corresponden a las necesidades laborales y de investigación de los funcionarios de CORPOURABA.

II. Administración del Centro de Cómputo

La Subdirección de Planeación y Ordenamiento Territorial tiene asignado un responsable para la administración del centro de cómputo, quien es el encargado de administrar en su parte física y lógica los servicios de la red de voz y datos de La Corporación. Es el único responsable que podrá acceder al área de centro de cómputo o autorizar el acceso a terceros; en caso de ausencia, el Subdirector de Planeación y Ordenamiento Territorial delegará un tercero para la administración del mismo.

Nota: La administración de la seguridad en cuanto a contraseña de cada uno de los servidores será responsabilidad del administrador del área de centro de cómputo.

III. Uso Adecuado de los Equipos de Cómputo

- La Corporación facilitará a los funcionarios los recursos de hardware y Software disponibles, para que sirvan como apoyo en sus actividades laborales.
- La administración de los equipos de cómputo, es responsabilidad de la Subdirección de Planeación y Ordenamiento Territorial y del personal encargado en el área de TIC.
- Todos los funcionarios que usen los equipos de la corporación y de los servicios de red deben estar identificados mediante un nombre de usuario y una clave, las cuales son asignadas por el área de sistemas. De acuerdo a las funciones propias del usuario se les asignan permisos a las diferentes áreas de almacenamiento y/o aplicativos de la Corporación.
- Todos los equipos de la corporación deben tener protección contra ataques por medio de antivirus o programas similares, lo mismo que la red de datos.

IV. Normas Básicas para la Utilización de las Oficinas donde hay Equipos de Cómputo

La utilización por parte de los usuarios de las oficinas de trabajo donde hay equipos de cómputo será de acuerdo con las siguientes condiciones:

- Los usuarios sólo pueden utilizar los servicios para los cuales están autorizados. No se permite tener acceso directo al servidor de la red, instalar Software en los equipos de cómputo sin la debida autorización de la subdirección.
- El uso de los equipos de cómputo y de los servicios de Red, deben ser para fines exclusivamente laborales. Está prohibido usar los equipos de La Corporación y los servicios de red para jugar, enviar o recibir información pornográfica o de propósito netamente comercial que no tengan que ver con los objetivos planteados por La Corporación.
- En caso de pérdida, daño o deterioro de los equipos usados, el usuario debe reportar inmediatamente al área de almacén, quien informará al área de TIC para proceder a su reparación, si es del caso. El área de TIC presentará un diagnostico

con las posibles causas que llevaron al evento de falla, según el reporte el Líder de cada área determinará las acciones a tomar.

- Cuando el área de almacén dé de baja un equipo de cómputo informa al área TIC, quien realiza el formateo del disco duro para evitar la fuga de información.

V. Servicios de Internet.

- El servicio de internet estará sujeto a los lineamientos de las directivas de La Corporación y la red corporativa debe utilizarse solo para fines de trabajo y la red de visitantes solo para las actividades personales o de los usuarios visitantes.

- El área de TIC no será responsable por problemas externos a la corporación de conectividad y comunicación, esta es responsabilidad de cada funcionario y/o del área de almacén para los planes de datos.

- El proveedor con acompañamiento del área de sistemas es responsable de la configuración inicial de los equipos.

- El uso del servicio de internet, estará restringido de acuerdo a los siguientes lineamientos de La Corporación.
    - Modificar o alterar los computadores para el acceso a sitios prohibidos.
    - Transmitir información no autorizada de propiedad de la Corporación o de sus usuarios y/o funcionarios
    - Acceder a páginas web con temática relacionada a pornografía, tráfico y construcción de armas, drogas, juegos en línea, hacking, cracking y/o cualquier página que presente contenidos en detrimento de la moral o que no estén autorizados por la función de la empresa.
    - Descargar y/o publicar todo tipo de software o contenido no autorizado por la Corporación y que atente contra la seguridad de la información y/o la propiedad intelectual de sus autores.

VI. Servicios de Correo Electrónico.

Todas las cuentas bajo el dominio corpouraba.gov.co son de propiedad de la Corporación de igual forma sus contenidos esto en concordancia con el código único disciplinario ley 734 de 2002, por lo que pueden ser monitoreados sin notificación previa, por Control Interno o entidades de control.

- La cuenta de correo asignada es de carácter individual; por lo tanto, ningún funcionario bajo ninguna circunstancia debe usar la cuenta de correo de otro funcionario.

- La cuenta de correo asignada solo debe ser usada para el desempeño de las funciones asignadas y los usuarios son responsables de todas las actividades realizadas con estas cuentas de correo.

- El proveedor de los buzones de correo es GOOGLE WORKSPACE, la Corporación ha adquirido tres tipos de Cuentas:

    - Plus: para puestos secretariales y notificaciones judiciales.
    - Standard: para los profesionales y/o técnicos que tienen amplio uso y se conectan a reuniones virtuales.
    - Starter: para contratistas
      Cada cuenta tiene configurados aspectos como seguimiento, tamaño y acceso a funcionalidades.

- Al enviar correos a múltiples destinatarios externos a la corporación, y con el fin de cumplir lo contemplado en la ley de protección de datos personales, las direcciones de correo deben ir en la sección “copia oculta”. Estos correos deben ser enviados solo de las cuentas institucionales.

- No se debe permitir la entrada ni salida de archivos ejecutables de aplicaciones, música, videos y presentaciones personales.

