Políticas de seguridad y privacidad de la información

La **REGIÓN ADMINISTRATIVA DE PLANIFICACIÓN EJE CAFETERO**, mediante la adaptación e implementación de los lineamientos del modelo de seguridad y privacidad de la información orientado a la gestión de sus buenas prácticas el cual conserva, administra y vigila la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información mediante la gestión de controles en la entidad. Previniendo acontecimientos cumplimiento las obligaciones reglamentarias encaminados a la protección de los Sistemas de Gestión de Seguridad de la Información controlando el acceso, uso y manejo adecuado de los sistemas informáticos a través de políticas y programas, para mejorar las actividades de los funcionarios.

El comité Institucional de gestión y desempeño debe aprobar las políticas de seguridad y privacidad de la información, demostrando así su compromiso con la seguridad de la información en la entidad. Una vez aprobada dichas políticas, la alta dirección entra a revisar periódicamente la aplicabilidad y vigencia de las siguientes políticas específicas de seguridad informática y ejecutar los ajustes necesarios sobre ellas para que sean funcional y se puede seguir exigiendo su cumplimiento por parte de todos los funcionarios y personal suministrado por terceras partes que proveen los servicios.

CONDICIONES GENERALES

- El Ingeniero de sistemas con el apoyo de las demás dependencias que hacen parte de la entidad, serán los responsables de hacer cumplir las políticas enunciadas de acuerdo con las indicaciones y lineamientos establecidos.
- La Región Administrativa y de Planificación Eje Cafetero hará responsable al usuario del conocimiento de la presente política y las consecuencias que se derivan del incumplimiento. Así mismo, el usuario deberá conocer las políticas desde su ingreso a la organización.
- La Región Administrativa y de Planificación Eje Cafetero se reserva el derecho a evaluar periódicamente el incumplimiento de esta (Tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo a los procedimientos establecidos por la entidad y en estricto acato de las estipulaciones legales vigentes.
- En materia de Irregularidades o incumplimiento en el uso del software, el usuario que no cumpla la política será directamente responsable de las sanciones legales (que, por responsabilidad laboral, penal Y/o civil se incurra) derivadas de sus propios actos.

GESTIÓN DE ACTIVOS

La Región Administrativa y de Planificación EJE CAFETERO tiene definida las responsabilidades y deberes con respecto a la seguridad de la información, y asegurar la concientización de funcionarios y terceros respecto a la importancia y el cumplimiento de la normatividad definida.

Los Terceros que efectúen el tratamiento de la información propia de la entidad o sobre la cual sea responsable, deben cumplir con la política de seguridad de la información

- Una vez al año se deben revisar, verificar y actualizar los activos de información para definir deberes, obligaciones, responsabilidades y posibles fallas que se requieran mejorar
- Implementar una gestión de riesgos en los activos de información teniendo clara las herramientas a usar de acuerdo con el Manual de riesgos sugerido por el MINTIC
- Solo él personal del área de TI está autorizado para realizar descargas, instalaciones, modificaciones o cambios en los equipos de cómputo, periféricos, software y redes en las instalaciones de la entidad.
- Cualquier cambio o modificación que se necesite hacer, se debe informar por escrito al área de gestión de TI
- Se debe promover el buen uso de los activos de información, conservando el derecho a la intimidad, privacidad, el habeas data, y la protección de los datos y de sus propietarios.
- Una vez Cese la relación laboral con la entidad todo funcionario o contratista debe entregar los activos de información a su cargo con el jefe directo o supervisor de cada área.
- La entidad se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente.
- Los controles serán diseñados para proveer un nivel de protección de la información apropiado y consistente dentro de la empresa, sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.
- Todos los activos de información están inventariados y/o identificados por la Subgerencia Administrativa y Financiera, Su responsabilidad será entregada a cada usuario durante su tiempo de uso.
- El usuario que tiene bajo su custodia los recursos tecnológicos debe velar por los mismos, acatando las normas del uso adecuado para evitar daños.
- La Subgerencia Administrativa y Financiera con apoyo del subproceso de Gestión de Sistemas de las tecnologías de la información, administra los recursos TI de la Entidad y fijará las indicaciones para la modernización tecnológica de la entidad, en función de la mejora continua para la optimización de los servicios prestados a los usuarios internos y externos.
- En caso de requerir soporte técnico, el usuario debe hacer la solicitud al Subproceso de Gestión TI.
- En caso de detectar alguna violación a las políticas y lineamientos de TI mencionadas, reportar a soporte técnico y/o por la herramienta de Gestión de Recursos de TI de la entidad

