POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL GUAVIO

ALCANCE

Las presentes políticas de seguridad aplican o están destinadas a todos los servidores públicos, contratistas y terceras partes relacionadas con la Corporación Autónoma Regional del Guavio que utilicen los recursos o infraestructura de tecnología de la misma.

Este documento procura ser una forma de comunicación con todos los usuarios, ya que se establece como un canal formal de actuación del personal en relación con los recursos y servicios informáticos de la Corporación.

En este sentido, es importante tener cuenta las características que definen la seguridad de un sistema:

INTEGRIDAD: Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

CONFIDENCIALIDAD: Propiedad por la cual la información relativa a una entidad o parte no se pone a disposición de individuos, entidades o procesos no autorizados ni se revela a éstos.

DISPONIBILIDAD: Propiedad de la información de ser accesible y utilizable a petición por una entidad autorizada. Es decir, que se pueda acceder a la información o recursos por las personas, procesos o aplicaciones, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.[1]

IRREFUTABILIDAD (No repudio): Posibilidad de impedir que un emisor niegue posteriormente que ha enviado un mensaje o realizado una acción, igual el receptor.

Las políticas de seguridad están encaminadas principalmente a proteger la información, el uso apropiado de los equipos y el manejo eficiente de los servicios informáticos que presta la Corporación, por esto deben ser socializadas de acuerdo a las actualizaciones que surjan y ser publicadas en un sitio al que pueda acceder el personal objeto de las mismas.

El proceso de Tecnologías de la Información y las Comunicaciones es el responsable de efectuar el seguimiento a las políticas y verificar que se estén cumpliendo y aplicando de forma adecuada. En caso de observarse o detectarse algún incumplimiento, éste debe ser reportado a la Secretaría General.

[1] *UIT-T (Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones)*

DEFINICIONES

ACTIVO: Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Son tres los elementos principales que conforman los activos:

- **Información:** Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.
- **Equipos que la soportan:** Software y hardware.
- **Usuarios:** Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

APLICACIÓN: Cada uno de los programas que nacen de la necesidad de la Entidad, propios o adquiridos, los cuales una vez ejecutados, permiten trabajar con el computador. Diseñados para cumplir una función específica.

CONFIDENCIAL: Se aplica a lo que se hace o dice de manera reservada o secreta o con seguridad recíproca entre varias personas: informe, proyecto confidencial.

CONTRASEÑA: Una contraseña o clave (en inglés password) es una forma de autentificación que utiliza información secreta para controlar el acceso a algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. Aquellos que desean acceder a la información se les solicitan una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

CUENTA: Es una colección de información que indica a los usuarios que puede obtener acceso a diferentes medios informáticos, archivos y carpetas. Las cuentas de usuario permiten que se comparta el mismo equipo entre varias personas, cada una de las cuales tiene sus propios archivos y configuraciones.

Cada persona obtiene acceso a su propia cuenta de usuario con un nombre de usuario y contraseña.

HARDWARE: Conjunto de componentes materiales de un sistema informático. Cada una de las partes físicas que forman un computador, incluidos sus periféricos.

INFORMACIÓN: Conjunto de datos sobre una materia determinada. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se

distribuye o almacena, siempre debe ser protegida en forma adecuada. Tipos de información:

- **Información privilegiada:** Es aquella de carácter concreto que se refiere a uno o varios emisores de valores o a los mismos valores, que no se haya hecho pública y que de hacerse pública podría influir de manera apreciable sobre la cotización de esos valores.
- **Información pública:** Es la información que toda persona tiene derecho a manifestar por medio de la libertad de expresión y difusión de pensamiento oral o escrito, por cualquier medio de comunicación, sin previa autorización, sin censura o impedimento, siguiendo los reglamentos de la ley. También es la información que todo el mundo tiene derecho a solicitar y a recibir de parte de cualquier entidad pública, así sea que tenga un costo o un plazo para ser entregada. Un ejemplo de esto son los informes del estado que deben estar a disposición de cualquiera que lo exija.
- **Información privada:** Es una información que la ley no permite divulgar ya que afecta la intimidad personal, la seguridad nacional, o simplemente es excluida por la ley. Por ejemplo los datos de carácter personal que existen en registros o bancos de datos adquiridos por organismos públicos o privados. Son datos personales que sólo pueden ser divulgados con consentimiento del titular.
- **Información Interna:** Es la información que circula al interior de una empresa u organización. Busca llevar un mensaje para mantener la coordinación entre los distintos departamentos, permite la introducción, difusión y aceptación de pautas para el desarrollo organizacional. Los trabajadores necesitan estar informados para sentirse parte activa de la organización. Esta información es útil para tomar decisiones.

