

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

ALCANCE DE LAS POLÍTICAS

Las políticas definidas en el presente documento aplican a todos los funcionarios públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la Corporación Autónoma Regional del Atlántico – CRA.

DIVULGACION

Las políticas de seguridad de la información serán comunicadas y dadas a conocer a través de: Intranet. Socializadas cada vez que se genere el ingreso de un funcionario, contratistas y/o terceros al momento de solicitar la creación de usuario y asignación de contraseña para el acceso a los sistemas de información que posee la entidad.

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.

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".

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

Página 1 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

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

CRA: Corporación Autónoma Regional del Atlántico

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Información: Puede existir en muchas formas. 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.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Página 2 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

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.

Política: son instrucciones mandatorias que indican la intención de la Dirección General respecto a la operación de la organización.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Recurso: En informática, los recursos son las aplicaciones, herramientas, dispositivos (periféricos) y capacidades con los que cuenta una computadora.

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

Página 3 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

Página 4 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

DESCRIPCIÓN DE LAS POLITICAS

POLITICA 1: ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen o laboran para la CRA deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la CRA, la Dirección General o Subdirector de la Dependencia pertinente, será el responsable de solicitar la autorización al responsable de la Oficina de Sistemas para generar el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

El otorgamiento de acceso a la información esta regulado mediante las normas y procedimientos definidos para tal fin.

Todas las prerrogativas para el uso de los sistemas de información de la CRA deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la CRA.

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 CRA, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la CRA.

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 CRA, 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

Página 5 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

información se deberán documentar y realizar las acciones tendientes a su solución.

CONTROL DE ACCESO Estas políticas hace referencia a todas aquellas directrices mediante las cuales la CRA determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos; las políticas relacionadas con el control de acceso deben contemplar como mínimo:

- **Control de acceso con usuario y contraseña:** El profesional especializado de la Oficina de Sistemas, elaborará la política sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la entidad, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas, en cada una de las plataformas que corresponda. Es responsabilidad de los funcionarios de la oficina de sistemas de información, la creación de usuario y asignación de contraseña temporal a funcionarios, contratistas o terceros, se ha definido que el usuario esta definido por la inicial del primer nombre acompañado del primer apellido completo, en caso de existir homónimos se definirá el usuario al agregarle la inicial del segundo apellido, se debe estipular y resaltar que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La entidad ha establecido que por cada funcionario, contratista o tercero se debe tenerse un usuario y una contraseña para el acceso.
- **Suministro del control de acceso:** Los funcionarios de la oficina de sistemas de información determinará los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en

Página 6 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad.

- **Gestión de Contraseñas:** Esta política define los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad. Una vez creado el usuario será notificado a los funcionarios, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considerada como fuerte, gestión de cambio de contraseña, debe determinar que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura.
- **Perímetros de Seguridad:** La política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuales no, la política debe definir los responsables de autorizar o no ingresos a las áreas delimitadas como de acceso restringido.
- **Responsabilidad y Custodia de la información contenida en los equipos de la Entidad entregados a funcionario, contratistas y/o terceros:** En ocasión a la emergencia sanitaria es necesario implementar medidas para el uso adecuado del acceso a la información de la Entidad, en donde la Oficina de Sistemas de Información sinistrará a Recursos Físicos documento la **guía de uso de equipo en tiempos de aislamiento**.

POLITICA 2: ADMINISTRACION DE CAMBIOS

Página 7 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

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 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 la CRA, 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.

POLITICA 3: SEGURIDAD DE LA INFORMACION

Los funcionarios públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por

Página 8 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

la Corporación, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA, 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 públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA. 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 público, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA, 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 esta 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.

Página 9 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

POLITICA 4: SEGURIDAD PARA LOS SERVICIOS INFORMATICOS

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 Corporación se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA autorizará a la Corporación para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

Los funcionarios públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA, 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 firmada 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, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA, que hayan recibido aprobación para tener

Página 10 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

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" con el fin de que los usuarios eviten haber realizado alguna acción.

Los siguientes aspectos son tenidos en cuenta al momento de evidenciar una acción de no repudio, ya que fueron configuradas en los softwares que posee la entidad:

- **Trazabilidad:** La política hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
- **Retención:** La política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad.

Página 11 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

- **Auditoría:** La política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
- **Intercambio electrónico de información:** La política incluirá en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

Los funcionarios de la Oficina de Sistemas de Información deberán proveer material para recordar regularmente a los empleados, temporales y consultores acerca de sus obligaciones con respecto a la seguridad de los recursos informáticos.

