POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, Y CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS TIC

REGIÓN ADMINISTRATIVA Y DE PLANEACIÓN ESPECIAL
RAP-E REGION CENTRAL

DIRECCIÓN ADMINISTRATIVA Y FINANCIERA
Proceso Gestión TIC
2024

REGIÓN CENTRAL
RAP-E | Estamos Construyendo Región

Contenido

I. Introducción 4

II. Objetivo 5

III. Alcance 5

IV. Marco Conceptual y Conjunto de Estándares 6

i. Definiciones 6

ii. Normatividad 7

V. Declaración de la Política 7

i. Política de Seguridad de la Información 7

ii. Organización de la seguridad de la información 8

CLASIFICACIÓN DE LA INFORMACIÓN 8

CONTROL DE ACCESO 9

SEGURIDAD DEL CABLEADO 11

MANTENIMIENTO A LOS EQUIPOS 11

POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA 11

PROTECCIÓN CONTRA CÓDIGO MALICIOSO 12

REGISTRO Y SEGUIMIENTO 12

SINCRONIZACIÓN DE RELOJES 13

SEGURIDAD DE LAS COMUNICACIONES 13

SEGURIDAD DE LOS RECURSOS HUMANOS 15

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 16

iii. POLÍTICA DE CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS TIC 18

COPIAS DE RESPALDO (BACKUP) 18

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 19

iv. POLÍTICA DE DISPOSITIVOS MÓVILES Y TELETRABAJO 20

SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES 21

v. RESPONSABILIDAD DE LOS USUARIOS 22

USO DE INFORMACIÓN CONFIDENCIAL 22

ROLES Y RESPONSABILIDADES 22

VI. Roles de Responsabilidad 24

Línea Estratégica 24
Primera Línea 24
Segunda Línea 24
Tercera Línea 24
VII. Reportes al Comité Institucional de Gestión y Desempeño: 24
VIII. Vigencia de la Política 25
IX. Armonización 25
Modelo Integrado de Planeación y Gestión (MIPG) 25
Otras Políticas de la RAP-E Región Central 25
X. Control de cambios 25

I. Introducción

La implementación de la política de seguridad y privacidad de la información tiene como objetivo desarrollar capacidades mediante la implementación de lineamientos de seguridad y privacidad de la información en todos los procesos, procedimientos, servicios y en general todos los activos de información de la Región Administrativa de Planificación Especial RAP-E para proteger la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Teniendo en cuenta como insumos principales la información que la entidad genera, almacena y administra, por tanto, es primordial establecer políticas claras y contundentes para la recolección, almacenamiento, administración y entrega de la información, la cual sirve de insumo para la toma de decisiones de la Entidad.

De igual modo, la tecnología es el recurso clave para el buen manejo de dicha información, la cual se desarrolla, crece y evoluciona de manera rápida y constante, requiriendo establecer lineamientos de seguridad que minimicen los riesgos de: alteración, fuga o indisponibilidad de la información durante las etapas de fabricación, diseño e implementación de las herramientas, incluso durante el uso de estas.

Por esta razón la política de seguridad y privacidad de la información define los lineamientos, controles, roles perfiles y responsabilidades para la gestión de la información, y gestiona al máximo las amenazas a los sistemas de información, con ello se busca limitar la superficie tecnológicamente vulnerable que permita a los atacantes perpetrar ataques para violentar y dar un mal uso a la información.

Por lo anterior, la entidad consolida en el presente documento las políticas en seguridad de la información para garantizar la confidencialidad, integridad, disponibilidad, no repudio y cumplimiento de las obligaciones en materia de tratamiento de datos personales, el buen uso y cuidado de la información y el funcionamiento adecuado de los recursos tecnológicos puestos a disposición de los usuarios.

II. Objetivo

- Evaluar y gestionar actividades con el objetivo de garantizar la Seguridad de la Información para ello se definen las etapas y actividades correspondientes para establecer la estrategia.
- Controlar y optimizar la gestión de la seguridad de la información al interior de la RAP-E Región Central.
- Gestionar la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad y privacidad de la información dispuesto en la política de Gobierno Digital y demás normas asociadas al proceso.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Identificar los Riesgos de Seguridad de la Información que pueden afectar la integridad, confidencialidad y disponibilidad de la Información, gestionando sus debidos planes de tratamiento para la mitigación de estos.

III. Alcance

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC aplica a toda la entidad, sus funcionarios, contratistas que tengan relación directa con la entidad, que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura tecnológica, canales de comunicación de la entidad, bases de datos y en general los archivos informáticos que conforman el Sitio Web, Subsistemas de Información y documentos físicos de la RAP-E.

Todas las políticas contenidas en este documento, las cuales están basadas en los lineamientos de la norma ISO 27001:2022 y los lineamientos del Modelo de Seguridad y Privacidad de Información (MSPI) establecida por MINTIC a través del Decreto 1078 de 2015, y sus correspondientes guías de apoyo, serán aplicadas a los procesos estratégicos, misionales y de apoyo de toda la RAP-E.

