MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE CONTROL DE ACCESOS

OFICINA ASESORA DE DIRECCIONAMIENTO ESTRATEGICO TIC

SEGURIDAD DE LA INFORMACIÓN

Ibagué – Colombia

Diciembre 1 de 2023

INDICE DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVOS 5
2.1 GENERAL 5
2.2 OBJETIVOS ESPECÍFICOS 5
3. ALCANCE Y ÁMBITO DE APLICACIÓN 6
4. NORMATIVIDAD 7
5. DEFINICIONES Y TÉRMINOS 8
6. DESCRIPCIÓN DE LA POLÍTICA 9
6.1 LINEAMIENTOS GENERALES DE CONTROL DE ACCESO A LA INFORMACION Y SU PLATAFORMA TECNOLOGICA 9
6.2 RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN 10
6.3 RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN 14
6.4 ACCESO A REDES Y A SERVICIOS DE RED 14
6.4.1 UTILIZACIÓN DE LOS SERVICIOS DE RED 15
6.4.2 ACCESO A INTERNET 16
6.4.3 CONTROL DE ACCESO AL SISTEMA OPERATIVO 16
6.5 GESTIÓN DE ACCESOS DE USUARIOS 17
6.5.1 REGISTRO Y CANCELACIÓN DE REGISTRO DE USUARIOS 17
6.5.2 GESTIÓN DE PRIVILEGIOS 18
6.5.3 GESTIÓN DE CLAVES DE USUARIO 18
6.5.4 GESTIÓN DE CLAVES CRÍTICAS 19
6.5.5 REVISIÓN DE DERECHOS DE ACCESO DE USUARIOS 20
6.6 RESPONSABILIDAD DEL USUARIO 20
6.7 USO DE CONTROLES DE AUTENTICACIÓN 21
6.8 CONTROL DE ACCESO AL SISTEMA Y LAS APLICACIONES 22
6.8.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN 22
6.8.2 INGRESO SEGURO A SISTEMAS Y APLICACIONES 22
6.8.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS 23

6.8.4 USO DE UTILITARIOS DE SISTEMA 23
6.8.5 CONTROL DE ACCESO AL CÓDIGO FUENTE 24
6.9 MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS 24
7. RESPONSABLES 25
8 SANCIONES 25
9 REFERENCIAS 26
10.APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS 26
11. CONTROL DE CAMBIOS 27

1. INTRODUCCIÓN

El presente documento establece las políticas y normas para garantizar un adecuado control de acceso a la infraestructura de TI, servicios de red e internet, los sistemas de información y los servicios y plataformas de la **CORPORACION AUTONOMA REGIONAL DEL TOLIMA - CORTOLIMA**.

Para **CORTOLIMA** dentro de sus procesos de mejoramiento y aseguramiento de la Seguridad y Privacidad de la Información, es importante definir los parámetros que se tendrá por parte de sus funcionarios, contratistas y visitantes para el acceso principalmente a la Infraestructura de TI, acceso a los equipos de cómputo, servicios de red e internet, sistemas de información, plataformas, programas y aplicaciones que hacen parte de los activos de la información de forma segura; por lo cual limita el acceso de usuarios de aplicaciones tecnológicas únicamente a los funcionarios, contratistas y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones dentro de las instalaciones de **CORTOLIMA** dispuestas en su sede central y las oficinas territoriales y demás espacios dispuestos para el servicio y operación de sus actividades y misionales.

En tal sentido, se hace necesario controlar y restringir el acceso a toda la información indistinto si se encuentra en la infraestructura de red, medios físicos y/o digitales; garantizando así la confidencialidad e integridad de ésta.

2. OBJETIVOS

2.1 GENERAL

Garantizar que la información, las áreas de procesamiento de información, la infraestructura de redes de datos e internet, los recursos de las plataformas tecnológicas, los programas, aplicaciones y los sistemas de información de la CORPORACION AUTONOMA REGIONAL DEL TOLIMA – CORTOLIMA se encuentren debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

2.2 OBJETIVOS ESPECÍFICOS

● Impedir el acceso no autorizado a los sistemas de información, bases de datos, información almacenada en los equipos de cómputo, sistemas de gestión documental, unidades de almacenamiento en red y servicios de información.

● Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización; mediante políticas claras para la asignación, mantenimiento, cambio y actualización en las contraseñas e identificaciones de los dispositivos y usuarios por parte de los funcionarios, contratistas y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades dentro de la infraestructura de TI de **CORTOLIMA**.

● Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas y de la información.

● Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de claves y cambios de las mismas, equipos de cómputo e información; así como la responsabilidad que presupone el hecho de compartir dichas claves o el intento de acceder o apoderarse de contraseñas de otros usuarios para beneficios propios o personales.

● Garantizar la seguridad de la información cuando se utiliza computación móvil, redes inalámbricas y/o trabajo remoto en caso de ser estrictamente necesario.

● Controlar el acceso a las infraestructura de red, redes inalámbricas, accesos remotos y acceso a las diferentes plataformas de CORTOLIMA, garantizando la seguridad de la información por parte de los empleados públicos de la Corporación.