- El servicio de correo no debe tener restricciones de horario para los funcionarios y estará disponible 24 horas diarias, 7 días a la semana, para todos los usuarios inscritos.

- Se prohíben las cadenas de mensajes de cualquier tipo y la propaganda de tipo comercial, político o religioso entre otros y, cualquier contenido ofensivo para los funcionarios de la Corporación.

- Ante cualquier eventualidad en el correo asignado el usuario debe dar aviso a la oficina TI.

- Toda información enviada por correo debe llevar al final del cuerpo del mensaje la firma institucional del propietario del correo electrónico corporativo asignado por la oficina de comunicaciones.

- Es responsabilidad de los usuarios leer y responder oportunamente los correos electrónicos, dado que son Mecanismos Oficiales de Comunicación.

- El uso inapropiado del servicio de correo electrónico puede ocasionar sanciones disciplinarias para los funcionarios o la desactivación del mismo para los contratistas. Ejemplos de uso inapropiado:

    - Envío de correos masivos, cadenas de correo, mensajes con contenido no institucional o que atenten contra la dignidad o la ley.
    - Uso para fines comerciales ajenos a la entidad.
    - Usar mecanismos que intenten ocultar o suplantar la identidad del emisor.
    - Enviar correos SPAM.
    - Enviar archivos adjuntos con programas ejecutables.
    - Usar la cuenta como contacto para redes sociales para uso no institucional.

- Cuando se requiera enviar un correo a todos los correos asignados (sólo para información corporativa de interés para todos) se debe utilizar el grupo "corporacion@corpouraba.gov.co". Se solicita responder este correo solo a la persona o área que lo emite para evitar saturar a los usuarios del servicio. Las cuentas autorizadas para enviar estos correos masivos institucionales son:

    - Cuentas de los directivos de la corporación o sus secretarias y asistentes.
    - Cuenta de la funcionaria de talento humano
    - Cuenta de los responsables de seguridad de la información.
    - Cuenta del profesional de talento humano.
    - Cuenta de la jefe de oficina jurídica.
    - Cuenta del sindicato de la entidad.

- Las subdirecciones, áreas u oficinas pueden solicitar al área de TI la creación de los grupos que se requieran.

- Los correos de importancia para la corporación deben ser enviados con la opción de seguimiento de lectura, esta opción no debe utilizarse para los otros correos.

- Abstenerse de responder correos de remitentes desconocidos o con asuntos sospechosos, informar a la oficina de TI ante cualquier duda.

- Cuando un funcionario esté en comisión, vacaciones o fuera de oficina la oficina de TI debe configurar un mensaje y redireccionarlo, si es requerido, para que sea recibido por un delegado. Todo esto mediante comunicación de talento humano, acorde a lo contemplado en los procedimientos: "*P-TH-02 LIQUIDACIÓN DE NOMINA Y PRESTACIONES SOCIALES*" y "*P-RI-04 CONTRATACION".*

A.8.1.4 Devolución de activos

Todos los empleados y usuarios de partes externas deben devolver todos los activos de la Corporación que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo para lo cual se sigue el procedimiento "*P-TH-08 RETIRO DEL SERVIDOR PUBLICO*" y lo contemplado en el procedimiento "*P-RI-04 CONTRATACION*".

A.8.2 Clasificación de la información

Se debe asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Corporación.

A.8.2.1 Clasificación de la información

La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

A.8.2.2 Etiquetado de la información

Con base en la "*Guía para la Gestión y Clasificación de Activos de Información*[2]" se realiza el etiquetado de la información, de acuerdo con el esquema de clasificación de información, descrito en la ley 1712 del 2014.

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

.

- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.

.

- **Información pública reservada:** Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley.

A.8.2.3 Manejo de Activos *Control*

Con base en la "*Guía para la Gestión y Clasificación de Activos de Información*" se gestiona la información clasificada.

A.8.3 Manejo de medios

Se debe evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

A.8.3.1 Gestión de medios removibles

En la medida de lo posible toda información solicitada a la corporación y que requiere ser entregada en un medio removible debe ser enviada en CD para evitar la manipulación del archivo original, si bien no se controlan los medios removibles, el control se realiza como control de acceso a la información.

A.8.3.2 Disposición de los medios

Cuando ya no se requieran los medios removibles deben ser entregados al almacén para su reutilización en caso de ser un medio reescribible que se requiera desechar se entregará a la oficina de TI para su borrado seguro o destrucción.

A.8.3.3 Transferencia de medios físicos

En la medida de lo posible toda información solicitada a la corporación y que requiere ser entregada en un medio removible debe ser enviada en CD para evitar la

[2] https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

manipulación del archivo original, y debe estar embalado para evitar daños en el trasporte.

A.9 CONTROL DE ACCESO

A.9.1 Requisitos del negocio para control de acceso

Se debe limitar el acceso a información y a instalaciones de procesamiento de información.

A.9.1.1 Política de control de acceso y A.9.1.2 Acceso a redes y a servicios en red

Los equipos de la Corporación deben tener control de acceso, para lo cual solo el personal que se agregue al dominio puede hacer uso de los mismos.

El acceso a la red WIFI se realiza mediante contraseña de acceso.

A.9.2 Gestión de acceso de usuarios

Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

A.9.2.1 Registro y cancelación del registro de usuarios

Sólo se posibilita la asignación de los derechos de acceso a los usuarios nuevos que diligencien el formato "R-RI-80: ROLES Y ACUERDO DE RESPONSABILIDADES USUARIOS TI".