- Las aplicaciones, los computadores y cuentas inscritas que son entregadas a los Usuarios para facilitar su trabajo. no tienen privacidad en relación con la información manejada el cual pertenece a la Entidad.
- Toda información, aplicaciones o contenido encontrado en los equipos tecnológicos de la Entidad, que no cumpla requerimientos laborales, será borrada y se reportara el usuario para las sanciones
- El subproceso de Gestión de TI mantendrá actualizado las hojas de vida de los equipos tecnológicos e informará de los ajustes pertinentes a la Subgerencia Administrativa y Financiera, Control Interno y demás dependencias que lo requieran.
- Los usuarios deben tener copias de respaldo de la información relevante de su labor en el servidor de almacenamiento en el área de trabajo.
- verificar que los equipos de la entidad utilizan usuario y contraseña
- Conservar al día todas las solicitudes relacionadas con los equipos tecnológicos (sistemas de información, redes, servidores, conectividad, especificaciones técnicas y aplicaciones)
- Toda modificación no autorizada de información de la Entidad almacenada en medios físicos removibles, como USB, Cd, DVD, entre otros están prohibidas
- Está Prohibido el uso de software no licenciado en los equipos de la entidad.
- Está prohibido copiar el software licenciado de la entidad en los equipos personales sin previa autorización del Subproceso de Gestión de sistemas de información
- El uso de la red de la entidad para los equipos que no hacen parte de esta sólo es permitido por el wifi

SEGURIDAD EN EL RECURSO HUMANO

Capacitar en seguridad de la información y de los procedimientos de gestión de incidentes de seguridad a funcionarios y contratistas para reconocer la normatividad relacionada con la seguridad de la información en la empresa ya que el desconocimiento de esta no los exonerará de los procesos disciplinarios definido ante violaciones de las políticas de seguridad

SEGURIDAD FÍSICA

- Disponer de áreas seguras para la gestión, almacenamiento y procesamiento de información de la RAP. Las áreas deben contar con protecciones físicas y ambientales acordes con el valor y la necesidad de aseguramiento de los activos que se protegen, incluyendo la definición de perímetros de seguridad, controles de acceso físicos, seguridad para protección de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales adecuadas de operación y sistemas de contención, detección y extinción de incendios.

- El ingreso de terceros al centro de datos y cableado debe estar debidamente registrado por el personal de vigilancia.
- Los privilegios de acceso físico a los centros de datos deben ser actualizados en caso de terminación o cambio del contrato del personal encargado
- El centro de Datos debe contar con mecanismos de control de Acceso tales como puertas de seguridad, sistemas de alarmas o controles biométricos; sistemas de detección y extinción automáticas de incendios, control de inundación y alarmas en caso de detectarse condiciones inapropiadas, estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.
- Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los funcionarios se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.
- Los funcionarios o terceros que presten sus servicios a la RAP no deben intentar ingresar a áreas a las cuales no tenga la debida autorización
- La seguridad de los equipos de cómputo fuera de las instalaciones será responsabilidad de cada funcionario y contratista asignado, junto con una autorización del jefe inmediato.
- Los accesos a áreas seguras deberán tener un control de acceso físico, y no se debe permitir ingresar equipos fotográficos, de filmación, grabación de audio u otras formas de registro salvo con autorización especial del responsable del área segura.
- Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.
- Es responsabilidad del usuario mantener el área del equipo libre de alimentos, bebidas u otro cualquier elemento que pueda dañar sus componentes.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

- A efectos de proteger la integridad y confidencialidad de los activos de información es imprescindible que se cuente con protecciones contra el software malicioso, mantenimiento de los equipos de cómputo, administración de red y bloqueo de puertos de red de telecomunicaciones
- La oficina de gestión de sistemas de información debe garantizar los recursos necesarios que aseguren la separación de ambientes de desarrollo, pruebas y producción, así como de la independencia de los funcionarios que ejecutan dichas labores
- Todos los usuarios de activos de información tecnológicos y recursos informáticos que requieran la adición o modificación de funcionalidades de estos, deben solicitar el cambio por medio del procedimiento vigente para dicha acción.