3. ALCANCE Y ÁMBITO DE APLICACIÓN

El presente documento tiene aplicabilidad a todas las formas de acceso de todos los funcionarios, contratistas o terceros a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos, documentación, programas o servicios de información y redes de datos de **CORTOLIMA**.

4. NORMATIVIDAD

NORMA	AÑO	DESCRIPCIÓN
Ley 594	2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones
Ley 1712	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Ley 1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
Decreto 1727	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.
Ley 734	2002	Por la cual se expide el Código Disciplinario Único
Decreto 1078	2015	Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones
Ley 2052	2020	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones
Decreto 088	2022	Conceptos, lineamientos, plazos y condiciones técnicas transversales para la digitalización y automatización de trámites y su realización en línea
Decreto 767	2022	Establece los lineamientos generales de la Política de Gobierno Digital, entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones

5. DEFINICIONES Y TÉRMINOS

Activo: Cualquier cosa que tenga valor para la organización. (ISO/IEC 13335-1:2004).

Activos de Información: Es todo aquello que contiene, procesa, trate y/o manipule información valiosa para la Corporación y que son necesarios para que la Corporación funcione y cumpla con los objetivos establecidos para dicho fin.

Acceso: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la CORPORACION AUTONOMA REGIONAL DEL TOLIMA – CORTOLIMA en un momento dado.

Acceso Físico: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio de la Corporación.

Acceso lógico: En general, el acceso lógico es un acceso electrónico o digital o intento de acceder a archivos, navegar en el servidor, enviar un correo electrónico, apoderarse de las credenciales, usuarios o contraseñas de otros usuarios, transferir archivos, acceder a información que no se tenga permisos concedidos o adquirir permisos no asignados por cualquier medio.

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Corporación. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Propietario de la Información: Es una parte designada de **CORTOLIMA**, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información sea clasificada adecuadamente y mantenga una clasificación acorde con su nivel de confidencialidad.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo y consignarlos en la matriz de riesgo de seguridad de la información.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Incidente: Cualquier evento que no forma parte de una operación normal de un servicio y que causa o puede causar una interrupción o reducción de la calidad del servicio.

6. DESCRIPCIÓN DE LA POLÍTICA

La **CORPORACION AUTONOMA REGIONAL DEL TOLIMA – CORTOLIMA** debe establecer las medidas de control de acceso a toda la información física (dentro de la infraestructura de TI de la Corporación) o virtual de propiedad de la Corporación; sin importar el medio en el que se almacene, procese, utilice, transmita mediante espacios públicos y privados, redes, sistemas operativos, aplicaciones, sistemas de información; servicios de TI, entre otros en la sede principal, oficinas territoriales y cualquier espacio que utilice la Corporación para el cumplimiento de sus objetivos misionales.

Los controles de acceso deben ser idóneos y robustos, con el fin de impedir el acceso no autorizado a los activos de información de la Corporación. Éstos deben ser conocidos por todos los funcionarios, colaboradores y terceras partes que cuentan con privilegios de acceso a la información de **CORTOLIMA** y deben controlar los privilegios sobre los activos de información de acuerdo con lo permitido y según lo estrictamente necesario para el desempeño de su función.

Se deben implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, bases de datos y servicios, estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

6.1 LINEAMIENTOS GENERALES DE CONTROL DE ACCESO A LA INFORMACION Y SU PLATAFORMA TECNOLOGICA

La Oficina Asesora de Direccionamiento Estratégico TIC tiene dentro de su propósito da definición la definición de lineamientos, normas y procedimientos para la gestión de accesos a todos los sistemas, bases de datos y servicios de información, el monitoreo del uso de las instalaciones de procesamiento de la información, el uso de dispositivos móviles, reportes de incidentes relacionados, la revisión de registros de actividades y el ajuste de relojes de acuerdo con un estándar preestablecido.

Adicionalmente, es responsable de:

● Establecer los mecanismos de control de acceso necesarios con base a los requisitos de seguridad de la información y de los requisitos propios de la Corporación.

● Definir, implementar y monitorear los controles de acceso adecuados para proteger la información y las instalaciones en donde se procesa, almacena, trata y se transmite.

● Analizar y realizar seguimiento permanente de las medidas de control de acceso utilizadas, verificando su eficiencia y efectividad.

● Permitir el acceso a los activos de información y a los servicios y recursos tecnológicos provistos por la **CORPORACION AUTONOMA REGIONAL DEL TOLIMA – CORTOLIMA** únicamente a los usuarios que hayan sido permitidos específicamente y de acuerdo con el propósito de sus funciones y responsabilidades, verificando los privilegios otorgados sobre los activos de información.

● Se debe realizar la asignación del menor privilegio frente a los activos de información de la Corporación. Los mismos deben ser otorgados únicamente por el tiempo que sea necesario para la ejecución de las funciones y actividades propias del rol, controlando su proceso de asignación, modificación, cancelación, desactivación y/o eliminación mediante comunicaciones internas desde la Oficina de Talento Humano y acorde a las solicitudes realizadas por subdirectores, jefes de oficinas asesoras y coordinadores de grupo.

