



POLITICA DE SEGURIDAD

ALCANCE DE LAS POLÍTICAS

Las políticas definidas en el presente documento aplican a todos los funcionarios públicos, contratistas y pasantes de la Corporación Para el Desarrollo Sostenible del Sur de la Amazonia - Corpoamazonia, personal temporal y otras personas relacionadas con terceras partes que utilicen recursos informáticos.

DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Certificado Digital: un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor

Cifrar: quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama "descodificar" o "descifrar". Los sistemas de ciframiento se llaman "sistemas criptográficos".

CORPOAMAZONIA: Corporación para el Desarrollo Sostenible del Sur de la Amazonia Colombiana

Criptografía de llave pública: es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Información: es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.

Política: son instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios de CORPOAMAZONIA, pero que por las actividades que realizan en la Entidad, deban tener acceso a Recursos Informáticos

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOA (PUTUMAYO)
TERRITORIALES: AMAZONAS: Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506



Sistema de información: Conjunto de elementos interactúan entre sí para procesar los datos y la información (incluyendo procesos manuales y automáticos) y distribuirla de la manera más adecuada posible en una determinada organización en función de sus objetivos

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

No repudio: este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

DESCRIPCIÓN DE LAS POLÍTICAS

POLÍTICA 1: ACCESO A LA INFORMACIÓN

- Todos los funcionarios públicos, contratistas, pasantes que laboran para CORPOAMAZONIA deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a CORPOAMAZONIA, la Secretaria General, Subdirectores, jefes de Oficina, responsable de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.
- El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.
- Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad.
- Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.
- Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad y con fundamento en el proceso de GESTION DE RECURSOS INFORMATICOS.
- Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

POLÍTICA 2: ADMINISTRACIÓN DE CAMBIOS

- Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOIA (PUTUMAYO)
TERRITORIALES: **AMAZONAS:** Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506



formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud.

- Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.
- Para la administración de cambios se efectuará el procedimiento correspondiente definido por el proceso de GESTION DE RECURSOS INFORMATICOS de CORPOAMAZONIA, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.
- Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.
- Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

POLÍTICA 3: SEGURIDAD DE LA INFORMACIÓN

- Los funcionarios públicos, contratistas, y pasantes de CORPOAMAZONIA son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.
- Los funcionarios públicos, contratistas, y pasantes no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.
- Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.
- Los funcionarios, contratistas y pasantes deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad, el buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario, contratistas y pasantes de CORPOAMAZONIA deben comprometerse a no utilizar, comercializar o divulgar los productos o a información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información está en la obligación de reportar el hecho al grupo de control interno disciplinario.
- Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOA (PUTUMAYO)
TERRITORIALES: **AMAZONAS:** Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506



POLÍTICA 4: SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS

- El sistema de correo electrónico, grupos de charla y utilidades asociadas de la entidad debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas y pasantes.
- La entidad se reserva el derecho de acceder y de velar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, el funcionario o contratista autorizará a la entidad para realizar las revisiones y/o auditorías respectivas directamente o a través de terceros.
- Los funcionarios públicos, contratistas y pasantes no deben utilizar versiones escaneadas de Firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico ó cualquier otro tipo de comunicación electrónica haya sido firmado por la persona que la envía.
- La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la entidad. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.
- Los funcionarios públicos, contratistas y pasantes que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.
- En cualquier momento que un trabajador publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la entidad.
- Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la oficina de informática, no utilizar el computador y desconectarlo de la red.
- El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de "no repudio".
- El Asesor de seguridad informática en conjunto con la oficina asesora de comunicaciones debe proveer material para recordar regularmente a los empleados, temporales y consultores acerca de sus obligaciones con respecto a la seguridad de los recursos informáticos.

POLÍTICA 5: SEGURIDAD EN RECURSOS INFORMÁTICOS

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

- Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOCHA (PUTUMAYO)
TERRITORIALES: **AMAZONAS:** Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56

Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95

Correo: correspondencia@corpoamazonia.gov.co

Línea de Atención al Cliente: 01 8000 930 506



frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

- Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el Administración de usuarios.
- Plan de auditoría: Hace referencia a las pistas o registros de los sucesos relativos a la operación.
- Las puertas traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.
- El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.
- Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, contratistas y pasantes de CORPOAMAZONIA son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.
- Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
- Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.
- Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.
- Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de ciframiento para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.
- Antes de que un nuevo sistema se desarrolle o se adquiera, los subdirectores, jefes de oficina, en conjunto con el asesor de seguridad informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.
- La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.
- Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

POLÍTICA 6: SEGURIDAD EN COMUNICACIONES

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOA (PUTUMAYO)
TERRITORIALES: **AMAZONAS:** Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506



- Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser considerados y tratados como información confidencial.
- La red de amplia cobertura geográfica a nivel nacional debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.
- Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la entidad, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de ciframiento y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.
- Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar de acuerdo con la política de Gobierno en Línea.
- Los computadores de CORPOAMAZONIA se conectarán de manera directa con computadores de entidades externas, conexiones seguras, previa autorización del área de informática.
- Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá estar cifrada.