IV. Marco Conceptual y Conjunto de Estándares

i. Definiciones

- Activo de Información: Es todo aquello que en el Ministerio de Educación Nacional es considerado importante o de alto valor para la entidad, porque contiene información importante, como son los datos creados o utilizados por procesos de la organización, en medio digital, en papel o en otros medios. Ejemplos: bases de datos con usuarios, contraseñas, números de cuentas, informes etc.

- Confidencialidad: Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

- Continuidad de negocio: Conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de la misionalidad de la entidad y la prestación de sus servicios.

- Dato: Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- Disponibilidad: Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- Información: Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

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

- Seguridad digital: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante, incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

ii. Normatividad

- Ley 1581 de 2012, la cual se dictan disposiciones generales para la Protección de Datos Personales.
- Ley 1712 de 2014, Por la cual se crea la ley de transparencia y el derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- Decreto 1727 de 2009, Por el cual se determina la forma en la cual los operadores de los Bancos de Datos de Información Financiera, Crediticia, Comercial, de Servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.
- Decreto 2952 de 2010, Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008.
- Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014, Por el cual se reglamenta el artículo de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

V. Declaración de la Política

i. Política de Seguridad de la Información

La Política General de Seguridad de la Información enuncia el compromiso de la Gerencia, con el fin de liderar la estrategia corporativa a partir de lineamientos para la protección de la información, involucrando tanto la información digital como física, a fin de ser conocidos, divulgados y cumplidos de forma obligatoria por todos los funcionarios públicos, contratistas y terceros (partes interesadas) de la RAP-E, en la procura de prevenir, detectar y neutralizar de forma oportuna una posible fuga, pérdida o alteración no autorizada de información.

La política general de seguridad de la información tiene como objetivo la consolidación de una cultura de Seguridad de la Información al interior de la entidad, que permita a su vez el cuidado de la información como su activo más valioso.

Con dicha política, se pretende fortalecer las capacidades de las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en el entorno digital, en un marco de colaboración y asistencia, esto se logrará a través de las siguientes actividades:

- La definición, socialización, aplicación y seguimiento de las políticas de seguridad y privacidad de la información.
- la definición de roles y responsabilidades en seguridad digital.
- La segmentación de deberes.

- El contacto con las autoridades y grupos de interés.
- La incorporación de la seguridad digital en la gestión de los proyectos.
- La identificación y clasificación de los activos de información.
- Identificación, valoración y definición del plan de tratamiento de riesgos de seguridad digital.
- La definición de controles para la mitigación de los riesgos, reduciéndolos a un nivel aceptable.

Así las cosas, la información es reconocida por la RAP-E como uno de los activos más importantes para lograr su objetivo fundamental de concertar y gestionar proyectos de alcance supra-departamental, a partir de los intereses comunes y de acuerdos entre los socios a nivel Regional y fortalecer la seguridad de la información a través del establecimiento, implementación y mejora continua de controles; cuyo fin es el aseguramiento de la integridad, disponibilidad y confidencialidad de la información mediante la gestión y tratamiento adecuado de los riesgos, en el marco de los requisitos de la entidad, los legales o reglamentarios, y las obligaciones de seguridad contractuales; con servidores públicos, proveedores y partes interesadas, comprometidos a participar activamente en el desarrollo de la cultura de seguridad de la información.

ii. Organización de la seguridad de la información

La RAP-E garantiza el soporte operativo para las actividades de la Información, para ello debe mantener un esquema de seguridad de la información en donde existan roles y responsabilidades que consideren actividades de administración, operación y gestión de la información.

CLASIFICACIÓN DE LA INFORMACIÓN

La RAP-E debe asegurar que la información es tratada y protegida adecuadamente de acuerdo con el nivel de clasificación otorgado. La información física es clasificada de acuerdo con las tablas de retención documental de la entidad.

Esquema de Clasificación

Toda información perteneciente a RAP-E deberá ser identificada y clasificada de acuerdo con los siguientes niveles los cuales son establecidos por la ley 1712 de 2014 de Transparencia y Acceso a la Información Pública:

1. Información pública.
2. Información pública clasificada.
3. Información pública reservada.

La dirección administrativa y financiera, en conjunto con la Oficina Asesora de Planeación, son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento o manejo que deben darse de acuerdo con el nivel de clasificación al que pertenecen.

Etiquetado y Manejo de la Información

La RAP-E, desarrollará e implementará un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado.

Transferencia de Medios de soporte físicos

La información clasificada como CLASIFICADA o RESERVADA que se desee almacenar en medios removibles y estos sean transportados fuera de las instalaciones de RAP-E, debe cumplir con las disposiciones de seguridad indicadas por la dirección administrativa y financiera, a cargo del proceso gestión TIC, específicamente aquellas referentes al empleo de técnicas de cifrado.