● Realizar el registro de las actividades relacionadas con el acceso a los activos de información de la Corporación, realizando auditorías continuas sobre los mismos y verificando el cumplimiento de los lineamientos y ejecución efectiva de los procedimientos asociados.

● Verificar el cumplimiento de los lineamientos establecidos, relacionados con control de accesos, registro de usuarios, administración de privilegios, administración de claves, utilización de servicios de red, uso controlado de utilitarios del sistema, registro de eventos, protección de puertos.

6.2 RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

La **Oficina Asesora de Direccionamiento Estratégico TIC** con fundamente en el acuerdo 014 está a cargo de definir normas y procedimientos para la gestión de accesos a todos los activos de información, así como de las instalaciones en donde se procesa o almacena información confidencial. Los accesos y privilegios deben ser limitados únicamente a personas autorizadas y se considera acceso no autorizado el intento o apropiación de cualquier información que no tenga competencia con las actividades o responsabilidades del cargo y funciones asignadas al funcionario, contratista y/o cualquier persona externa o interna de la **CORPORACION**.

De acuerdo a esto la **Oficina Asesora de Direccionamiento Estratégico TIC** define los siguientes lineamientos generales para el uso del hardware y software la Corporación:

- ✓ Todos los equipos de computo y dispositivos en general que son de propiedad de la Corporación deben ingresarse al Dominio del directorio Activo implementado: **Cortoli1.local**
- ✓ Todos los equipos de cómputo y dispositivos en general pertenecientes a contratistas, practicantes, personal de convenios y terceros que tengan dentro de sus funciones interacción directa con la infraestructura de TI y requieran acceso a los sistemas de información de desarrollos propios de la Corporación que así lo requieran, deben ingresarse al dominio del directorio Activo implementado: **Cortoli1.local**
- ✓ Todos los equipos de cómputo y dispositivos en general pertenecientes a contratistas, practicantes, personal de convenios y terceros que dentro de sus funciones requieran acceso a los sistemas de información de desarrollos web propios de la Corporación y externos, deben identificarse con la estructura de nombres definida por la **Oficina Asesora de Direccionamiento Estratégico TIC** determinándose la estructura de la Subdirección y/o Oficina Asesora o de Apoyo, el área al cual pertenece y el proceso sobre el cual desarrolla funciones; anteponiendo a la estructura la letra C, que lo identifica como contratista o de acuerdo al proyecto o convenio al que pertenezca (Por ejemplo: UT); sobre las cuales se definirán unos controles sobre el uso de los servicios hacia internet y hacia la Corporación, limitándose su uso a los servicios propios que requiera, previa solicitud por su supervisor, jefe de oficina, coordinador de grupo de proceso y/o subdirector de alguno de los procesos misionales de la Corporación al cual pertenece
- ✓ Todos los equipos de computo y dispositivos en general que pertenezcan al domino de la Corporación, deberán contar con los programas y aplicaciones licenciadas y de uso libre definidos de acuerdo a su función y previa solicitud por su supervisor, jefe de oficina, coordinador de grupo de proceso y/o subdirector de alguno de los procesos misionales de la Corporación al cual pertenece
- ✓ Todos los equipos de cómputo y dispositivos en general que pertenezcan al domino de la Corporación, deberán contar con el programa de antivirus definido por la **Oficina Asesora de Direccionamiento Estratégico TIC** y aquellos NO SON de propiedad de la Corporación; la Procedimiento de Gestión de soporte TIC de la Subdirección Administrativa y Financiera deberá verificar al momento de identificar lo equipos que tenga un antivirus instalado o en su defecto habilitar el antivirus propietario de Microsoft Windows o acorde al Sistema Operativo instalado
- ✓ La Oficina **Asesora de Direccionamiento Estratégico TIC** bajo solicitud previa de supervisores, jefes de oficina, coordinadores de grupo de proceso y/o subdirector de alguno de los procesos misionales de la Corporación; evaluará las solicitudes de software requeridos por cada uno de los procesos al cual pertenece y verificará su

pertinencia y realizará la gestión necesaria para su adquisición o evaluación de herramientas de distribución libre que brinden funcionalidades similares a aquellas del software solicitado