POLÍTICA: Son instrucciones mandatarias que indican la intención de la alta dirección respecto a la operación de la organización.

RIESGO: Posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización.

SEGURIDAD: Estado de cualquier tipo de información que nos indica que ese sistema está libre de peligro, daño o riesgo.

SOFTWARE: Conjunto de programas de distinto tipo (Sistema Operativo y aplicaciones diversas) que hacen posible operar con el computador.

USUARIO: Persona que solicita un servicio o acceso a algún programa, aplicativo o sistema, o para atender un incidente o problema que se presente con la tecnología informática, sea contratista, servidor público u otro que esté autorizado para prestar servicios para la Entidad.

DESCRIPCIÓN DE LAS POLÍTICAS

POLÍTICA 0: IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Toda aquella información que tiene valor para la Corporación y por lo tanto debe protegerse. En este sentido, un activo de información es todo elemento que manipule o contenga información. Se debe entender como activos de información los datos, aplicaciones, personal, tecnología, instalaciones y equipamiento auxiliar.

- Cada proceso de la Corporación deberá elaborar un inventario de los activos de información que posee. Dentro del inventario deberá realizar la correspondiente clasificación, valoración, ubicación y acceso de la información, de tal manera que el proceso de Tecnologías de la Información y las Comunicaciones pueda brindar herramientas que permitan la administración, garantizando la integridad, disponibilidad y confidencialidad de los datos que lo componen.
- Todo servidor público, contratista o colaborador que utilice los recursos tecnológicos de la Corporación igualmente tiene la responsabilidad de velar por la integridad, disponibilidad y confidencialidad de la información que manipula, especialmente si esta información ha sido clasificada como: información privilegiada, privada, interna o tiene algún tipo de reserva.
- Ningún servidor público, contratista o colaborador debe suministrar información de la Corporación a ninguna persona o ente externo sin la debida autorización.
- Todo servidor público, contratista y colaborador de la Corporación, al dejar de prestar sus servicios debe hacer entrega de la información producto de sus labores a su jefe inmediato o supervisor y comprometerse a no hacer uso indebido de esta, ya sea comercializándola o divulgándola directamente o a través de terceros.
- Cualquier servidor público, contratista o colaborador que detecte el uso indebido de la información, está en la obligación de reportar el hecho a la Secretaría General.
- El proceso de Tecnologías de la Información y las Comunicaciones hará los respectivos respaldos de la información o copias de seguridad de acuerdo a la clasificación entregada por cada proceso de la Corporación.
- Todo servidor público, contratista o colaborador de la Corporación debe tener acceso solamente a la información necesaria para el desarrollo de sus labores y se debe tener en cuenta la clasificación de la misma a la hora de asignar privilegios o permisos sobre esta.
- La información procesada, manipulada o almacenada por el servidor público, contratista o colaborador en el desarrollo de sus actividades es de propiedad exclusiva de la Corporación.
- Los servidores públicos, contratistas y colaboradores son responsables de la información que procesan, por lo tanto de su respaldo o almacenamiento.

POLÍTICA 1: SEGURIDAD FÍSICA

Trata de la seguridad física del entorno informático de la Corporación (computadores, hardware de red, dispositivos electrónicos, entre otros), de todo el entorno que los rodea en el lugar donde están ubicados (edificio, sistemas eléctricos, seguridad de las puertas,

entre otros) y de los servidores públicos, contratistas o colaboradores que están encargados de su vigilancia o cuidado o de la vigilancia del acceso a este entorno informático.