Para desactivar usuarios del dominio y de los servicios de Internet, Correo, entre otros… el usuario o su jefe inmediato diligencia el formato "R-TH-38: LISTA DE CHEQUEO ENTREGA INFORME PUESTO TRABAJO Y DE LOS BIENES Y VALORES ENCOMENDADOS".

A.9.2.2 Suministro de acceso de usuarios

Luego de cumplido los requisitos de ingreso la oficina de TI realiza la creación del usuario en el dominio, MS Exchange e Intranet, y los coordinadores de los aplicativos gestionan el acceso requerido.

A.9.2.3 Gestión de derechos de acceso privilegiado

En el formato "R-RI-80: ROLES Y ACUERDO DE RESPONSABILIDADES USUARIOS TI" se define a que aplicativos y que privilegios tiene el usuario. Una vez sea asignada la cuenta y permisos solicitados, el usuario es responsable por el cumplimiento y buen uso de los mismos. Cada cuenta de usuario es única y de uso personal.

A.9.2.4 Gestión de información de autenticación secreta de usuarios

Para el acceso a la red, equipos y aplicativos cada usuario debe tener una cuenta con una contraseña segura, en el dominio y MS Exchange se solicita cada tres meses el cambio de contraseña.

A.9.2.5 Revisión de los derechos de acceso de usuarios

Los propietarios de los activos (sistemas de información) deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

A.9.2.6 Retiro o ajuste de los derechos de acceso

Para desactivar usuarios del dominio y de los servicios de Internet, Correo, entre otros… el usuario o su jefe inmediato diligencia el formato "R-TH-38: LISTA DE CHEQUEO ENTREGA INFORME PUESTO TRABAJO Y DE LOS BIENES Y VALORES ENCOMENDADOS".

A.9.3 Responsabilidades de los usuarios

Los usuarios deben rendir cuentas por la salvaguarda de su información de autenticación.

A.9.3.1 Uso de información de autenticación secreta

Todos los usuarios que tengan acceso a los servicios de TI deben cumplir las prácticas de la corporación descritas en este documento, está prohibido modificar o inhabilitar los controles de seguridad.

A.9.4 Control de acceso a sistemas y aplicaciones

Se debe evitar el acceso no autorizado a sistemas y aplicaciones.

A.9.4.1 Restricción de acceso a la información

El acceso a la información y a las funciones de los sistemas de las aplicaciones debe ser verificado por los dueños de la información.

A.9.4.2 Procedimiento de ingreso seguro

El acceso a la infraestructura de red, los equipos y aplicativos está asociado al uso de identificación de usuarios y contraseñas asignadas por la oficina de TI o los dueños de los aplicativos.

A.9.4.3 Sistema de gestión de contraseñas

La oficina de TI y los dueños de los aplicativos garantizar que los sistemas de gestión de contraseñas sean interactivos y aseguren la calidad de las contraseñas.

Actividades Diarias

Adicionar nuevos usuarios al dominio, generándole permisos de acuerdo al formato "R-RI-80: ROLES Y ACUERDO DE RESPONSABILIDADES USUARIOS TI". El registro "R-RI-80: ROLES Y ACUERDO DE RESPONSABILIDADES USUARIOS TI" se deberá archivar en las hojas de vida de los funcionarios y/o carpetas de los contratistas según aplique.
Desactivar usuarios del dominio y de los servicios de Internet, Correo, entre otros… de acuerdo al formato "R-TH-38: LISTA DE CHEQUEO ENTREGA INFORME PUESTO TRABAJO Y DE LOS BIENES Y VALORES ENCOMENDADOS".

Actividades Trimestrales

Los usuarios deben cambiar sus contraseñas, el área de TI configurará el envío de alertas a los usuarios**.**
Revisar las cuentas de usuarios actuales y no usadas.

Actividades Semestrales

Realizar cambio de contraseña de servidores.

A.9.4.4 Uso de programas utilitarios privilegiados

El acceso a los aplicativos privilegiados está asociado al uso de identificación de usuarios y contraseñas asignadas por los dueños de los aplicativos.

A.9.4.5 Control de acceso a códigos fuente de programas

La oficina de TI restringe el acceso a los códigos fuente de los programas.

A.10 CRIPTOGRAFÍA

A.10.1 Controles criptográficos

Se debe asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

A.10.1.1 Política sobre el uso de controles criptográficos

La oficina de TI velará por la implementación y proponer una postura institucional que regule el uso de controles criptográficos para la protección de la información, sobre su uso, su protección y el ciclo de vida de las claves criptográficas.

A.10.1.2 Gestión de llaves *Control*

En caso de requerirse encriptación, se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar sus claves privadas, considerándolo crítico o de alto riesgo.

A.11 SEGURIDAD FÍSICA Y DEL ENTORNO

A.11.1 Áreas seguras

Busca prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la Corporación.

A.11.1.1 Perímetro de seguridad física

La Corporación implementó el control de acceso a la corporación mediante la contratación de un vigilante y la instalación de un torniquete, al centro de datos solo tiene acceso el personal de TI o sus autorizados.

A.11.1.2 Controles de acceso físicos

Las áreas seguras se protegen mediante controles de acceso físicos como puertas, las cuales se mantienen cerradas o con personal responsable, y muros para asegurar que solo se permite el acceso a personal autorizado.