- ✓ Ningún funcionario, contratista, subdirector, practicante, jefe de oficina, coordinador de grupo de proceso, personal externo que tenga algún tipo de convenio o vinculación con la Corporación y/o visitantes podrán ingresar equipos de cómputo, routers, módems, dispositivos de almacenamiento en red (NAS), equipos multimedia, dispositivos de red y comunicaciones y cualquier hardware sin la aprobación por parte de La **Oficina Asesora de Direccionamiento Estratégico TIC;** dicha revisión deberá ser controlada y registrada por la oficina de gestión administrativa en los ingresos dispuestos por la Corporación; asís como su registro e identificación acorde a los presentes lineamientos y por requerimiento de sus funciones en la Corporación en el formato creado para tal fin
- ✓ Ningún funcionario, contratista, subdirector, practicante, jefe de oficina, coordinador de grupo de proceso, personal externo que tenga algún tipo de convenio o vinculación con la Corporación y/o visitantes podrán compartir servicios de conectividad con sus dispositivos móviles con otros equipos de cómputo dentro de las instalaciones de la Corporación y bajo supervisión de la Procedimiento de Gestión de soporte TIC de la Subdirección Administrativa y Financiera de la Corporación
- ✓ Cuando se requieran uso de algún hardware y software específico por personal externo que vaya a participar en alguna conferencia, reunión, exposición o cualquier evento programado por la Corporación deberá ser verificado y registrado al ingreso por la oficina de Gestión Administrativa en los ingresos dispuestos por la Corporación y se debe verificar que tengan antivirus plenamente identificado y/o habilitado; teniendo en cuenta licenciamiento de software, programas y aplicaciones de tipo malicioso; así como su registro e identificación acorde a los presentes lineamientos en el formato creado para tal fin
- ✓ Ningún funcionario, contratista, subdirector, practicante, jefe de oficina, coordinador de grupo de proceso, personal externo que tenga algún tipo de convenio o vinculación con la Corporación y/o visitantes podrá realizar ningún tipo de conexión en los puntos de red de la infraestructura de conectividad de la Corporación que no pertenezcan a su oficina, área, subdirección y que estén plenamente identificado acorde a los lineamientos indicados en la presente política; dadas las configuraciones, controles, restricciones y demás elementos de seguridad previamente definidos y aprobados por la **Oficina Asesora de Direccionamiento Estratégico TIC** y con base a las características definidas

Además, la **Oficina Asesora de Direccionamiento Estratégico TIC** cuenta con un profesional de la seguridad y privacidad de la información, quien es responsable de:

- ✓ Verificar la asignación y/o actualización de privilegios a usuarios por parte de la persona asignada por la jefe de la Oficina Asesora de Direccionamiento Estratégico TIC.
- ✓ Analizar y sugerir medidas a ser implementadas para que el control de acceso a los activos de información y servicios de la Corporación, así como verificar su cumplimiento y su efectividad.
- ✓ Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de claves, utilización de servicios de red, uso controlado de utilitarios del sistema, registro de eventos, verificación de que se ejecuten los procesos de auditoría.
- ✓ Apoyar a los usuarios sobre el uso apropiado de claves y de equipos de trabajo.
- ✓ Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- ✓ Acceder a los registros de auditoría a fin de realizar el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.
- ✓ Controlar los accesos a los servidores, unidades de almacenamiento en red, dispositivos de red y telecomunicaciones, equipos de computo y demás elementos de la infraestructura tecnología
- ✓ Controlar el acceso a los datacenters y espacios de distribución de los servicios de red (racks y cuartos de telecomunicaciones)
- ✓ Realizar los análisis de vulnerabilidades a nivel de toda la infraestructura de TI, servidores, datacenters, servicios, sistemas de información y generar los informes que se requieran con el ánimo de velar Controlar el acceso a los datacenters y espacios de distribución de los servicios de red (racks y cuartos de telecomunicaciones)

6.3 RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

Los propietarios de los activos de información deben determinar las normas de control de acceso y la asignación de los privilegios sobre ésta, de acuerdo con la política de seguridad de la información y el análisis de riesgos. Así mismo, son los responsables de:

● Identificar toda la información que corresponda a su área de responsabilidad cualquiera que sea su forma y medio de conservación; así como su respaldo en los recursos definidos por la **CORPORACION** para dicho fin.

● Clasificar todos los datos de su propiedad de acuerdo con el grado de criticidad de éstos y mantener un registro actualizado de la información más sensible.

● Autorizar el acceso sobre sus activos de información a colaboradores, contratistas o terceros de la Corporación, de acuerdo con sus respectivas funciones.

● Aprobar y solicitar la asignación de privilegios sobre la información a los diferentes usuarios, ya sea en situaciones rutinarias como excepcionales a modo propio o para aquellos funcionarios, contratistas y personas externas o internas de la **CORPORACION** que deban tener acceso dicha información bajo su dependencia o supervisión contractual.

6.4 ACCESO A REDES Y A SERVICIOS DE RED

El acceso a los activos de información y a los servicios y recursos tecnológicos provistos por la **CORPORACION AUTONOMA REGIONAL DEL TOLIMA – CORTOLIMA** debe ser otorgado únicamente a los usuarios que hayan sido permitidos específicamente y según a sus funciones y responsabilidades. Así mismo, se deberán realizar las comunicaciones por parte de la coordinación de talento humano, subdirectores, jefes de oficina, coordinadores de grupo de las diferentes dependencias sobre los funcionarios, contratistas y el personal externo o interno que ingresa, sale a periodo de vacaciones o termina su contratación, convenio o acuerdo con la **CORPORACION**, liberándose todas las asignaciones, permisos, contraseñas y accesos concedidos.