- La responsabilidad de la custodia de cualquier elemento mantenido, usado o producido por el servidor público, contratista o colaborador que se retira o cambia de cargo debe estar o recaer en el jefe inmediato o supervisor y este proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.
- La Corporación debe determinar los mecanismos de control de acceso en las dependencias o áreas que considere críticas.
- Los servidores (equipos de cómputo) deben estar en lugares de acceso restringido (centro de cómputo o de datos) y cualquier persona que ingrese a esta área, deberá registrar el motivo de ingreso y en caso de no tener la correspondiente autorización, deberá ingresar en compañía del personal autorizado.
- Cualquier persona (servidor público, contratista, colaborador o visitante) que se encuentre dentro de las instalaciones de la Corporación, ya sea en Sede central o en una Oficina de enlace, debe portar su identificación en un lugar visible.
- En lo posible, en todas las áreas de la Corporación deberán existir elementos de control contra incendio o inundación y cada proceso deberá contar con un plan de contingencia en caso de materialización del riesgo.
- Las zonas o áreas de la Corporación que se consideren críticas deberán tener demarcación con zonas de circulación y zonas restringidas, y contar con los mecanismos de acceso correspondientes para que solamente ingrese el personal que por su rol pueda estar allí.
- Las áreas de cableado deben estar señalizadas como zonas de alto riesgo, tener limitación y control de acceso.
- Todos los elementos (computadores, módems, equipos de comunicación, video beam, cámaras, entre otros) deben registrar su ingreso y salida, sean de propiedad de la Corporación o del personal que labora o visita las instalaciones.
- Equipos tales como: computadores, servidores, equipos de comunicaciones (p.e. router o switch), entre otros, no deben moverse o reubicarse sin que sea informado a la Subdirección de Planeación y Administrativa y Financiera.
- Las copias de seguridad de la información deben estar salvaguardadas en un lugar diferente al que se produce.
- Se debe contar con un sistema de redundancia de los servidores y almacenamiento de datos por lo menos en un sitio alterno al lugar donde están ubicados.
- Los elementos de suministro de energía o tomas eléctricas no deben sobrecargarse (conectar más de un dispositivo) y los equipos de cómputo, deben estar conectados a la red regulada (toma de color naranja).
- En lo posible no consumir alimentos o bebidas cerca de los equipos de cómputo o cualquier elemento de hardware.
- Se debe asegurar el suministro estable y continuo de energía a través de una UPS (Sistema de alimentación ininterrumpida) que regulará la tensión evitando los picos de voltaje que pueda traer la red y proporcionará un tiempo de autonomía en caso de cortes del suministro eléctrico.
- Los equipos de comunicaciones como router o concentradores deben estar en un lugar que permita su control de acceso.
- El personal externo que deba trabajar o manipular hardware de propiedad de la Corporación deberá estar debidamente identificado, estar acompañado del personal

autorizado por la Entidad y registrar las operaciones relacionadas en el formato correspondiente.

- Ningún servidor público, contratista o colaborador está autorizado para intervenir o arreglar dispositivos de tecnología de propiedad de la Corporación a menos que esté autorizado por la Subdirección de Planeación.
- Todo servidor público, contratista o colaborador que deba ingresar en fin de semana o fuera del horario laboral a las instalaciones de la Corporación y necesite utilizar recursos informáticos (internet, impresoras, entre otros) deberá estar autorizado por la Subdirección Administrativa y Financiera e informar a la Oficina de Sistemas con el fin de proveerle dichos servicios.