A.11.1.3 Seguridad de oficinas, recintos e instalaciones

La seguridad física a oficinas, recintos e instalaciones está enmarcada en el aislamiento de las oficinas mediante puertas y muros y la instalación de cámaras de vigilancia con grabación y monitoreadas por el vigilante, lo visitantes no pueden ingresar a ninguna oficina si no va acompañado de alguno de los ocupantes de la misma.

A.11.1.4 Protección contra amenazas externas y ambientales

La protección física contra desastres naturales, ataques maliciosos o accidentes se fundamentan en prevención del fuego, medios de extinción, centro de datos dentro de otra oficina y con puerta adicional, mantenimientos periódicos de la infraestructura para evitar goteras, ubicación en segundo piso para evitar inundaciones y red eléctrica protegida y con respaldo ante sobre o sub voltajes.

A.11.1.5 Trabajo en áreas seguras

Se tienen los siguientes procedimientos para trabajo en áreas seguras: los lugares de trabajo para funcionarios, contratistas y terceros que no tienen atención al ciudadano se encuentran aisladas por puertas de las zonas de tránsito, se tiene restricción de acceso de los terceros a las oficinas.

A.11.1.6 Áreas de despacho y carga

La Corporación controla los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, estos puntos se encuentran aislados de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

A.11.2 Equipos

Busca prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la Corporación.

A.11.2.1 Ubicación y protección de los equipos

El almacenista lleva control de los equipos de la infraestructura tecnológica de la Corporación identificando responsable del bien y la ubicación del mismo según lo contemplado en el procedimiento “P-RI-01 COMPRAS E INFRAESTRUCURA”.

A.11.2.2 Servicios de suministro

Los equipos se protegen contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro mediante varias UPS en el centro de datos de la oficina central y UPS pequeñas en las territoriales, Laboratorio, Hogar de Paso y otras oficinas descentralizadas.

A.11.2.3 Seguridad del cableado

El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se verifica periódicamente, preferiblemente cada año, contra interceptación, interferencia o daño.

La Corporación cuenta con las siguientes redes:

- Red de VoIP: red de Voz (telefónica) basado en IP y un PBX como punto de entrada.
- Red de datos: Comprendida por una red de cableado estructurado y dos redes WIFI, con salida al exterior vía Internet.
- Red de energía: contamos cableado estructurado centralizado y con respaldo eléctrico central con UPS.
- El Centro de Cómputo de la Red está conformado por un grupo de servidores, NAS y switches que atienden y respaldan los sistemas de información.

Actividades Diarias

Realizar mantenimiento correctivo del cableado de red.

Actividades Semestrales

Realizar pruebas al sistema de energía y sus respaldos.

Actividades Anuales

Realizar mantenimiento preventivo del cableado de red.

Servicio de Impresión.

- El servicio de impresión se brinda a todos los usuarios de La Corporación.
- Los funcionarios de La Corporación solo deben realizar impresiones que tengan que ver con el objeto de La Corporación.

- Se prohíbe la realización e impresión de documentos de carácter obsceno, así como los restringidos por la ley (billetes, certificados y cualquier otro documento de valor).
- El usuario debe verificar cuando envié una orden de impresión –*especialmente cuando utilice papel reciclado*- que el papel usado no tenga ganchos, grapas u otro elemento que pueda generar atascos o daños en los rodillos, unidad fusora o demás componentes de la impresa.

A.11.2.4 Mantenimiento de equipos

Para que los equipos se mantengan correctamente para asegurar su disponibilidad e integridad continuas se realiza el contrato de soporte tecnológico (mesa de ayuda) quien realiza mantenimiento semestral a los equipos de TI y atención a fallas puntuales. A continuación, se relacionan las actividades preventivas a realizar:

Actividades Diarias

- Verificar que todas las aplicaciones necesarias del sistema del servidor de datos (Directorio Activo, DHCP, Microtiks, Sophos, Exchange, entre otras) se están ejecutando o corriendo.
- Revisar estado y brindar el soporte de primer nivel del aplicativo SIIF.
- Revisar estado y brindar soporte de primer nivel del aplicativo SINAP.
- Revisar estado y administrar los servicios de Internet dedicado y Canales Dedicados Locales y Nacionales.
- Administrar Sitio Web Corporativo en los diferentes cambios o agregaciones que se requiera.
- Administrar Sitio Web a nivel intranet en las diferentes actualizaciones que sean necesarias.
- Realizar depuración de las carpetas públicas o unidad mapeada Pública.
- Revisar estado y administrar el servidor Web.
- Diagnóstico de equipos siniestrados.
- Actualizaciones extemporáneas de las aplicaciones, respuesta a incidentes, atención de mantenimientos correctivos y casos que afectan la operación normal de los sistemas de la Corporación.

Actividades Semanales

Revisar entradas de Spam a través de los buzones de correo.

Actividades Mensuales

Verificar estados de los aplicativos actuales de la Corporación.

Actividades Semestrales

- Realizar mantenimiento preventivo a equipos servidores.

- Realizar mantenimiento preventivo a equipos de cómputo (Hardware y software incluyendo impresoras y escáneres en la sede principal y sedes territoriales.

Actividades Anuales

Actualizar los aplicativos a las versiones de software más recientes.

A.11.2.5 Retiro de activos

Los equipos, información o software no se deben retirar de su sitio sin cumplir con lo contemplado en el procedimiento “P-RI-01 COMPRAS E INFRAESTRUCURA”.