Dentro de las responsabilidades del coordinador de la Oficina de Talento Humano, subdirectores, supervisores, jefes de oficina y coordinadores de grupo están las de informar a la Oficina Asesora de Direccionamiento Estratégico TIC las situaciones administrativas – novedades que se presenten con los empleados públicos de la Corporación una vez el personal que termina su vinculación con la CORPORACIÓN, se traslada para otra oficina o

cualquier novedad que afecte su vinculación, para su correspondiente eliminación de permisos y accesos; así mismo, el subdirector, jefe de oficina, encargado de proceso o supervisor debe solicitar la asignación de los accesos y permisos a las distintas aplicaciones y sistemas de información para el desarrollo de las funciones u obligaciones contractuales en el momento de la contratación o traslados entre oficinas de los funcionarios, contratistas y personas externas (convenios) que así lo requieran, mediante el procedimiento de solicitud en la mesa de ayuda de las persona que tengan a cargo.

6.4.1 UTILIZACIÓN DE LOS SERVICIOS DE RED

Las conexiones no seguras a los servicios de red pueden afectar a la Corporación, por lo tanto, se debe controlar el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de éstos.

El profesional universitario de la Oficina Asesora de Direccionamiento Estratégico TIC encargado de la seguridad y privacidad de la información, tendrá a cargo otorgar el acceso y los privilegios sobre los servicios, aplicaciones, sistemas de información y recursos de red y las siguientes responsabilidades:

● Identificar las redes y servicios de red a los cuales se permite el acceso.

● Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

● Establecer controles y procedimientos de gestión para proteger el acceso a la información y a los servicios de red.

● Establecer controles para la identificación y autenticación de los usuarios otorgados a terceros a las redes o recursos de red de la Corporación, previa solicitud y aprobación por la oficina que lo requiera.

● Establecer los mecanismos necesarios para realizar conexiones seguras a los servicios de red y a la información, desde cualquier lugar y/u origen, lo cual incluye accesos remotos para los funcionarios que por su labor así lo requieran. Los accesos deben ser aprobados, registrados y auditados.

● Verificar que los funcionarios y terceros que requieran acceder a los activos de información a través de sus equipos personales cumplan con todos los requisitos o controles para registrarse y/o autenticarse y únicamente podrán realizar las funciones para las que fueron autorizados.

● Verificar que todos los funcionarios y terceras partes jurídicas o naturales cumplan las políticas de seguridad y privacidad de la Información y firmar todos los acuerdos y cláusulas estipuladas para tener acceso a los sistemas de información de la Corporación.

Los privilegios para el acceso a la red serán otorgados por el profesional universitario de la Oficina Asesora de Direccionamiento Estratégico TIC o quien haga sus veces, únicamente a través de la solicitud formal del responsable del área correspondiente del personal a su cargo y para cumplimiento de las funciones asignadas. Para ello, se debe seguir el procedimiento definido para la activación y desactivación de derechos de acceso a las redes y servicios de información mediante el formulario destinado para tal fin.

6.4.2 ACCESO A INTERNET

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. Los accesos serán autorizados formalmente por jefe del área correspondiente y a cargo del personal que lo solicite. Así mismo, se debe dar un uso adecuado y racional por parte de los funcionarios, contratistas y personal interno o externo que desarrollo funciones dentro de la Corporación y sus territoriales y centros de atención.

Para el acceso a puntos de red sobre los puestos de trabajo y la infraestructura de red inalámbrica se organizará de acuerdo a la estructura orgánica de la Corporación teniendo en cuenta subdirecciones, oficinas asesoras, oficinas, coordinaciones y áreas internas, acorde a la vinculación para funcionarios y contratistas, con las restricciones respectivas.

6.4.3 CONTROL DE ACCESO AL SISTEMA OPERATIVO

Todos los usuarios tendrán un identificador único (ID de usuario) solamente para su uso personal y exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no deben indicar ningún indicio del nivel de privilegio otorgado, sino debe estar bajo la estructura definida por la Oficina de direccionamiento Estratégico TIC.

En circunstancias excepcionales, cuando existe un claro beneficio para la Corporación y/o dadas las características de las funciones de los Subdirectores de Área, Coordinadores o Jefes de Oficina, podrá utilizarse un código de usuario compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se debe documentar la justificación y aprobación del propietario de la Información de que se trate; teniendo en cuenta que dicha autorización no lo exime de las responsabilidades que puedan derivarse por el mal uso que le puedan dar las personas a las que se le asigne.

Se implementará un método de autenticación unificado con el ánimo de simplificar la asignación de contraseñas en los diferentes dispositivos, sistemas y plataformas de la **CORPORACION**. deberá implementarse un procedimiento que incluya:

- ✓ Asignar la herramienta de autenticación.
- ✓ Registrar los usuarios autorizados.
- ✓ Revocar códigos de acceso al momento de la desvinculación de los colaboradores, contratistas o terceros.
- ✓ Revocar códigos de acceso, en caso de compromiso de seguridad.