CONTROL DE ACCESO

- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información debe ser asignado de acuerdo con la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la entidad, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

- Todas las áreas junto con la dirección administrativa y financiera, a cargo del proceso gestión TIC asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo con procesos formales de autorización los cuales deben ser revisados periódicamente por el profesional especializado a cargo del proceso TIC.

- La dirección administrativa y financiera, a cargo del proceso gestión TIC garantizará el establecimiento de privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la RAP-E. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y garantizará que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

Acceso a redes y servicios en red

- La RAP-E suministra a los usuarios las claves respectivas para el acceso a los servicios de red y de sistemas de información a los que haya sido autorizado, es importante recordar que son de uso personal e intransferible.

- El servicio de correo electrónico debe ser utilizado exclusivamente para actividades laborales, la navegación en la intranet e internet será monitoreada por la dirección administrativa y financiera, a cargo del proceso gestión TIC, y el tiempo está definido de acuerdo con los privilegios asignados por la misma.

- Para tener acceso a cualquier red inalámbrica de la entidad los funcionarios, contratistas o terceros deben:

    1. Conectarse a través de protocolos seguros.
    2. Acceder mediante las direcciones IP asignadas.
    3. Todos los usuarios tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

- Para mantener la seguridad en los servicios de red solo se deben mantener instalados y habilitados los programas, y aplicativos avalados por la dirección administrativa y financiera.

Gestión De Acceso A Usuarios

- La RAP-E controla el acceso a los sistemas y servicios de información estableciendo un procedimiento de novedades de los usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información.

- Se mantendrá evidencia de cambios realizados a los identificadores de usuario (ID), perfiles y estado de las cuentas de usuario.

- Se debe retirar o bloquear inmediatamente los derechos de acceso a los funcionarios y/o contratistas a los cuales se revoca la autorización de acceso, vinculación contractual o sufren pérdida o robo de credenciales de acceso.

- Se deben efectuar revisiones periódicas a los Identificadores de Usuarios (ID) identificando y cancelando cuentas redundantes o inactivas y comprobando la integridad de accesos modificados por las novedades de usuario reportadas.

- Las actividades de revisión periódica del estado, cambios de roles y bloqueo de usuarios serán responsabilidad de la dirección administrativa y financiera, a cargo del proceso gestión TIC.

Suministro de Acceso a Usuarios

- Cada uno de los directores y jefes de Oficina de la entidad debe aprobar el acceso a los sistemas de información que le competen, de acuerdo con los roles y perfiles establecida para los usuarios y de acuerdo con sus funciones.

- El administrador de cada sistema de información monitoreará periódicamente los roles y perfiles definidos y los privilegios asignados a los usuarios y si necesitan realizar alguna modificación deben solicitarlo a la dirección administrativa y financiera, a cargo del proceso gestión TIC.

- De igual manera, se revisará periódicamente el acceso a los usuarios de información que fueron asignados con el fin de realizar procesos de autocontrol.

Cancelación o ajuste a los derechos de usuario

- Cada uno de los directores y jefes de Oficina de la entidad y los supervisores de los contratistas son los responsables de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Correo electrónico corporativo a la dirección administrativa y financiera, a cargo del proceso gestión TIC. Cuando se solicite una cuenta institucional se debe justificar e informar de la persona responsable de dicho buzón. Si se detecta que se solicita una cuenta institucional y que no se hace uso de ella, la dirección administrativa y financiera, a cargo del proceso gestión TIC podrá eliminar dicha cuenta.

- Los funcionarios, en el desarrollo de sus tareas habituales u ocasionales que utilicen cualquier servicio de tecnología de la información y comunicaciones (TIC) que provea la RAP-E, son responsables del cumplimiento y seguimiento de esta política.

SEGURIDAD DEL CABLEADO

Se protege el cableado tanto de energía como de comunicaciones en los servicios de procesamiento de información tanto de daños como de interceptaciones, por consiguiente, en la RAP-E, se tienen separadas las rutas de cableado de energía y comunicaciones con el fin de evitar interferencias.

El cableado estructurado está debidamente marcado y se cuenta con un plano para hacer correcciones o inserciones de manera efectiva.

MANTENIMIENTO A LOS EQUIPOS

Se realizan las siguientes acciones de acuerdo con el procedimiento establecido por la entidad:

1. Efectuar mantenimiento preventivo y correctivo a intervalos de tiempo definido a los equipos y solo por personal autorizado. Esta labor se debe hacer tanto a aquellos equipos que procesen información como aquellos que soporten estos activos.
2. Se deben conservar los registros de los mantenimientos realizados.
3. Se debe tener un cronograma de mantenimientos.

POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

- El personal de RAP-E debe conservar su escritorio libre de información propia de la entidad, que pueda ser obtenida, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- Para el personal que esté ubicado en zonas de atención al público, al ausentarse de su puesto deberá guardar también los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada.