POLITICA 7: SEGURIDAD PARA USUARIOS TERCEROS

- Los dueños de Recursos Informáticos que no sean propiedad de la entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento.
- Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de CORPOAMAZONIA para el funcionamiento de recursos que no sean propios de la entidad y que deban ubicarse en sus instalaciones, los recursos serán administrados por el área técnica de CORPOAMAZONIA.
- Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el Jefe inmediato o coordinador. En todo caso deberán firmar el acuerdo de buen uso de los Recursos Informáticos.
- Si se requiere un equipo con módem, este equipo no podrá en ningún momento estar conectado a la Red al mismo tiempo.
- La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por el Área de Informática con el fin de no comprometer la seguridad de la información interna de la entidad.
- Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Entidad.
- Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por la entidad. La

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOCA (PUTUMAYO)
TERRITORIALES: **AMAZONAS:** Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506



entidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La entidad se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la entidad.

POLÍTICA 8: SOFTWARE UTILIZADO

- Todo software que utilice CORPOAMAZONIA será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.
- Todo el software de manejo de datos que utilice CORPOAMAZONIA dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.
- Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios públicos, contratistas y pasantes de las implicaciones que tiene el instalar software ilegal en los computadores de CORPOAMAZONIA.
- Existirá un inventario de las licencias de software de CORPOAMAZONIA que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

POLÍTICA 9: ACTUALIZACIÓN DE HARDWARE

- Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.
- La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.
- Los equipos de microcomputadores (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador del área involucrada.

POLÍTICA 10: ALMACENAMIENTO Y RESPALDO

- La información que es soportada por la infraestructura de tecnología informática de CORPOAMAZONIA deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.
- Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.
- La entidad definirá la custodia de los respaldos de la información que se realizará externamente con una compañía especializada en este tema.
- El almacenamiento de la información deberá realizarse interna y/o externamente a la Entidad, esto de acuerdo con la importancia de la información para la operación de CORPOAMAZONIA.
- El área dueña de la información en conjunto con la oficina Informática definirá la estrategia a

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOCHA (PUTUMAYO)
TERRITORIALES: **AMAZONAS:** Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506



seguir para el respaldo de la información.

- Los funcionarios públicos son responsables de los respaldos de su información en los microcomputadores, siguiendo las indicaciones técnicas dictadas por la oficina de informática. La oficina de informática será la autorizada para realizar el seguimiento y control de esta política.

POLÍTICA 11: CONTINGENCIA

- La administración de la Entidad debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.
- Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la Entidad, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoría.
- Todos los archivos de auditorías deben proporcionar suficiente información para apoyar el monitoreo, control y auditorías.
- Todos los archivos de auditorías de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.
- Todos los archivos de auditorías deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.
- Todos los computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoría sea correcto.

POLÍTICA 13: SEGURIDAD FÍSICA

- La Entidad deberá contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las dependencias que la entidad considere críticas.
- Los visitantes de las oficinas de la entidad deben ser escoltados durante todo el tiempo por un empleado autorizado, asesor o contratista. Esto significa que se requiere de un escolta tan pronto como un visitante entra a un área y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta incluyendo clientes, antiguos empleados, miembros de la familia del trabajador.
- Siempre que un trabajador se dé cuenta que un visitante no escoltado se encuentra dentro de áreas restringidas de la entidad, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad del edificio.

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOA (PUTUMAYO)
TERRITORIALES: **AMAZONAS:** Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506



- Los centros de cómputo o áreas que la entidad considere críticas deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.
- Toda persona que se encuentre dentro de la entidad deberá portar su identificación en lugar visible.
- En los centros de cómputo o áreas que la entidad considere críticas deberán existir elementos de control de incendio, inundación y alarmas.
- Los centros de cómputo o áreas que la entidad considere críticas deberán estar demarcados con zonas de circulación y zonas restringidas
- Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.
- Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión del área de informática.
- Todos los visitantes deben mostrar identificación con fotografía y firmar antes de obtener el acceso a las áreas restringidas controladas por la entidad.
- Los equipos de microcomputadores (PCs, servidores ,equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.
- Los funcionarios públicos se comprometen a NO utilizar a la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que genere caídas de la energía.
- Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no están autorizados para utilizar los recursos informáticos de la entidad.

POLÍTICA 14: ESCRITORIOS LIMPIOS

- Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, USB memory key, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

POLÍTICA 15: ADMINISTRACIÓN DE LA SEGURIDAD

- La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.
- Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOA (PUTUMAYO)
TERRITORIALES: **AMAZONAS:** Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506



corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al Asesor de Seguridad Informática.

- Los funcionarios públicos, contratistas y pasantes de CORPOAMAZONIA que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los Recursos Computacionales. La implementación debe ser consistente con las prácticas establecidas por la oficina informática.
- El asesor de Seguridad Informática divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportara a la dirección General, los casos de incumplimiento con copia a las oficinas de control interno e informática

SEDE PRINCIPAL: Tel.: (8) 4 29 66 41 - 4 29 66 42 – 429 52 67, Fax: (8) 4 29 52 55 , MOCOA (PUTUMAYO)
TERRITORIALES: AMAZONAS: Tel.: (8) 5 92 50 64 - 5 92 76 19, Fax: (8) 5 92 50 65, **CAQUETÁ:** Tel.: (8) 4 35 18 70 - 4 35 74 56
Fax: (8) 4 35 68 84, **PUTUMAYO:** Telefax: (8) 4 29 63 95
Correo: correspondencia@corpoamazonia.gov.co
Línea de Atención al Cliente: 01 8000 930 506