6.5 GESTIÓN DE ACCESOS DE USUARIOS

La Corporación por medio de la Oficina Asesora de Direccionamiento Estratégico TIC debe implementar controles y procedimientos formales con el objeto de impedir el acceso no autorizado a la información y de garantizar la confidencialidad, disponibilidad e integridad de la información; y establecerá la asignación de derechos de acceso a los sistemas, a las redes de datos, los recursos tecnológicos y los servicios de información.

Así mismo, velará porque los funcionarios, contratistas, terceras partes, y todo aquella persona natural o jurídica que tenga interacción con la información de la Corporación, tengan acceso únicamente a la información necesaria para el desarrollo de sus funciones y la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

6.5.1 REGISTRO Y CANCELACIÓN DE REGISTRO DE USUARIOS

● La Oficina Asesora de Direccionamiento Estratégico TIC debe registrar todos los usuarios en el directorio activo de usuarios especificando y/o asociando el rol a desempeñar.

● La creación de un nuevo usuario solo será realizada después de la solicitud formal de acuerdo con los procedimientos establecidos, y bajo la solicitud y aprobación explícita del responsable del área, de lo contrario no se efectuará el trámite de dicha solicitud.

● Se deben utilizar métodos para proporcionar una id Corporación reconocible bajo códigos de identificación únicos, de manera que se puedan relacionar sus acciones y evitando la existencia de múltiples identificadores de acceso para un mismo empleado.

● Se debe verificar que el usuario tiene autorización del Propietario de la Información para el uso de la información, del sistema, base de datos o servicio de información.

● Se debe verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario.

● Se debe mantener un registro formal de todas las personas registradas para utilizar el servicio.

● Se debe cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron su rol y/o área o de aquellos a los que se les revocó la autorización, se desvincularon de la Corporación o sufrieron la pérdida/robo de sus credenciales de acceso, dadas las novedades administrativas reportadas por la oficina de talento humano, y se deberán solicitar nuevamente los permisos para el caso de los traslados de los funcionarios a otra oficina.

6.5.2 GESTIÓN DE PRIVILEGIOS

● Se debe identificar, limitar y controlar la asignación y el uso de los accesos privilegiados de cada sistema, proceso o servicio, siendo la Oficina Asesora de Direccionamiento Estratégico TIC la responsable de realizarlo.

● Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación.

6.5.3 GESTIÓN DE CLAVES DE USUARIO

La asignación de claves se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

● Incluir cláusulas en contratos y condiciones de puesto de trabajo sobre el mantenimiento de las credenciales de acceso y/o información de autenticación.

● Garantizar que los usuarios cambien las claves iniciales que les han sido asignadas la primera vez que ingresan al sistema.

● Generar claves temporales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la clave y los usuarios deben dar acuse de recibo cuando la reciban.

● No compartir las credenciales de acceso.

● Almacenar las claves sólo en sistemas informáticos protegidos.

● Configurar un estándar de claves de acceso.

● Cambiar las credenciales de acceso a los sistemas que han sido utilizados por personal externo, luego de realizar sus actividades.

● La Oficina Asesora de Direccionamiento Estratégico TIC deberá velar por la seguridad en el acceso a los servicios de red y sistemas y se encargará de implementar políticas y controles de autenticación requeridas para los diferentes servicios y plataformas que permitan garantizar la seguridad, confidencialidad y el acceso de los usuarios.

6.5.4 GESTIÓN DE CLAVES CRÍTICAS

En los diferentes ambientes de procesamiento existen códigos de usuarios con los cuales es posible efectuar actividades críticas como la instalación de plataformas o sistemas, habilitación de servicios, actualización de software y configuración de componentes informáticos. Dichas cuentas no serán de uso habitual, sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por claves con un mayor nivel de complejidad que el habitual.

Las cuentas con accesos privilegiados deben ser controladas y gestionadas a través de los mecanismos necesarios para garantizar el gobierno y protección sobre éstas y estarán bajo la responsabilidad de la Oficina Asesora de Direccionamiento Estratégico TIC y el profesional responsable del procedimiento de Gestión de Soporte de la Subdirección Administrativa y Financiera.

6.5.5 REVISIÓN DE DERECHOS DE ACCESO DE USUARIOS

El área de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad y Privacidad de la Información establecido en la Corporación debe efectuar un proceso formal de revisión, a intervalos regulares, a fin de verificar los derechos de acceso de los usuarios y de mantener un control eficaz del acceso a los datos y servicios de información. Para ello, la Corporación debe contemplar los controles necesarios, entre otros, los siguientes:

- ✓ Revisar los derechos de acceso de los usuarios a intervalos planificados y registrar los cambios que se realicen.
- ✓ Colocar límites de tiempo para los derechos de acceso con privilegios especiales.
- ✓ Revisar las asignaciones de privilegios a intervalos planificados, a fin de garantizar que no se obtengan privilegios no autorizados.
- ✓ Revisar los derechos de acceso a la terminación del contrato de los funcionarios o cambios dentro de la Corporación (cambios de funciones o promociones).