- El personal de RAP-E debe bloquear la pantalla de su computador con el protector de pantalla designado por la entidad, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo. Al finalizar sus actividades diarias, deberán salir de todas las aplicaciones y apagar la estación de trabajo.

- En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar la información CLASIFICADA o RESERVADA protegida bajo llave. Esto incluye: documentos impresos, CD´s, dispositivos de almacenamiento USB y medios removibles en general.

- Los equipos de reproducción de información (impresoras, fotocopiadoras, escáneres, etc.), están ubicados en lugares de acceso controlado y cualquier documentación con información pública clasificada o pública reservada se debe retirar inmediatamente del equipo y ser puesta en un lugar seguro.

PROTECCIÓN CONTRA CÓDIGO MALICIOSO

- La RAP-E establece medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos.

- La infraestructura de procesamiento de información cuenta con un sistema de detección/prevención de intrusos, sistema anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos. Así mismo, se restringirá la ejecución de aplicaciones y se mantendrá instalado y actualizado un sistema de antivirus, en todas las estaciones de trabajo y servidores de RAP-E.

REGISTRO Y SEGUIMIENTO

Todos los eventos que se presenten en los sistemas de información de la RAP-E cuentan con registros de auditoría que contienen excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría incluyen:

1. Identificador del usuario.
2. Fecha y hora DE INICIO Y TERMINACIÓN.
3. Registros de intentos exitosos y fallidos de acceso al sistema.
4. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.
5. Dirección IP desde donde se origina la conexión.

SINCRONIZACIÓN DE RELOJES

- Los relojes de todos los sistemas de procesamiento de información de la entidad deberán ser sincronizados con una única fuente de referencia de tiempo.

- Para garantizar la integridad de la información debe existir un registro de cualquier modificación realizada al sistema de procesamiento de la información, por tal razón se debe tener en cuenta lo siguiente:

    - Documentar de manera clara y explícita cuando hayan ocurrido fallas, la forma como fueron corregidas y el porcentaje de avance de la acción de mejora.

GESTIÓN DE VULNERABILIDADES TÉCNICAS

Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información con la finalidad de garantizar la confidencialidad, integridad y disponibilidad, para ello se evalúa la exposición de la entidad a estas vulnerabilidades y se tomen las medidas apropiadas para tratar el riesgo asociado.

Restricciones sobre la Instalación de Software

- Los funcionarios de la entidad no podrán instalar ningún software, programa o aplicativo en los equipos designados para su labor en la entidad o bajo la modalidad de teletrabajo.

SEGURIDAD DE LAS COMUNICACIONES

- El acceso a las redes de la entidad debe estar limitado a los funcionarios de la entidad y demás personas autorizadas por la misma por medio de claves de acceso a los sistemas de información.

- Se establecerá un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de garantizar el buen uso de estos y mantener los niveles de seguridad establecidos.

- La entidad proporciona a los funcionarios todos los recursos tecnológicos de conectividad necesarios, para que puedan desempeñar las funciones/actividades para las cuales fueron contratados, por tal motivo no se permite conectar a las estaciones de trabajo o a los puntos de acceso corporativos, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la dirección administrativa y financiera, a cargo del proceso gestión TIC.

Separación de las Redes

- Se debe establecer un esquema de segregación de redes con el fin de controlar el acceso a los diferentes segmentos de red. El tráfico entre estos segmentos de red estará controlado mediante un elemento de red que permita una autorización a un nivel de detalle específico (Dirección IP, puerto).

- Se prohíbe el envío de información confidencial o sensible de la entidad a personal externo de la entidad sin autorización previa.

- Está prohibido el uso del correo electrónico personal (Hotmail, Gmail personal, entre otros) para el envío o recepción de cualquier tipo de información relacionada con la entidad.

- No está permitido el intercambio de información pública clasificada y reservada de la entidad, por medio telefónico o por correo electrónico, sin las debidas protecciones y controles necesarios que la ameritan por su nivel de clasificación. Para tal fin, se pueden apoyar en soluciones tecnológicas de cifrado para la información en medio digital.

- La información física, no se debe dejar abandonada en impresoras, en el puesto de trabajo o un área de circulación alta de personas.

Mensajes Electrónicos

Con el fin de garantizar la confidencialidad de la información, se deben establecer parámetros para el envío de la información a terceros por medio del correo electrónico de la entidad para proteger adecuadamente la información incluida en la mensajería electrónica, para tal fin:

- Los funcionarios de la entidad serán responsables de todas las actividades realizadas con su cuenta de correo institucional.

- En el caso de recibir un correo electrónico de un destinatario desconocido, esté no debe ser abierto y el empleado debe notificar de forma inmediata, para evitar que en caso de que este contenga algún virus, infecte el sistema.