POLÍTICA 2: SEGURIDAD DE LA RED CORPORATIVA

- La Corporación cuenta con red inalámbrica, el acceso a esta es solo para el personal autorizado (servidores públicos, contratistas, colaboradores y usuarios invitados).
- El uso de internet es para fines Corporativos y es recomendable no mantener abiertas más de tres páginas web en simultánea.
- Los usuarios de la red inalámbrica pueden tener acceso a los servicios de correo electrónico e internet.
- Todo usuario conectado a la red inalámbrica es responsable de tener antivirus actualizado en los equipos de su propiedad.
- El servicio de impresión debe ser solicitado y autorizado para el caso de usuarios invitados y los documentos deben ser de carácter oficial.
- Los usuarios de la red son responsables por la seguridad de la información enviada o recibida a través de esta.
- Las cuentas de correo electrónico asignadas a servidores públicos, contratistas o colaboradores, deben ser usadas solamente para el envío o recepción de información oficial y documentos relacionados con el ejercicio de sus funciones.
- Los servidores públicos, contratistas o colaboradores a los que se les ha asignado una cuenta son directamente responsables de todas las acciones y mensajes que envíen a través de esta.
- Está completamente prohibido la difusión o distribución de cadenas o publicidad de tipo comercial.
- Los mensajes masivos solo pueden ser enviados cuando sean de carácter oficial y de interés general y solo por personas autorizadas. En lo posible evitar adjuntar archivos de gran tamaño.
- La cuenta de correo electrónico es de asignación personal e intransferible, por lo tanto, no deben hacer uso de ella terceras personas.
- La contraseña del correo electrónico no debe ser cedida o facilitada a otros usuarios, siendo de propiedad del usuario su custodia.
- Cuando el usuario de la cuenta de correo electrónico se ausenta de la Corporación por motivos de vacaciones, licencias, permisos, entre otros, deberá informar a la Subdirección de Planeación con el fin que la cuenta sea bloqueada por el tiempo necesario.
- La cuenta de correo electrónico asignada no debe ser usada para el envío o distribución de mensajes con contenido considerado difamatorio, sexual, matoneo o que pueda ofender a alguien.

- Los servidores públicos, contratistas o colaboradores no deben hacer uso de la navegación para participar en discusiones, chats, páginas sociales, foros, entre otros, a menos que su participación sea de carácter oficial y tenga relación con las funciones que desempeña.
- Está prohibido descargar archivos que puedan ser perjudiciales para la infraestructura tecnológica de la Corporación, como: programas maliciosos, virus, software espía o desconocido que ponga en riesgo la seguridad de la información.
- Cualquier sistema de la Corporación debe contar con la definición de perfiles de usuario de acuerdo con la función del usuario que deba acceder a él.
- Cualquier tipo de desarrollo o adquisición de software deberá tener definidas las especificaciones de seguridad por parte de la Subdirección de Planeación.
- Está prohibido el uso de los equipos de propiedad de la Corporación para actividades de lucro, como: compra o venta de productos, negocios privados, juegos de azar, trabajos de consultoría, entre otros.
- En caso de presentarse alguna falla física o lógica en cualquier equipo (computadores o accesorios) de propiedad de la Corporación, éste deberá ser informado a la Oficina de Sistemas.
- La conexión entre sistemas internos de la Corporación y de terceros deberá ser autorizada por la Subdirección de Planeación.
- Cualquier alteración en el tráfico de la red, será motivo de verificación.
- El acceso a configuración de los sistemas operativos estará a cargo únicamente de la Subdirección de Planeación y por las personas autorizadas para esta tarea.
- El mantenimiento de las aplicaciones y software de sistemas estará a cargo exclusivamente de la Subdirección de Planeación y del personal autorizado que se disponga para esta tarea.
- La Oficina de Sistemas hará monitoreo del uso de internet, con el fin de garantizar la correcta utilización del servicio.

POLÍTICA 3: SEGURIDAD DE USUARIOS

- Cuando se haga entrega de equipo, este debe ir acompañado de la hoja de vida, en la cual se detalla la ubicación, configuración, programas y aplicativos que contiene, a partir de ese momento es de responsabilidad y cuidado del usuario al cual le fue asignado, el cual deberá ser devuelto (por motivos de: desvinculación, terminación o traslado) en las condiciones entregadas, salvo el desgaste normal del equipo.
- Al finalizar la jornada de trabajo, todo servidor público, contratista o colaborador debe cerrar sesiones abiertas de aplicaciones y apagar el computador o elemento que esté utilizando, a menos que por algún proceso especial, este deba permanecer encendido.
- Imprimir en lo posible por ambas caras de la hoja a menos que el documento deba ser impreso de otra forma.
- Los escritorios o zonas de trabajo deben permanecer en orden y estar limpios, con el fin de proteger los elementos de tecnología que estén cerca (documentos en papel, memorias USB, CD´s, entre otros).
- En caso que el servidor público, contratista o colaborador deba retirarse por un tiempo considerable de su escritorio, deberá bloquear la pantalla del computador o equipo que esté manipulando, con el fin de reducir el riesgo de accesos no autorizados, pérdida o daño de información.