A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Los funcionarios que realicen el retiro de los activos de las instalaciones deben aplicar medidas de seguridad a los activos, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

A.11.2.7 Disposición segura o reutilización de equipos

Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso, cumpliendo con lo dispuesto el procedimiento “P-RI-01 COMPRAS E INFRAESTRUCURA”.

A.11.2.8 Equipos de usuario desatendido

Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada y tener activo el protector de pantalla.

A.11.2.9 Política de escritorio limpio y pantalla limpia

Los usuarios de los equipos deben adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información y tener activo el protector de pantalla.

A.12 SEGURIDAD DE LAS OPERACIONES

A.12.1 Procedimientos operacionales y responsabilidades

Busca asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

A.12.1.1 Procedimientos de operación documentados y A.12.1.2 Gestión de cambios

Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios la documentación necesaria, cumpliendo con el procedimiento “P-MJ-01 CONTROL DOCUMENTOS Y REGISTROS”.

Actividades Cuatrimestrales
Reuniones con el equipo de trabajo encargado de la configuración y la administración informática respecto a la seguridad.

Actividades Semestrales

Revisión y actualización del manejo de riesgos.

Actividades Anuales

- Revisar que los procedimientos y estándares para la operación sigan ajustados a las políticas actuales y si es del caso, actualizarlos de ser necesario.
- Realizar seguimiento y actualizar el “R-RI-81: PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN – PETI”.
- Realizar seguimiento y actualizar el “R-RI-82: PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN – PESI Y MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI”.

A.12.1.3 Gestión de capacidad *Control*

En la elaboración y seguimiento del PETI se hace seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.

A.12.1.4 Separación de los ambientes de desarrollo, pruebas, y operación

Los diferentes aplicativos tienen ambientes separados de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

A.12.2 Protección contra códigos maliciosos

Busca asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

A.12.2.1 Controles contra códigos maliciosos

Se implementan controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. Así:

Actividades Diarias

Verificar que todas las aplicaciones necesarias del sistema del servidor de datos (Directorio Activo, DHCP, Microtiks, Sophos, Antivirus, Exchange, entre otras) se están ejecutando o corriendo.

Verificar que los servicios de antivirus estén actualizándose normalmente.

Actividades Semanales

Revisar entradas de Spam a través de los buzones de correo.

Actividades Mensuales

Depurar servidores de Malwares, archivos con extensión .tmp, galletas (cookies), actividad de cada funcionario a partir de alertas del servidor**.**

Actividades Anuales

Actualizar las licencias de Antivirus y AntiSpam y demás aplicativos relacionados con la seguridad de la información.

A.12.3 Copias de respaldo

Busca proteger contra la pérdida de datos.

A.12.3.1 Respaldo de la información

Se hacen copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con la política de copias de respaldo acordadas, así.

Actividades Diarias

- Verificar que las Copia de seguridad de las bases de datos se realicen de acuerdo a la programación de cada aplicativo.
- Verificar que la copia de seguridad de la carpeta “P: Corporación”, donde se encuentran todos los archivos importantes para La Corporación se realicen diariamente.
- Uso obligatorio del GOOGLE DRIVE en territoriales y hogar de paso que todos los usuarios utilicen este aplicativo para realizar copia de seguridad de los archivos importantes, también para auto gestionar el manejo de su cuota de almacenamiento.
- En la sede centro y laboratorio la información importante debe ser salvaguardada en el disco corporativo “P”, y los usuarios deben auto gestionar las copias de seguridad de sus archivos en el GOOGLE DRIVE.

Actividades Semanales

Con el apoyo del Área de TI, se realizarán copias de seguridad en discos duros externos y/u otros mecanismos disponibles (NEXTCLOUD, etc…) a la información relacionada al accionar institucional o de sus unidades de apoyo (análisis de aguas, trámites ambientales, proyectos Corporativos, gestión Corporativa, entre otros) de los equipos del Laboratorio de Análisis de Aguas y/o Sedes Territoriales Caribe, Atrato,

Nutibara y Urrao. La realización de las copias de seguridad estará a cargo de los Coordinadores del Laboratorio y/o Territoriales o a quienes estos deleguen.

Actividades Semestrales

- Recuperar copia de seguridad al azar para validar si están buenas.
- Hacer imágenes de los servidores Exchange y Directorio Activo incluido los archivos de sistemas en la NAS, reemplazando las imágenes anteriores.
- Simular un evento y poner a prueba el plan de contingencia.
- Alertar a los usuarios para borrar archivos innecesarios, cuidado de la NAS al 70%.

Actividades Anuales

Verificar que el sistema de backup sea soportable para la seguridad informática.

A.12.4 Registro y seguimiento

Busca registrar eventos y generar evidencia.

A.12.4.1 Registro de eventos

Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. Para ello cada sistema debe proveerse con registros de eventos “Logs”.

A.12.4.2 Protección de la información de registro

Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

A.12.4.3 Registros del administrador y del operador

El contratista de soporte tecnológico debe registrar, y los registros se deben proteger y revisar con regularidad.

A.12.4.4 Sincronización de relojes

Los relojes de todos los sistemas de procesamiento de información en la Corporación se deben sincronizar con una única fuente de referencia de tiempo.

A.12.5 Control de software operacional

Busca asegurarse de la integridad de los sistemas operacionales.

A.12.5.1 Instalación de software en sistemas operativos A.12.6.2 Restricciones sobre la instalación de software

Todos los equipos de la Corporación tienen protección para evitar la instalación de software en sistemas operativos.

A.12.6 Gestión de la vulnerabilidad técnica

Busca prevenir el aprovechamiento de las vulnerabilidades técnicas.