- El servicio de correo electrónico debe ser usado únicamente para el ejercicio de las funciones de competencia de cada usuario.

SEGURIDAD DE LOS RECURSOS HUMANOS

La RAP-E protege la información por medio de la validación y concientización del recurso humano que hará uso de esta.

Selección de personal

- Dentro de los procesos de contratación de personal para la prestación de servicios se realiza la verificación de antecedentes cuando así lo amerite del personal que va a ingresar a laborar en la entidad.

- La dirección administrativa y financiera, es el área encargada de realizar la verificación de los antecedentes, de estudios, de experiencia, de referencia laborales y revisar que estén acordes con los estudios previos de acuerdo con las políticas de contratación que existan en la RAP-E.

- De igual manera, se solicita firmen un Acuerdo y/o Cláusula de Confidencialidad; este documento debe ser anexado a los demás documentos relacionados con la ocupación del cargo

- Cada Supervisor de Contrato debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad para los contratistas y por terceras partes, antes de otorgar acceso a la información de la RAP-E.

Términos y condiciones Laborales

- Los funcionarios, contratistas y terceros de la RAP-E deben cumplir con los requerimientos de seguridad de la información, deben conocer y aceptar la Política de Seguridad de la Información y Protección de Datos de la que trata este documento.

- Cada funcionario y contratista de la RAP-E debe firmar los Acuerdos de Confidencialidad en la que se garantice la confidencialidad e integridad de la información que ellos manejen. Así mismo cumplir con la cláusula de Derechos de Autor de acuerdo con el artículo 20 de la Ley 23 de 1982, modificado por el artículo 28 de la Ley 1450 de 2011.

Durante la ejecución del empleo

- Los funcionarios de la RAP-E son capacitados para las funciones y actividades a desempeñar con el fin de proteger adecuadamente los recursos y conocer las políticas de seguridad de la información de la entidad. Esta capacitación o reinducción será responsabilidad de cada área en conjunto con la dirección administrativa y financiera, a cargo del proceso gestión TIC.

Política de desvinculación, licencias, vacaciones y personal provisto por terceros

- la dirección administrativa y financiera, a cargo del proceso gestión TIC, realizara el proceso de desvinculación, por cuestión de vacaciones licencias, o demás situaciones administrativas, en las que se encuentre inmerso el funcionario o contratista de la entidad llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Acuerdos de Confidencialidad o 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 entidad para la protección de la información.

En todo convenio o contrato que la entidad firme con sus funcionarios, contratistas, y demás personal será necesario:

- Establecer una cláusula de confidencialidad de la información.
- En el caso de los contratistas se debe incluir dentro de los contratos la cláusula de confidencialidad y reserva de la información a la cual tengan acceso mientras permanezcan en la entidad.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

La RAP-E, debe asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, incluyendo los requisitos para sistemas de información que prestan servicios sobre redes públicas.

- Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

Análisis y Especificaciones de Requisitos de Seguridad de la Información

- La RAP-E, establecerá los requisitos relacionados con seguridad de la información, los cuales deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

Seguridad de Servicios de las Aplicaciones en Redes Públicas

- La RAP-E, debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas, mediante un proceso de gestión de tecnología de información y comunicación.

Política de desarrollo seguro

- La RAP-E debe establecer las condiciones y vigilar que el desarrollo y mantenimiento llevado a cabo, tanto internamente como por proveedores externos, para que cumplan con buenas prácticas para el desarrollo seguro, además de establecer criterios de seguridad que deben ser considerados en todas las etapas de desarrollo.

Requisitos de Seguridad en el Desarrollo de los Sistemas de Información

- La construcción y modificación de sistemas de información o la implementación de nuevos módulos a los sistemas de información misionales o de apoyo, desarrollados al interior de la entidad o contratados con terceras partes, deben contemplar un completo análisis de requerimientos en cuanto a seguridad de la información, análisis de riesgos y posibles escenarios de riesgos asociando los controles respectivos para la mitigación de estos.

Procedimiento de Control de Cambios

- Cualquier tipo de cambio sobre los sistemas de información deberá seguir lo establecido en las buenas prácticas de desarrollo, debe tener en cuenta la aceptación de las pruebas técnicas y funcionales dictaminadas por cada uno de los responsables a quienes afectan los cambios que se realicen.

- Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.

- Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.

Desarrollo de Software Contratado Externamente

- El desarrollo de software contratado con terceras partes deberá contemplar todos los requisitos en cuanto a seguridad de la información fijados en este documento, solo se darán por recibidos desarrollos realizados sobre los estándares de la entidad en cuanto a herramienta de desarrollo, y pruebas técnicas y funcionales.

- Los contratos de desarrollo de software con terceros deberán tener claramente definidos los alcances de las licencias, los derechos de propiedad del código desarrollado y los derechos de propiedad intelectual, junto con los requerimientos contractuales relacionados con la calidad y seguridad del código desarrollado.

