CORPORACION AUTONOMA REGIONAL DEL QUINDIO

OFICINA ASESORA DE PLANEACION

NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA

SISTEMA DE GESTION DE SEGUIRIDAD Y PRIVACIDAD DEL AINFORMACION SGSI

SEPTIEMBRE 2025

INTRODUCCION

La dirección de Corporación Autónoma Regional del Quindío, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para Corporación Autónoma Regional del Quindío, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

La información es un activo que, como otros activos importantes de la entidad, tiene valor para la organización y requiere en consecuencia una protección adecuada, adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad de la misión institucional, minimizar los daños a la organización y maximizar la eficiencia de esta.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Corporación Autónoma Regional del Quindío
- Garantizar la continuidad del negocio frente a incidentes.
- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;
- Su integridad, asegurando que la información y sus métodos de proceso son exactos y completos;
- Su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.
- Su seguridad, garantizando que se deben tener mecanismos que permitan su continuidad cuando se presenten eventos naturales y/o antropicos.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

En una organización la gestión de seguridad puede tornarse compleja y difícil de realizar, esto no por razones técnicas, mas bien por razones organizativas, coordinar todos los esfuerzos encaminados para asegurar un entorno informático institucional, mediante la simple administración de recurso humano y tecnológico, sin un adecuado control que integre los esfuerzos y conocimiento humano con las técnicas depuradas de mecanismos automatizados, tomará en la mayoría de los casos un ambiente inimaginablemente hostil, para ello es necesario emplear mecanismos reguladores de las funciones y actividades desarrolladas por cada uno de los empleados de la institución.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y

debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

El documento que se presenta como normas y políticas de seguridad, integra estos esfuerzos de una manera conjunta. Éste pretende, ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la institución, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias.

Las normas y políticas expuestas en este documento sirven de referencia, en ningún momento pretenden ser normas absolutas, las mismas están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad.

Toda persona que utilice los servicios que ofrece la red, deberá conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

GLOSARIO DE TERMINOS

Activo: Son los bienes de información y procesamiento, que posee la institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración Remota: Forma de administrar los equipos informáticos o servicios de la C.R.Q, a través de terminales o equipos remotos, físicamente separados de la institución.

Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Archivo Log: Ficheros de registro o bitácoras de sistemas, en los que se recoge o anota los pasos que dan (lo que hace un usuario, como transcurre una conexión, horarios de conexión, terminales o IP´s involucradas en el proceso, etc.)

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Confidencialidad: Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Cuenta: Mecanismo de identificación de un usuario, llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.

Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Disponibilidad: Los recursos de información sean accesibles, cuando estos sean necesitados.

Encriptación Es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los

datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.

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.

Integridad: Proteger la información de alteraciones no autorizadas por la organización.

Impacto: consecuencia de la materialización de una amenaza.

ISO: (Organización Internacional de Estándares) Institución mundialmente reconocida y acreditada para normar en temas de estándares en una diversidad de áreas, aceptadas y legalmente reconocidas.

IEC: (Comisión Electrotécnica Internacional) Junto a la ISO, desarrolla estándares que son aceptados a nivel internacional.

Normativa de Seguridad ISO/IEC 17799:2000 (Código de buenas prácticas, para el manejo de seguridad de la información) Estándar o norma internacional que vela por que se cumplan los requisitos mínimos de seguridad, que propicien un nivel de seguridad aceptable y acorde a los objetivos institucionales desarrollando buenas prácticas para la gestión de la seguridad informática.

Outsourcing: Contrato por servicios a terceros, tipo de servicio prestado por personal ajeno a la institución.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Responsabilidad: En términos de seguridad, significa determinar que individuo en la institución, es responsable directo de mantener seguros los activos de cómputo e información.

Servicio: Conjunto de aplicativos o programas informáticos, que apoyan la labor educativa, académica y administrativa, sobre los procesos diarios que demanden información o comunicación de la institución.

SGSI: Sistema de Gestión de Seguridad y Privacidad de la Información

Soporte Técnico: (Personal en Outsourcing) Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la institución.

Riesgo: posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

Terceros: Funcionarios de Planta/Contratistas, instituciones, proveedores de software, que tengan relación directa o indirecta con la institución.

Usuario: Defínase a cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga una especie de vinculación laboral con la institución.

Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

LINEAMIENTOS DEL SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

En términos generales el manual de normas y políticas de seguridad y privacidad de la información engloba los procedimientos más adecuados, tomando como lineamientos los siguientes criterios, que se detallan a continuación:

Seguridad Organizacional

Dentro de este, se establece el marco formal de seguridad que debe sustentar la institución, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, Integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad Lógica

Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

Seguridad Física

Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

Seguridad Legal

Integra los requerimientos de seguridad que deben cumplir todos los empleados y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la Corporación Autónoma Regional del Quindío en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país, derechos de autor, propiedad intelectual y contrataciones externas. Cada uno de los criterios anteriores, sustenta un entorno de administración de suma importancia, para la seguridad de la información dentro de la red institucional.

Análisis de riesgos, requerimientos y establecimiento de políticas de seguridad informática.

El análisis de riesgos, como su nombre lo indica, consiste en analizar el sistema de información y su entorno para detectar todos los riesgos que amenazan su estabilidad y su seguridad.
A partir de dicho análisis, se define una serie de requerimientos que se deben satisfacer para alcanzar el nivel de seguridad deseado. El proceso de análisis también debe usarse para modelar el documento de políticas de seguridad informática, que debe reflejar el estado óptimo de seguridad informática que desea obtener la organización, y las políticas que se deben seguir para obtenerlo.