6.6 RESPONSABILIDAD DEL USUARIO

Los colaboradores, contratistas y terceros que hacen uso de los activos de información de la Corporación son responsables de las acciones que, realizadas sobre los mismos, así como de las credenciales de acceso que le son asignadas para su uso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad de la información, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el uso y ejecución de controles de acceso eficaces, en particular aquellos relacionados con el uso de credenciales y la seguridad de los equipos de cómputo y a la información.

Ningún colaborador debe compartir sus cuentas de usuario, contraseñas y/o factores de autenticación asignados para el ingreso a los servicios de red y sistemas de información con otros colaboradores, funcionarios o terceros.

Los funcionarios, colaboradores, contratistas y terceros que posean acceso a los activos de información de CORTOLIMA deben acogerse a las normas y mejores prácticas establecidas para la configuración de contraseñas asignadas por la Corporación.

Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por clave.

Todos los escritorios físicos y digitales deben permanecer despejados con el fin de reducir los riesgos de acceso no autorizado, pérdida o daño de la información durante la jornada laboral o fuera de ella.

6.7 USO DE CONTROLES DE AUTENTICACIÓN

Las claves constituyen un medio de validación y autenticación de la Corporación de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. En tal sentido la Corporación debe establecer e implementar las normas para el uso de las credenciales de acceso y los factores de autenticación proporcionados a los usuarios, teniendo en cuenta las mejores prácticas, entre las cuales se establecen las siguientes:

- ✓ Los usuarios de los diferentes sistemas de información de la Corporación deben seguir buenas prácticas de seguridad en la selección y uso de claves.
- ✓ Los usuarios con accesos a los activos de información deben mantener las claves en secreto, no divulgarlas ni compartirlas.
- ✓ Las contraseñas deben ser cambiadas cada vez que el sistema se lo solicite o siempre que exista un posible indicio de compromiso del sistema o de las claves. Así mismo, las claves temporales deben cambiarse en el primer inicio de sesión.
- ✓ Evitar registrar y/o almacenar las credenciales de acceso en cualquier tipo de elemento físico y/o digital.
- ✓ Las contraseñas utilizadas por los usuarios deben ser robustas con el fin de evitar que sean comprometidas fácilmente. Las mismas no deben estar basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, datos generales, o de la Corporación. Las mismas, no deben tener caracteres idénticos consecutivos o grupos totalmente numéricos o alfabéticos.
- ✓ Evitar incluir claves en los procesos automatizados especialmente en los relacionados con el inicio de sesión.
- ✓ Notificar cualquier incidente de seguridad relacionado con sus claves: pérdida, robo o indicio de pérdida de confidencialidad.

6.8 CONTROL DE ACCESO AL SISTEMA Y LAS APLICACIONES

6.8.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

La información es un activo de vital importancia para la Corporación. y como tal debe ser protegido y contar con los mecanismos de control de acceso más adecuados. El acceso a la información está dado directamente por medio de los programas o aplicativos que manejan los datos y que son operados directamente por los usuarios autorizados; o indirectamente por medio de programas utilitarios que son operados por personal de soporte. En cualquiera de los casos se deben consideren los diferentes controles de frente al acceso a la información:

- El acceso de los usuarios a los sistemas, a la información, a las aplicaciones, o a los recursos
- de la Corporación, debe ser limitado de acuerdo con sus responsabilidades y funciones.
- Existirán privilegios de acceso a la información, debidamente definidos por los propietarios de la información y estos privilegios deben usarse de una manera responsable por parte de los usuarios y no se debe realizar o intentar acceder a información para la cual no se está autorizado.
- Se debe controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
- Se deben considerar mecanismos de control de acceso físicos y lógicos adicionales para sistemas o información sensible.

6.8.2 INGRESO SEGURO A SISTEMAS Y APLICACIONES

La Corporación debe establecer los mecanismos para garantizar el acceso controlado y seguro a los sistemas, aplicaciones y activos de información de la Corporación. Así mismo, se debe propender por:

- El mecanismo de acceso debe de corroborar que corresponde a un usuario específico, por lo cual corrobora la id del usuario.
- Considerar autenticación sólida y robusta, a través del uso de otros factores de autenticación adicionales al usuario y contraseña, principalmente para los sistemas e información crítica.
- Evitar que cualquier información relacionada con el activo de información sea entregada al usuario que realiza el procedimiento de ingreso, sin que éste haya sido exitoso, y solo en caso de que sea absolutamente necesario hacerlo.

- Los mecanismos de acceso a los activos de información de la Corporación deben ser sometidos a pruebas periódicas de seguridad, con el propósito de identificar y gestionar los riesgos y vulnerabilidades asociados a dichos componentes.
- Realizar el registro de las actividades sobre los accesos a la información de la Corporación.
- La transmisión de las credenciales de acceso y de los mecanismos de autenticación debe realizarse mediante algoritmos de cifrado robustos y no vulnerables.
- Las sesiones inactivas deben ser finalizadas de forma automática por los sistemas y aplicaciones.
- El ingreso de autorizará por solicitud escrita del subdirector, jefe de oficina o coordinador del área en donde se desempeñará el funcionario de acuerdo a sus funciones u obligaciones contractuales; teniendo en cuenta el procedimiento de creación de usuarios definido.