- Se debe realizar un análisis de vulnerabilidades técnicas a los sistemas de información desarrollados y que estén en proceso de paso a producción, para garantizar que los nuevos desarrollos no exponen la seguridad de la información de la RAP-E ni su infraestructura. Esta actividad debe quedar claramente definida con los terceros.

iii. POLÍTICA DE CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS TIC

La RAP-E garantiza que para asegurar la continuidad de los servicios TIC, existen roles y responsabilidades para la operación del Plan de contingencias de TI, para ello en esta política se presentan la identificación de los riesgos y los responsables de su administración, contiene el inventario de activos de TI, sobre los cuales se deben realizar las actividades prioritarias en caso de presentarse un evento que pongan en riesgo la continuidad de la operación y la prestación de los servicios de TI.

Ante la ocurrencia de eventos no previstos en cuanto a la indisponibilidad del centro de datos principal, la RAP-E debe contar y asegurar la implementación de un Plan que asegure la continuidad de las operaciones tecnológicas de sus procesos críticos.

Para ello, la entidad teniendo claro que su recurso más importante es el Recurso Humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier situación, hará uso de los brigadistas en caso de tener que abandonar las instalaciones de la oficina.

La RAP-E dispone de las instalaciones de procesamiento de información las cuales no cuentan con redundancia suficiente para cumplir los requisitos de disponibilidad de la información por lo cual es requerido definir cuales sistemas se consideran prioritarios para que a aquellos activos crear un plan específico.

COPIAS DE RESPALDO (BACKUP)

- La RAP-E proporcionar medios de respaldo adecuados para asegurar que la información esencial y el software asociado se puedan recuperar después de una falla.

- La información crítica de la entidad, como backups específicos, bases de datos de los sistemas de información, o información solicitada de manera electrónica se respaldada regularmente sobre un medio de almacenamiento en Disco Externo, de acuerdo con su nivel de criticidad identificada en el inventario de activos de información.

- Los medios se almacenarán en la sala de equipos de cómputo, la cual cuenta con los mecanismos de protección ambiental como detección de humo y aire acondicionado, todo esto de acuerdo con los procedimientos establecidos para la ejecución y restauración de copias de respaldo.

- Se deben realizar pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad. Estos aspectos técnicos se deben registrar en el formato de Control de Restauración de Información, todo esto de acuerdo con los procedimientos establecidos para la ejecución y restauración de copias de respaldo. (Ver Procedimiento de Administración de Backups y Restore).

- El profesional especializado de la dirección administrativa y financiera, con responsabilidades del procedimiento de Gestión TIC, es el garante de definir la frecuencia de respaldo, el tipo, el medio de almacenamiento y los requerimientos de seguridad de la información.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- La RAP-E debe gestionar adecuadamente los incidentes de seguridad de la información presentados en el contexto de la entidad, y debe ser administrador e informados a la dirección administrativa y financiera.

- Es responsabilidad de cada uno de los funcionarios de la entidad y terceras partes, reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información; esto con el fin de proceder con el tratamiento respectivo.

- A todos los incidentes de seguridad reportados, se les debe dar el tratamiento y seguimiento respectivo, realizando el respectivo trámite ante las instancias correspondientes.

- Responsabilidades y Procedimientos.

- El procedimiento para la gestión de los incidentes reportados por colaboradores y usuarios debe ser revisado periódicamente por el Jefe de la dirección administrativa y financiera, a cargo del proceso gestión TIC con el fin de identificar cambios o ajustes pertinentes que garanticen la eficiencia y eficacia de las respuestas.

- Se asigna como responsable para la entidad de la gestión de los incidentes de seguridad al Profesional especializado encargado del proceso de gestión TIC, quien debe documentar y conservar trazabilidad de los eventos y debilidades reportadas por los colaboradores y usuarios. Los registros deben ser conservados garantizando que se reciben notificación de los resultados después de tratado y solucionado el problema, en el Sistema de Medición análisis y Reporte para la toma de decisiones SMART.

Reporte de Eventos de Seguridad de la Información

- El reporte de eventos, debilidades o incidentes que comprometan la gestión de datos personales, seguridad de la información o continuidad del negocio es una actividad obligatoria para todos los colaboradores y usuarios asociados a los activos y servicios de la Rap-E

- Por ello, se debe velar por que los colaboradores y usuarios reciban capacitación para registro y/o reporte de eventos y debilidades de gestión de la privacidad, seguridad de la información y continuidad del negocio.

- Cuando se detecte un evento o incidente en la seguridad de la información que puede culminar en una acción legal, se debe iniciar el tratamiento del incidente acorde al procedimiento Gestión de Incidentes de la entidad.

iv. POLÍTICA DE DISPOSITIVOS MÓVILES Y TELETRABAJO

La RAP-E, garantiza la seguridad de Teletrabajo y el uso de dispositivos móviles a través del cumplimiento de las siguientes políticas:

POLÍTICA PARA DISPOSITIVOS MÓVILES

- La RAP-E, controla, gestiona y aprueba el manejo de los dispositivos móviles (teléfonos inteligentes, portátiles, discos duros, USB, DVD) institucionales [1]que hagan uso de los sistemas de información y/o equipos de la entidad.