POLITICA 5: SEGURIDAD EN RECURSOS INFORMATICOS

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

Administración de usuarios: Establece como deben ser utilizadas las claves de acceso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

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.

Página 12 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

Plan de auditoria: Hace referencia a las pistas o registros de los sucesos relativos a la operación

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.

El control de acceso a todos los sistemas de computación de la Corporación 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, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA, 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 el.

El nivel de superusuario de los sistemas críticos debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Página 13 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

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 y/o Coordinadores de oficina, en conjunto con el Responsable de Sistemas, 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.

POLITICA 6: SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.

La red de amplia cobertura geográfica a nivel **nacional e internacional** 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

Página 14 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

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 soportado con un acuerdo o documento de formalización.

Los computadores de la CRA se conectarán de manera directa con computadores de entidades externas, conexiones seguras, previa autorización del área de seguridad informática y/o la oficina de Sistemas.

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 los 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. Adicionalmente debe definir un documento de acuerdo oficial entre las partes.

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de la CRA para el funcionamiento de recursos que no sean propios de la entidad y que deban ubicarse en sus instalaciones, los recursos serán administrados por la Oficina de Sistemas o el área técnica a la que corresponda dentro de la CRA.

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.

Página 15 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

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 CRA y otros de terceros debe ser aprobada y certificada por el responsable de la Oficina de Sistemas con el fin de no comprometer la seguridad de la información interna de la CRA.

Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la CRA.

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 CRA. La CRA se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La CRA 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.

POLITICA 8: SOFTWARE UTILIZADO

Todo software que utilice la CRA será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la CRA o reglamentos internos.

Todo el software de manejo de datos que utilice la CRA 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 CRA que garantice el conocimiento por parte de los funcionarios públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la corporación, de las implicaciones que tiene el instalar software ilegal en los computadores de la

Página 16 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

CRA.

Existirá un inventario de las licencias de software de la CRA que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

Deberá existir una reglamentación de uso para los productos de software instalado en demostración los computadores de la CRA.

POLITICA 9: ACTUALIZACION 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 de las áreas involucradas 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 de red o profesional especializado de la oficina de sistemas o coordinador del área.

POLITICA 10: ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática de la CRA 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.

Página 17 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

La CRA 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 CRA, esto de acuerdo con la importancia de la información para la operación de la CRA.

El área dueña de la información en conjunto con la oficina de Sistemas definirán la estrategia a 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 Sistemas. La oficina de Sistemas será la autorizada para realizar el seguimiento y control de esta política.

POLITICA 11: CONTINGENCIA

La administración de la CRA 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, ataque cibernético.

POLITCA 12: AUDITORIA

Todos los sistemas automáticos que operen y administren información sensible, valiosa o crítica para la CRA, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoría.

Página 18 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

Todos los archivos de auditorias deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

Todos los archivos de auditorias 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 auditorias 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 CRA deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

El profesional especializado de la Oficina de Sistemas de Información será:

- Responsable de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías
- Almacenamiento de registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad

POLITICA 13: SEGURIDAD FISICA

La CRA 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.

Página 19 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

Los visitantes de las oficinas de la CRA 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 de cuenta que un visitante no escoltado se encuentra dentro de áreas restringidas de la CRA, 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.

Los centros de cómputo o áreas que la CRA 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 CRA deberá portar su identificación en lugar visible.

En los centros de cómputo o áreas que la CRA considere críticas deberán existir elementos de control de incendio, inundación y alarmas.

Los centros de computo o áreas que la CRA 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 del Subdirector o jefe de la

Página 20 de 22		
Elaboró:	Revisó:	Aprobó:
Lina Saavedra Bornacelli	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

Dependencia, Profesional competente y/o la validación de supervisión de la oficina de Sistemas.

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, del Jefe de Recursos Físicos y/o Oficina de Sistemas.

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 generen 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 CRA.

POLITICA 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, 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.

POLITICA 15: ADMINISTRACION 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

Página 21 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño

	OTROS			
	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
	Código: GS-OT-02	Versión: 2	Fecha: 13/11/2020	

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 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 Coordinador o Subdirector y este a su vez a la Oficina de Sistemas.

Los funcionarios públicos, contratistas, personal temporal, practicantes, pasantes y otras personas relacionadas con terceras partes que utilicen los recursos informáticos de la CRA, 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 de Sistemas.

El Responsable de la Oficina de Sistemas 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 la oficina de Control Interno.

Página 22 de 22		
Elaboró: Lina Saavedra Bornacelli	Revisó: Comité Institucional de Gestión y Desempeño	Aprobó: Comité Institucional de Gestión y Desempeño