A.12.6.1 Gestión de las vulnerabilidades técnicas

El contratista del soporte tecnológico y los contratistas de los diferentes sistemas de información deben informar acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la Corporación a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

A.12.7 Consideraciones sobre auditorías de sistemas de información

Busca minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

A.12.7 Controles de auditorías de sistemas de información

Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

A.13 SEGURIDAD DE LAS COMUNICACIONES

A.13.1 Gestión de la seguridad de las redes

Busca asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

A.13.1.1 Controles de redes

Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

A.13.1.2 Seguridad de los servicios de red

La oficina de TI debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

A.13.1.3 Separación en las redes

Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. El acceso a la infraestructura de red física está restringido a los usuarios activos en el directorio activo, lo mismo que la conexión por la red WIFI “Admin”. Los usuarios externos sólo se comunican por la red “Visitantes”.

Los usuarios autorizados para conectarse a la red principal deben realizarlo por VPN y estar previamente autorizados. La información de la VPN es personal e intransferible.

A.13.2 Transferencia de información

Busca mantener la seguridad de la información transferida dentro de una Corporación y con cualquier entidad externa.

A.13.2.1 Políticas y procedimientos de transferencia de información

Las siguiente políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones deben ser aplicadas por los usuarios.

- Todo funcionario, contratista o tercero de la Corporación es responsable por proteger la confidencialidad e integridad de la información y para la divulgación e intercambio de la misma se debe contar con la respectiva autorización del jefe inmediato.
- La transmisión, transferencia o comunicación de información de la Corporación se debe realizar por las redes de comunicaciones o dispositivos autorizados por la oficina de TI.
- Las actividades de teletrabajo o trabajo en casa deben cumplir con esta política.

A.13.2.2 Acuerdos sobre transferencia de información

Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.

A.13.2.3 Mensajería electrónica

Se protege adecuadamente la información incluida en la mensajería electrónica mediante la aplicación de los siguientes protocolos en la plataforma Exchange: SSL, SPF, SKIM, DMARC. Todos los usuarios tienen prohibido el uso de servicios interactivos como Facebook, KAZAA, Yahoo, MSN, etc… o para intercambio de información para fines diferentes a las actividades con el proveedor o tercero.

A.13.2.4 Acuerdos de confidencialidad o de no divulgación

Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la Corporación para la protección de la información, en especial las contempladas en los numerales 4 y 5 del artículo 34 del capítulo segundo. “Deberes” del código único disciplinario Ley 734 de 2002.

A.14 Adquisición, desarrollo y mantenimiento de sistemas

A.14.1 Requisitos de seguridad de los sistemas de información

Busca asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

A.14.1.1 Análisis y especificación de requisitos de seguridad de la información

Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

La oficina de TI debe garantizar que los servicios de las aplicaciones que pasan sobre redes públicas se protejan de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

A.14.1.3 Protección de transacciones de los servicios de las aplicaciones

La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

Los servicios de transacciones bancarias del objeto de la Corporación desarrolladas por medios digitales deben tener seguridad de doble vía con claves y tokens y se debe expedir un soporte en papel o digital de cada transacción.

Se debe garantizar que no hay suplantación de links en el sitio web, ni suplantado los certificados digitales, ni modificada indebidamente la resolución de sus DNS, con el fin de proteger la información pública.

A.14.2 Seguridad en los procesos de desarrollo y de soporte

Busca asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

A.14.2.1 Política de desarrollo seguro

Todo tercero debe seguir estándares, buenas prácticas o modelos de madurez de desarrollo seguro, basándose en (o publicadas por) OWASP, NIST, SANS, SAMM, BSIMM o MICROSOFT. Tales como: Validación de datos de entrada, Administración de autenticación y contraseñas, Administración de sesiones, Control de Acceso, Prácticas Criptográficas, Manejo de errores y Logs, y Protección de datos.

A.14.2.2 Procedimientos de control de cambios en sistemas

Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.

La Oficina de TI es responsable de gestionar los procesos de cambio que impliquen:

- Hardware
- Software y equipos de comunicaciones
- Sistemas de software
- Aplicaciones de software “en producción”
- Toda la documentación y procedimientos asociados con la ejecución, soporte y mantenimiento de los sistemas en producción.

Atendiendo a esto, los cambios en componentes que estén bajo el control de un proyecto de desarrollo de aplicaciones (y/o su despliegue en la Infraestructura) no se realizarán bajo el proceso de Gestión de Cambios, sino que estarían sujetos a los procedimientos de gestión de cambios del proyecto.

A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la Corporación. Estos cambios deben aprobarse por la oficina de TI y/o el dueño del sistema de información.

A.14.2.4 Restricciones en los cambios a los paquetes de software

Las modificaciones a los paquetes de software se deben limitar a los cambios necesarios y todos los cambios se deben controlar estrictamente y estar aprobados previamente por la oficina de TI.

A.14.2.5 Principios de construcción de los sistemas seguros

Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. Estos principios deben ser, pero no se limitan a, Control de Acceso a la información, definición y autenticación de usuarios, mecanismos de detección de intrusos, definición de mecanismos de cifrado de datos, administración de la información y confidencialidad e integridad y administración de la seguridad física de la información.

A.14.2.6 Ambiente de desarrollo seguro

La oficina de TI debe establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas en especial los contratados para desarrollar externamente.