- La dirección administrativa y financiera a cargo del proceso gestión TIC, debe establecer las configuraciones aceptables para los dispositivos institucionales o personales que hagan uso de los servicios provistos por la entidad.

- Los usuarios de los dispositivos móviles institucionales deben evitar el uso de estos en lugares que no les ofrezcan garantías de seguridad física para evitar pérdida o hurto.

- Los usuarios de los dispositivos móviles institucionales no deben modificar las configuraciones de seguridad, ni desinstalar software o instalar programas en los dispositivos móviles institucionales bajo su responsabilidad.

- Al conectar un dispositivo móvil a la red de la RAP-E, el propietario del dispositivo acepta las políticas definidas en el presente manual.

[1] Los equipos y dispositivos móviles propiedad de los funcionarios, con los cuales se acceda a los sistemas de información de la RAP-E por cuestiones de teletrabajo DEBEN cumplir con los requisitos expuestos en este documento.

- La dirección administrativa y financiera a cargo del proceso gestión TIC, designará personal con el fin de que realice la inspección técnica a los puestos de trabajo con el fin de garantizar que la comunicación y operación de los equipos de cómputo sea eficiente.

- Con relación a la información, dado que esta se considera como el recurso intangible de mayor importancia, se establecen las siguientes directivas con el fin de prevenir cualquier anomalía:

- Confidencialidad: asegurar el acceso a la información únicamente por las personas autorizadas, que son los teletrabajadores.

- De igual forma como se debe propender por reducir las amenazas relacionadas con los recursos intangibles, también se deben establecer los procedimientos relacionados con la protección de los recursos tangibles a través de un análisis de riesgos ocasionados por la implementación de teletrabajo, como por ejemplo establecer procesos de manejo de equipos, mantenimiento de equipos, entre otros.

SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

- Los equipos portátiles que contengan información CLASIFICADA o RESERVADA deberán almacenar en todo momento la información laboral en el ONE DRIVE, la dirección administrativa y financiera a cargo del proceso TIC, no se hace responsable por información almacenada de manera directa en los discos duros de los equipos.

- Los equipos portátiles no deberán dejarse a la vista en el interior de los vehículos. En casos de viaje siempre se deberán llevar como equipaje de mano.

- En caso de pérdida o robo de un equipo portátil se deberá informar inmediatamente a la Dirección de Gestión Corporativa y se deberá poner la denuncia ante la autoridad competente y allegar copia de esta.

- Cuando un equipo de cómputo deba retirarse de las instalaciones de RAP-E se esté queda baja la responsabilidad del funcionario.

v. RESPONSABILIDAD DE LOS USUARIOS

Los funcionarios y contratistas son responsables del usuario asignado y de su contraseña, por lo tanto, cualquier acción que se realice utilizando su usuario es responsabilidad del funcionario o contratista.

Las contraseñas son de uso personal e intransferible, deben estar compuestas por 8 caracteres, incluido mayúsculas. Minúsculas y caracteres especiales.

Los usuarios deben cambiar su contraseña la primera vez que se usen las cuentas asignadas igualmente lo deben hacer cada que el periodo esté próximo a vencer, ya que una vez pasado el tiempo dado por la Oficina de TIC, se bloqueará automáticamente.

USO DE INFORMACIÓN CONFIDENCIAL

Los servicios de información, las bases de datos, y demás sistemas de archivos, administrador por el proceso de Gestión TIC, tiene definido un procedimiento formal de registro de usuarios para otorgar y revocar el acceso, este procedimiento incluye:

- Identificadores de usuarios únicos de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo funcionario.
- Verificar que el usuario tiene autorización del propietario de la información para el uso del sistema, base de datos o servicios de información.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso a los usuarios que cambiaron sus tareas o aquellos a los que se les revocó la autorización, o se desvincularon
- Efectuar revisiones periódicas con el objeto de cancelar identificadores y cuentas de usuario redundantes, inhabilitando así las cuentas que estén inactivas por más de 30 días.

ROLES Y RESPONSABILIDADES

A continuación, se definen los tres niveles de gestión (estratégico, táctico y operativo) y sus responsabilidades durante una situación de contingencia de TI.

Esta definición de roles y responsabilidades permite a la entidad, segregar funciones y roles separando los deberes para que las tareas y áreas de responsabilidad no presenten conflicto alguno; en cada nivel se debe

establecer un plan de sucesión para que en caso de no estar disponible el funcionario principal, pueda actuar su reemplazo con la misma autoridad y responsabilidad:

- Nivel Estratégico: Este nivel corresponde básicamente a la planeación del logro de los objetivos del plan continuidad de la operación de los servicios tic, se basa en decidir las políticas, directrices y los recursos para lograr su efectividad en caso de presentarse una interrupción no planeada en la entidad.