6.8.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS

Las contraseñas constituyen uno de los principales medios de validación y autorización de permisos a un usuario para acceder a un servicio informático. Los sistemas de administración de credenciales deben constituir una herramienta eficaz e interactiva que garantice contraseñas robustas. El sistema de administración de credenciales debe:

- Imponer el uso de mecanismos de acceso individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas
- Imponer el uso de contraseñas robustas y rechazar contraseñas débiles.
- Obligar a los usuarios a cambiar las claves temporales en su primer procedimiento de autenticación.
- Evitar mostrar las claves en pantalla cuando son ingresadas.

6.8.4 USO DE UTILITARIOS DE SISTEMA

Los programas utilitarios que podrían tener la capacidad de pasar por alto las seguridades de los sistemas y aplicaciones, por lo cual su uso debe ser limitado y minuciosamente controlado. Se deben considerar los siguientes aspectos:

- Utilizar procedimientos de autenticación para utilitarios del sistema y programas con funciones administrativas.

- Separar los utilitarios de las aplicaciones del Sistema y segregar las funciones cuando sea posible.
- Limitar el uso de utilitarios del sistema únicamente a usuarios fiables y autorizados.
- Evitar que personas ajenas a la Corporación tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en los recursos informáticos.
- Solicitar la instalación únicamente de aplicaciones debidamente licenciadas o gratuitas.

6.8.5 CONTROL DE ACCESO AL CÓDIGO FUENTE

El código fuente de propiedad de la Corporación debe ser protegido frente al acceso no autorizado; para ello se debe:

- Establecer los controles para mantener registros de auditoría de los cambios realizados en el código fuente propietario de la Corporación.
- La Corporación debe tener ambientes de desarrollo apropiados y con todas las características de aseguramiento con el fin de proteger el ciclo de vida del software desde su inicio y en su etapa de operación y mantenimiento, para las aplicaciones propias.

6.9 MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS

Se deben generar registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad de acceso a las aplicaciones, programas e información. Los registros de auditoría deberán incluir como mínimo los siguientes datos:

- Identificación del usuario.
- Fecha y hora de inicio y terminación.
- Registros de intentos exitosos y fallidos de acceso al sistema.
- Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados.

7. RESPONSABLES

Comité institucional de gestión y desempeño: Aprobar las políticas y lineamientos definidos para garantizar la seguridad y privacidad de la información.

Director(a) General: Poner a disposición los recursos necesarios para el cumplimiento de los lineamientos descritos en la presente política.

Jefe de la Oficina Asesora de Direccionamiento Estratégico TIC: Diseñar e impartir las directrices, políticas y lineamientos para el cumplimiento de la presente política.

Coordinador(a) Oficina de Talento Humano: Deberá informar a la Jefe de la Oficina Asesora de Direccionamiento Estratégico TIC cuando finalice el contrato de cualquier miembro del personal de planta, contratista, practicante o convenios de la Corporación.

Coordinador Oficina de Gestión Administrativa: deberá informar a la Jefe de la Oficina Asesora de Direccionamiento Estratégico TIC cuando se requieran procesos o actividades dentro de la infraestructura para la instalación, configuración y adecuación de los equipos de cómputo de la Corporación de sus funcionarios y contratistas.

Subdirectores, Jefes de y Coordinadores de Grupo: Solicitar los permisos y accesos requeridos para cada uno de sus funcionarios así como su cancelación, descritos en la presente política.

Funcionarios, Contratistas, Pasantes y personal que accede a la Información: Evitar el acceso a las áreas seguras sin autorización, a excepción que sea en cumplimiento de sus obligaciones con la Corporación.

Dar cumplimiento a esta política.

8 SANCIONES

El incumplimiento de la Política de Gestión de Activos de Información de la Corporación podrá constituir falta disciplinaria y será sancionada en el marco del Código Disciplinario Único – Ley 734 de 2002.

9 REFERENCIAS

- Ministerio de Tecnologías de la Información y las Comunicaciones, Modelo de Seguridad y Privacidad de la Información – 2016.
- International Organization for Standardization, ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems.
- Icontec Internacional Guía Técnica Colombiana NTC-ISO/IEC 27002, Técnicas de seguridad.
- Código de Práctica para controles de seguridad de la información - 2015.
- Cumplimiento de sus obligaciones con la Corporación.

Dar cumplimiento a esta política.

10.APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Oficina Asesora de Direccionamiento Estratégico TIC y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de la Corporación.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Mauricio Rodriguez Garcia Cargo: Profesional Universitario Oficina Asesora de Direccionamiento Estratégico TIC Fecha: 02-08-2023	Nombre: Gladys Katherinne Silva Garibello Cargo: Jefe Oficina Asesora de Direccionamiento Estratégico TIC Fecha: 03-08-2023	Comité Institucional de Gestión del desempeño Fecha: 03-08-2023

11. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN
1/12/2023	00	Se implementa Documento Estrategico

ELABORO	REVISO	APROBO
Katherine Silva Garibello	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño 01 de Diciembre de 2023