A.14.2.7 Desarrollo contratado externamente

La oficina de TI debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

A.14.2.8 Pruebas de seguridad de sistemas

A.14.2.9 Prueba de aceptación de sistemas

Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad y para la aceptación de los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.

Algunas de estas pruebas pueden ser:

- Recopilación de Información
- Pruebas de gestión de la configuración
- Pruebas de la lógica de negocio
- Pruebas de Autenticación
- Pruebas de Autorización
- Pruebas de gestión de sesiones
- Pruebas de validación de datos
- Pruebas de denegación de Servicio
- Pruebas de Servicios Web
- Pruebas de AJAX

A.14.3 Datos de prueba

Busca asegurar la protección de los datos usados para pruebas.

A.14.3.1 Protección de datos de prueba

La oficina de TI debe seleccionar, proteger y controlar cuidadosamente los datos de prueba se.

A.15 RELACIONES CON LOS PROVEEDORES

A.15.1 Seguridad de la información en las relaciones con los proveedores

Busca asegurar la protección de los activos de la Corporación que sean accesibles a los proveedores.

A.15.1.1 Política de seguridad de la información para las relaciones con proveedores

La oficina de contratación y la oficina de TI acordar con los proveedores los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la corporación y se deben documentar.

A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

La oficina de TI debe establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la corporación.

A.15.1.3 Cadena de suministro de tecnología de información y comunicación

Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

A.15.2 Gestión de la prestación de servicios de proveedores

Busca mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

A.15.2.1 Seguimiento y revisión de los servicios de los proveedores
A.15.2.2 Gestión de cambios en los servicios de los proveedores

La oficina de TI debe coordinar y/o supervisar todos los contratos de TI con el fin de hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

A.16 Gestión de incidentes de seguridad de la información

A.16.1 Gestión de incidentes y mejoras en la seguridad de la información

Busca asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

A.16.1.1 Responsabilidades y procedimientos
A.16.1.2 Reporte de eventos de seguridad de la información
A.16.1.3 Reporte de debilidades de seguridad de la información

Todo funcionario, tercero o usuario de los servicios de TI de la Corporación debe reportar oportunamente a la oficina de TI cualquier situación que pueda considerar como un evento que pueda afectar la seguridad de la información.

El oficial de seguridad es responsable de evaluar todos los reportes y determinar si es un evento o un incidente de seguridad. Si el incidente implica robo o mal manejo de la información pública debe ser reportado a la superintendencia de industria y comercio.

A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

El oficial de seguridad de la información debe evaluar y debe decidir si se van a clasificar como incidentes de seguridad de la información.

A.16.1.5 Respuesta a incidentes de seguridad de la información

El oficial de seguridad de la información debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados y realizar el aislamiento y coordinar la recuperación de los accesos a sistemas de comunicación y cómputo afectados.

A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

Durante el cierre del evento de seguridad debe documentarse el conocimiento adquirido al analizar y resolverlo, esta información se debe usar actualizar la matriz de riesgos e implementar las acciones para reducir la posibilidad o el impacto de incidentes futuros.

A.16.1.7 Recolección de evidencia

Todos los intervinientes en el evento deben apoyar la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

A.17.1 Continuidad de seguridad de la información

Busca la continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la Corporación.

A.17.1.1 Planificación de la continuidad de la seguridad de la información

En el Plan Estratégico de Seguridad de La Información – PESI – y el Plan Estratégico de Tecnologías de La Información – PETI – la corporación determino sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

A.17.1.2 Implementación de la continuidad de la seguridad de la información

La oficina de TI realiza el seguimiento al cumplimiento anual del PESI y PETI con el fin de establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

La oficina de TI debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

A.17.2 Redundancias

Busca asegurar la disponibilidad de instalaciones de procesamiento de información.

A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.

Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. Algunas de las redundancias implementadas:

- UPS
- Respaldos de información
- Servicio de internet.
- Arreglos de discos en array 5
- Fuentes redundantes para servidores

A.18 CUMPLIMIENTO

A.18.1 Cumplimiento de requisitos legales y contractuales

Busca evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

La Corporación cumple con toda la legislación colombiana aplicable, las regulaciones de los entes de control, gubernamentales o nacionales que apliquen y las obligaciones contractuales adquiridas con terceros.

A.18.1.2 Derechos de propiedad intelectual

Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

El almacén y la oficina de TI son responsables de administrar el inventario y control de las licencias de software, hardware y aplicaciones utilizadas por la Corporación, así como los medios y contratos que se relacionan con la actividad comercial de compra de software y hardware.

Está prohibido el uso de software ilegal en los equipos de la Corporación.

El uso de información pública de la Corporación o de terceros está permitida siempre y cuando éstos cumplan con las reglamentaciones nacionales vigentes para la preservación de derechos morales e intelectuales de los obras o referencias citadas.

A.18.1.3 Protección de registros

Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

A.18.1.4 Privacidad y protección de información de datos personales

Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, y lo contemplado en POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES de la corporación, la cual se encuentra en la siguiente dirección http://corpouraba.gov.co/politica-de-tratamiento-y-proteccion-de-datos-personales/ cuando sea aplicable. Los datos personales que recolecta la Corporación se utilizarán única y exclusivamente para el desarrollo de sus actividades misionales y en cumplimiento de sus obligaciones legales y contractuales.

A.18.1.5 Reglamentación de controles criptográficos

Se deben usar controles criptográficos, en la información de la entidad clasificada como restringida o reservada.