- Nivel Táctico: Llevará a cabo la coordinación de las actividades que se deriven del Plan de continuidad de la operación de los servicios tic, así como, la evaluación de las situaciones de interrupción y dará lineamientos para la operación de estos, a su vez es el encargado de escalar al nivel estratégico en un lenguaje claro las necesidades de la operación y brindará los insumos para la evaluación.

- Nivel Operativo: Este nivel realiza la asignación de las tareas puntuales en el momento de presentarse un incidente o evento inesperado que activa el plan continuidad de la operación de los servicios tic, de la entidad. se ejecuta a partir de los lineamientos proporcionados por los niveles estratégico y táctico.

Contacto con las Autoridades

La RAP-E debe mantener contacto con todas las entidades que representan autoridad en temas de seguridad de la información con el fin de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información, se mantendrán contactos con las siguientes entidades especializadas en temas relativos a la seguridad de la información:

- **MINTIC** - Ministerio de Tecnologías de la Información y las Comunicaciones (y particularmente con:

- **COLCERT** – Grupo de Respuesta a Emergencias Cibernéticas en Colombia. (http://www.colcert.gov.co/). Tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual está enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

- **CSIRT-CCIT** – Centro de Coordinación Seguridad Informática Colombia. (http://www.cert.org.co/). CSIRT-CCIT es un centro de coordinación de atención a incidentes de seguridad informática colombiano, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas y está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas.

- **CCP** – Centro Cibernético Policial. (http://www.ccp.gov.co/). El Centro Cibernético Policial es la dependencia de la Dirección de Investigación Criminal e INTERPOL encargada del desarrollo de estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.

- **SIC** - Superintendencia de Industria y Comercio. A la Superintendencia de Industria y Comercio, corresponde la Protección de la Competencia, Propiedad Industrial, Protección.

VI. Roles de Responsabilidad

En concordancia con el esquema de líneas de defensa adoptado por la Región Administrativa y de Planeación Especial RAP-E Región Central, mediante la Resolución 057 de 2023, se definen los siguientes roles de responsabilidad para la implementación de la Política de Datos:

Línea Estratégica

La línea estratégica de la política de protección de datos personales de la Región Administrativa y de Planeación Especial estará a cargo del Comité Institucional de Gestión y Desempeño acorde con el marco funcional para su operación.

Primera Línea

Todos los funcionarios, contratistas y colaboradores que, en el desarrollo de sus funciones u obligaciones, según su tipo de vinculación, deberán velar operativamente por el cumplimiento de los lineamientos brindados en esta política de gestión, al igual que las regulaciones en materia de gestión documental asociadas a la correcta aplicación de la política de seguridad y privacidad de la información

Segunda Línea

Dirección Administrativa y Financiera, en cabeza del proceso de gestión TIC, Será responsable de implementar y supervisar las prácticas de seguridad de la información de acuerdo con la ley con el apoyo jurídico.

Tercera Línea

Control Interno.

VII. Reportes al Comité Institucional de Gestión y Desempeño:

Esta política será documentada y comunicada a todos los miembros de la organización y partes interesadas a través de la página web https://regioncentralrape.gov.co/ en cumplimiento a lo establecido en el artículo 7 de la Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

VIII. Vigencia de la Política

Esta política entrará en vigor a partir de la fecha de su aprobación y será revisada periódicamente para garantizar su relevancia y eficacia en armonización con lo establecido en los instrumentos de planeación. Mínimo una vez al año en el marco del comité, se realizará el seguimiento para establecer necesidades de ajuste o modificaciones.

IX. Armonización

Modelo Integrado de Planeación y Gestión (MIPG)

Este modelo surge como una iniciativa integradora del Sistema de Desarrollo Administrativo y el Sistema de Gestión de la Calidad, que además engrana el Sistema de Control Interno con el propósito de reducir tiempos, facilitar procesos y servir de guía para la toma de decisiones.

Es por esto, que la política que se declara mediante este documento se asocia de manera transversal bajo los siguientes objetivos y directrices:

Objetivo: Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua.

Dimensión - Información y Comunicación: En esta dimensión se reconoce claramente la importancia de los documentos ya que tiene como propósito garantizar un adecuado flujo de información interna

Otras Políticas de la RAP-E Región Central

La presente política reconoce el Manual de Políticas y de Operación como instrumento en el que se definen los componentes y lineamientos requeridos para la implementación del Modelo Integrado de Planeación y Gestión en la Región Central RAP-E. Este se constituye como un elemento de uso transversal para la declaración de las demás políticas en la entidad.

X. Control de cambios

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
Vr.1.0	05/08/2024	Gestión TIC	versión inicial