- Toda adquisición, mantenimiento y eliminación de medios de almacenamiento deberá ser realizada por el Subproceso de Gestión de Sistemas de Información, de manera que se garantice seguridad en estos activos de información

USO DEL CORREO ELECTRÓNICO

- Los servicios de mensajería electrónica son de uso exclusivo para actividades relacionadas con la entidad, por lo tanto, queda prohibida el uso para fines personales.
- Está restringido el envío de mensajes con archivos de música, videos, imágenes pornográficas y/o programas, ya que este tipo de archivos facilitan la propagación de virus e incrementa el ingreso de correos no solicitados. Al igual que él envió de correos que no hacen parte del desarrollo normal de la entidad.
- Se prohíbe el correo masivo de correos
- Se prohíbe él envió de copias con información confidencial sin el consentimiento del remitente original
- Se prohíbe a los usuarios suscribirse a las listas de correo electrónico o participar en grupo de noticias que divulguen información o mensajes ajenas a las funciones y labores de la RAP EJE CAFETERO
- Todo usuario del correo electrónico deberá leer y responder oportunamente los mensajes y citaciones que se envíen por este medio: con el fin de aprovechar el mayor beneficio que ofrece el correo electrónico que es la rapidez y efectividad de las comunicaciones
- No enviar correo spam como son cadenas, pornografía. Chistes, videos o cualquier otro similar
- Depurar la información del correo eliminando lo que no utilice y guardando los contenidos importantes para la entidad
- Todo correo enviado debe tener un TITULO y ASUNTO que refleje el contenido del mensaje
- No abrir correos cuyo remitente le sea desconocido o cuyo asunto le resulte sospechoso, por lo general estos contenidos vienen con virus
- El usuario del correo electrónico tiene derecho a manejar su información en forma confidencial, asumiendo toda responsabilidad por dicho uso.

CONTROL DE ACCESO

El compromiso de la entidad es realizar control de acceso a la información, sistemas y de red, así como a monitorear el ingreso, de tal forma que este sea seguro, sin importar si los mismos son electrónicos o físicos. De igual forma se protege la información generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activos, así como el riesgo que se genera de los

accesos otorgados a terceros como son proveedores y contratistas, son igualmente supervisados y controlados por la entidad.

- Deben establecerse medidas de control de acceso al sistema operativo, para garantizar la autenticación de los funcionarios.
- Los funcionarios no deben utilizar ninguna estructura o característica de contraseña que podría dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical. La longitud mínima de las contraseñas será igual o superior a 8 caracteres y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
- Se debe permitirse identificar de manera inequívoca cada usuario, dejar registro de las actividades que realiza.
- Los usuarios finales no deben configurar, instalar y eliminar software de los equipos de cómputo de la empresa, la interfaz del sistema operativo debe estar configurada de tal forma q tengas solo privilegios de invitado. todas las labores deben ser estrictamente realizadas por el proceso de gestión de sistemas de información.
- Todos los usuarios con acceso a un sistema de información o a la red informática de la RAP EJE CAFETERO dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña, serán responsables de las acciones realizadas por el usuario que ha sido asignado.
- el acceso a la información de la RAP EJE CAFETERO deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad
- El Sistema Operativo de los equipos de los funcionarios de la RAP EJE CAFETERO deben mantenerse bloqueados en ausencia de este.
- La asignación de privilegios a las aplicaciones informáticas presentes en la RAP EJE CAFETERO, debe ser solicitada al jefe inmediato o al área de gestión de sistemas de información.
- los entes externos que tienen acceso a información crítica de la RAP EJE CAFETERO, deben suscribir para acuerdos para salvaguardar la información.
- Los subgerentes de las áreas están en la obligación de avisar oportunamente el ingreso, retiro, cambio de funciones del personal al Subproceso de Gestión de TI, para la activación o inactivación de cuentas en los sistemas informáticos.
- Las cuentas de acceso de los Sistemas Informáticos son exclusivamente para cada usuario y no debe compartir.
- El acceso a los aplicativos será bloqueado con 5 intentos fallidos al digitar la contraseña. Su desbloqueo debe ser solicitado la Subproceso de Gestión TI

- El acceso a las instalaciones de procesamiento de datos es restringido a personas no autorizadas, al igual que los cuartos de equipos.
- Todos los funcionarios, deberán portar el carné en un lugar visible para facilitar el control de las personas que ingresan y transitan en la Entidad.
- Los equipos de la entidad deben estar conectados a los tomacorrientes regulados que disponen las instalaciones.