- Al finalizar la jornada de trabajo, todo servidor público, contratista o colaborador deberá recoger y asegurar todo material sensible de su lugar de labor.
- Todo servidor público, contratista o colaborador de la Corporación que tenga una cuenta de usuario activa (correo electrónico, de acceso al dominio, a los aplicativos, entre otros), deberá establecer una contraseña segura de acuerdo a las indicaciones del personal del proceso de Tecnologías de la Información y las Comunicaciones.
- Las contraseñas deben cambiarse periódicamente, en un plazo no mayor a 60 días.
- No se almacenarán las contraseñas en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y estar resguardado.
- Se evitará activar o hacer uso de la utilidad de: “Recordar Contraseña” o “Recordar Password” de las aplicaciones.

Criterios en la construcción de contraseñas seguras:

- La longitud debe ser al menos de 8 caracteres.
- Contener caracteres tanto en mayúsculas como en minúsculas.
- Puede tener dígitos y caracteres especiales como _, -, /, *, $, ¡, ¿, =, +, entre otros.
- No debe ser una palabra por sí sola, en ningún lenguaje, dialecto o jerga
- No debe ser basada en información personal, nombres de familia, fechas de cumpleaños, entre otros.
- Procurar no construir contraseñas que sean fáciles de recordar o deducir, como: cumpleaños, aniversarios, información personal, teléfonos, códigos postales, etc.
- No usar patrones como 1234?, aaabbb, qwerty, zyxwvuts, entre otros.

POLÍTICA 4: AUDITORÍA DE SEGURIDAD

- Todos los archivos de auditoría deben proporcionar la suficiente información con el fin de realizar monitoreo, control y seguimiento.
- Todos los equipos de propiedad de la Corporación deben contar con la fecha y hora exactas para que el registro de los archivos de auditoría sea el correcto.
- Todos los sistemas que operen y administren información sensible o crítica deben generar pistas de auditoría, ya sea de modificación, adición o borrado.
- Todos los archivos de auditorías de los diferentes sistemas de información deben guardarse según su criticidad de acuerdo a la clasificación de activos realizada por cada proceso y ser custodiados en forma segura por personas autorizadas.
- Cualquier auditoría de seguridad a los sistemas de la Corporación debe estar debidamente autorizada y aprobada por la Subdirección de Planeación, con visto bueno del Director.
- Las auditorías de seguridad de la información deben ser realizadas por personal preparado técnicamente, en caso de no existir, el personal asignado debe ser capacitado adecuadamente.

POLÍTICA 5: ASPECTOS LEGALES

- Las obligaciones relacionadas con el licenciamiento de software son responsabilidad de la Subdirección de Planeación.
- Todo software desarrollado internamente, por personal que labora para la Corporación, es de propiedad exclusiva de la Entidad.

- Cuando se contrate el desarrollo de alguna aplicación software, deberá especificarse el nivel de prestación del servicio, las medidas de seguridad y el personal involucrado en el proceso.
- Toda adquisición de software se hará dentro de los parámetros que indica la ley, en ningún momento se obtendrá software de forma fraudulenta.
- El software licenciado a la Corporación, es de propiedad exclusiva de la Corporación, por lo mismo no hará reproducción sin el permiso de sus autores.
- Todo servidor público, contratista o colaborador es responsable de la legalidad del software instalado en su equipo personal.
- Es responsabilidad del Proceso de Tecnologías de la Información y Comunicaciones evaluar, actualizar, verificar y socializar las políticas de seguridad informática, conforme a esto, el presente documento tendrá una revisión periódica, la cual se hará como mínimo cada año de forma planeada o antes en caso de ser necesario y en caso de detectar algún incumplimiento, deberá reportarlo a la Secretaría General.
- La Corporación debe respetar las normas relacionadas con propiedad intelectual y derechos de autor.