A.18.2 Revisiones de seguridad de la información

Busca asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

A.18.2.1 Revisión independiente de la seguridad de la información

La oficina de Control Interno verificará la implementación y el cumplimiento de los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información a intervalos planificados o cuando ocurran cambios significativos.

A.18.2.2 Cumplimiento con las políticas y normas de seguridad

La dirección general y los dueños de los sistemas de información deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

A.18.2.3 Revisión del cumplimiento técnico

La oficina de TI debe revisar periódicamente los sistemas de información para determinar el cumplimiento con las políticas y normas de seguridad de la información.

10. CONTROL DE CAMBIOS

Fecha	Resolución	Versión	Detalle
01/02/2008	03-01-02-000177	01	Aprobación inicial con código y nombre “D-RI-02: PRACTICAS DE ADMINISTRACIÓN Y SEGURIDAD INFORMÁTICA – PROTOCOLO PARA SEGURIDAD”.
16/12/2009	300-03-10-23-1624	02	Se realizan las siguientes modificaciones: • Se incluyeron los ítems: “Infraestructura Tecnológica” que contempla el “Organigrama del Área de Sistemas” y la “Red de Voz y Datos”; “Manejo de Licenciamiento del Software Corporativo”; “Uso del Centro de Computo y de los Equipos de

			Cómputo" que contempla "Reglas Generales", "Administración del Centro de Computo", "Uso Adecuado de los Equipos de Cómputo". • Las "Actividades Diarias", "Actividades Semanales", "Actividades Mensuales", "Actividades Bimensuales", "Actividades Cuatrimestrales", "Actividades Semestrales", "Actividades Anuales", "En Cualquier Momento del Año" y "Otras Actividades", se ubicaron en el ítem "Actividades de Administración y Seguridad Informática".
03/06/2010	300-03-10-23-0718	03	En el marco de la implementación de la "Estrategia de Gobierno en Línea" se incluye el ítem: "Administración del Sitio Web Corporativo" que contempla la "Política Editorial y de Actualización", la "Política de Privacidad, Seguridad y Condiciones de Uso".
02/07/2010	300-03-10-23-0817	04	Teniendo en cuenta la aplicabilidad y la operativización de las políticas de Gobierno en Línea, se determinó extraer el ítem: "Administración del Sitio Web Corporativo" del presente documento y crear un documento aparte con código y nombre: "D-MJ-03: POLÍTICAS RELACIONADAS A GOBIERNO EN LÍNEA". Se modifica el logo de La Corporación y se incluye el ítem control de cambios.
25/09/2013	300-03-10-23-1578	05	Se realizan ajustes en las actividades semanales, mensuales, anuales y en cualquier momento del año.
27/06/2014	300-03-10-23-0897	06	Incluida la nota como se llevara a cabo las copias de seguridad semanales de los equipos del Laboratorio de Análisis de Aguas, Sedes Regionales Caribe, Atrato, Nutibara y Urrao.
15/10/2015	300-03-10-23-1350	07	Se cambió el nombre de regionales por Territoriales, de acuerdo al ajuste de la estructura organizacional de CORPOURABA
16-10-2016	300-03-10-23-1014	08	Se cambia el logo de la Corporación
31/08/2017	300-03-10-23-1094	09	Actualización por cambios en la versión de ISO 9000: 2015, se actualiza la política de del Sistema de Gestión de Seguridad de la Información.
27/09/2018	250-03-10-23-1618	10	Se hace referencia a los planes estratégicos de Tecnologías de la información – PETI-, de seguridad de la información –PESI- y del Modelo de seguridad y privacidad de la información MSPI.
01/08/2019	300-03-10-23-0937	11	Se incluye código del SGC al PETI, PESI y MSPI, se realizan ajustes a las actividades periódicas, se actualizan los organigramas y se definen algunos roles faltantes y se ajustan los roles de los usuarios.
24/06/2020	300-03-10-23-0710	12	Se ajusta la normatividad aplicable. Se ajusta el documento para que se acople con lo requerido en la norma ISO 27001:2013, en especial lo concerniente a: • Nomenclatura conforme a los requisitos de la Norma. • Actividades relacionadas en el Anexo A. • Cambios en la documentación del SGC. Se incluyen varios aspectos relacionados con el manejo técnico en sistemas y la seguridad de la información, tales como: • Actividades y servicio del correo electrónico • Activos de Información y Activos de Control. • Control de acceso • Criptografía • Seguridad de las comunicaciones • Adquisición, desarrollo y mantenimiento de sistemas • Relaciones con los Proveedores • Gestión de Incidentes • Continuidad del negocio • Cumplimiento de requisitos legales
30/09/2021	300-03-10-23-1688	13	Se incluyen aspectos relacionados con el manejo de impresiones. Se revisa e incluye normatividad actualizada. Se ajustan detalles de redacción. Se incluyen actividades del oficial de seguridad. Inclusión de la política de tratamiento de datos personales.

16/05/2025	100-03-10-23-0824	14	Se ajustan las políticas de SGSI. Se mejora la redacción en torno a: • Concisión: Se ha reducido la extensión de las descripciones, eliminando redundancias y frases innecesarias. • Claridad: Se ha utilizado un lenguaje más directo y preciso. • Terminología Profesional: Se ha utilizado una terminología más profesional y coherente. • Enfoque: Se ha puesto el foco en la información esencial, facilitando la comprensión de los requisitos y procesos. Ajuste de servicios de correo electrónico, DRIVE y otros en la plataforma Google Workspace

Última línea-------última línea------última línea