SERVICIO DE INTERNET

- El acceso a Internet es SOLO de uso laboral. Por tal razón, está restringido según el requerimiento y funciones de cada usuario.
- El uso de salas de chat está prohibido
- Está prohibido la descarga de archivos de música, videos y similares. De ser necesario la descarga este debe ser validado por el personal encargado de la Gestión de TI
- Los usuarios que estén haciendo uso indebido de los recursos informáticos serán notificados a su jefe inmediato y se les suspenderá el servicio por una semana, de reincidir en la falla se le notificará a la subgerencia y el servicio será suspendido hasta nueva orden.
- Se garantiza la disponibilidad de internet en un 90%
- Se autoriza la navegación en ´paginas cuyo contenido este acorde a las necesidades de la entidad
- El uso indebido de internet es responsabilidad del usuario y se considerará una falta al reglamento interno de trabajo y será sancionado como tal.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

- LA RAP EJE CAFETERO debe asegurar que se haga el diseño e implementación de los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.
- La RAP EJE CAFETERO, debe establecer controles para cifrar la información que sea considerada sensible y evitar posibilidad de repudio de una acción por parte de un usuario del sistema. Se deben asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.
- La información tratada por las aplicaciones aceptadas por la empresa debe preservar su confiabilidad desde su ingreso, transformación y entrega.

GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- LA RAP EJE CAFETERO, debe asegurar que se establecen y ejecutan procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en la entidad de los incidentes de seguridad de la información.
- Todos los usuarios de la información de la RAP EJE CAFETERO deben reportar los incidentes de seguridad que se presenten, según el procedimiento vigente.
- En la gestión del incidente y cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables.

GESTIÓN DE LA CONTINUIDAD DE LOS PROCESOS

Debe evaluarse el impacto de las interrupciones que afectan la operación de los procesos críticos de la Empresa y definir e implementar planes de continuidad y de recuperación ante desastres para propender por la continuidad de esta. Los planes deben considerar medidas tanto técnicas como administrativas para que se puedan recuperar oportunamente las funciones de los procesos y la tecnología que las soporta.

- Los planes de continuidad y de recuperación deben probarse y revisarse periódicamente y mantenerlos actualizados para su mejora continua y garantizar que sean efectivos.
- Para los procesos críticos de la Empresa, se debe contar con instalaciones alternas y con capacidad de recuperación, que permitan mantener la continuidad de los procesos, aún en caso de desastre en las instalaciones de los lugares de Operación.
- Cada lugar debe incluir los controles establecidos para este tipo de áreas según su clasificación, para que no se vea disminuida los aspectos de seguridad en caso de desastre.
- Se debe seguir una estrategia de recuperación alineada con los objetivos de la RAP, formalmente documentada y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos, ante el evento de una contingencia.

CUMPLIMIENTO

- LA RAP EJE CAFETERO, gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo entre otros los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros, la privacidad, los, delitos informáticos, el uso inadecuado de recursos de procesamiento, el uso de criptografía y la recolección de evidencia.

- Cumplimiento de la normatividad y los controles relacionados con la seguridad de la información y los que son técnicamente compatibles con los diferentes ambientes o tecnologías de la empresa.
- Todos los productos de Software que se adquieran e instalen en los equipos de cómputo de la Empresa deben contar con su respectiva licencia de uso.
- Realización de auditorías, para verificar la eficacia de los controles y asegurar la administración de los riesgos de seguridad de la información.
- La Política junto con el Sistema de Gestión de Seguridad de la Información de la RAP EJE CAFETERO, debe ser auditado anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.
- La información de auditoría generada por el. Uso de los controles de seguridad de los Recursos de Tecnología, debe ser evaluada por el responsable para Detectar Violaciones a la Política.
- Reportar incidentes de seguridad. Constatar que los datos registrados incluyen evidencias suficientes para el seguimiento y resolución de incidentes de seguridad.
- Los contratos de trabajo y los contratos de desarrollo realizados por proveedores y contratistas deben contar con cláusulas respecto a la propiedad intelectual que le pertenece a LA RAP EJE CAFETERO.

NO REPUDIO

- Agregar registros que permite la trazabilidad en la modificación de cualquier dato o información en los sistemas de información.
- Toda información enviada por los medios institucionales debe ser responsabilidad de cada funcionario
- El Subproceso de gestión de TI provee estrategias de seguridad para el tratamiento de mensajes electrónicos en la Ley 527 de 1999 «Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las Entidades de certificación y se dictan otras disposiciones».