Aseguramiento de Componentes de Software

La seguridad de software busca optimizar los sistemas operativos y las aplicaciones que trabajan en el sistema de información, de manera que sean configurados de manera segura y solo permitan su utilización dentro de parámetros de funcionamiento predefinidos y aceptados (aseguramiento), que funcionen de manera continua y estable (disponibilidad), que ofrezcan un servicio con un nivel de calidad aceptable (calidad del servicio), que no permitan su utilización por personas no autorizadas (control de acceso), y que permitan establecer las responsabilidad de uso (accountability).

Aseguramiento de Componentes de Hardware

La seguridad de Hardware busca optimizar los componentes de hardware del sistema de información (equipos de cómputo, periféricos, medios de

almacenamiento removibles, etc.), de manera que sean configurados de manera segura y solo permitan su utilización dentro de parámetros de funcionamiento predefinidos y aceptados (aseguramiento), que funcionen de manera continua y estable (disponibilidad), que ofrezcan un servicio con un nivel de calidad aceptable (calidad del servicio), que no permitan su utilización por personas no autorizadas (control de acceso), y que permitan establecer las responsabilidad de uso (accountability).

Aseguramiento de Componente Humano

La seguridad humana busca optimizar el componente humano del sistema de información (usuarios, administradores, auditores, etc.) para que su interacción entre ellos y con terceros sea segura, no filtre información que pueda permitir la vulneración del sistema de información, y permita detectar ataques de ingeniería social en su contra.

Aseguramiento de Componentes de Ínterconectividad

La seguridad del componente de interconectividad busca optimizar el componente de comunicaciones del sistema de información (cableado, dispositivos de interconexión –hubs, switches, routers, etc.-, antenas, etc.), de manera que los canales funcionen de manera continua y estable (disponibilidad) se pueda establecer la identidad de los participantes (autenticación), los datos transmitidos puedan ser accesados únicamente por personas autorizadas (confidencialidad), los datos no puedan ser modificados durante su transmisión (integridad) y se pueda establecer el origen de toda comunicación.

Administración de la seguridad informática

La administración de la seguridad informática consiste en una serie de procesos que tienen como propósito mantener un nivel adecuado de seguridad informática en el sistema de información a lo largo del tiempo. Los procesos no se limitan al mantenimiento y la optimización de la seguridad informática en el presente, sino que incluyen también procesos de planeación estratégica de seguridad informática, que garanticen que el nivel de seguridad se mantendrá en el futuro, y que le permitan al sistema de seguridad informática anticiparse a los requerimientos de seguridad impuestos por el entorno, o por la organización a la cual el sistema de información sirve.

Estándares

La siguiente tabla muestra los estándares a ser adoptados:

Componente	ESTANDAR
Análisis de riesgos	ISO/IEC 17799, NIST SP 800-30, NIST SP 800-6
Análisis de requerimientos y establecimiento de políticas de seguridad informática	ISO/IEC 17799, CSC-STD-001-83, ISO 15408, NIST SP 800-55, NIST SP 800-42, NIST SP 800-26, NIST SP 800-18, NIST SP 800-16
Aseguramiento de Componentes de Datos	ISO/IEC 17799, IEEE P1363, NIST SP 800-36, NIST SP 800-21, NIST SP 800-14, NIST SP 800-12
Aseguramiento de Componentes de Software	ISO/IEC 17799, NIST FIPS 73, NIST SP 800-44, NIST SP 800-41, NIST SP 800-36, NIST SP 800-14, NIST SP 800-5
Aseguramiento de Componentes de Hardware	ISO/IEC 17799, NSA/CSS Manual 130-2, NACSIM 5000, NIST SP 800-36, NIST SP 800-14
Aseguramiento de Componente Humano	ISO/IEC 17799, NSA Security Guidelines Handbook, NIST SP 800-50, NIST SP 800-36, NIST SP 800-16, NIST SP 800-14, NSTISSI 4011, NSTISSD 500, NSTISSI 4013, NSTISSI 4014, NSTISSI 4015, CSC-STD-002-85
Aseguramiento de Componentes de Ínter conectividad	ISO/IEC 17799, IEEE P1363, NIST SP 800-45, NIST SP 800-47, NIST SP 800-41, NIST SP 800-36, NIST SP 800-25, NIST SP 800-21, NIST SP 800-14, NIST SP 800-13
Aseguramiento de Infraestructura Física	ISO/IEC 17799, DoD 5220.22-M, NSA Security Guidelines Handbook, NSTISSI 7000, NIST SP 800-36, NIST SP 800-14, NIST SP 800-12
Administración de la seguridad informática	ISO/IEC 17799, ISO/IEC DTR 13335, ISO/IEC DIS 14980, NIST SP 800-64, NIST SP 800-61, NIST SP 800-50, NIST SP 800-55, NIST SP 800-42, NIST SP 800-40, NIST SP 800-36, NIST SP 800-35, NIST SP 800-34, NIST SP 800-18, NIST SP 800-16, NIST SP 800-6, NIST SP 800-5

PRINCIPIOS QUE SOPORTAN EL SISTEMA DE GESTION DE SEGUIRIDAD DE LA INFORMACION

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

- La Corporación Autónoma Regional del Quindío protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La Corporación Autónoma Regional del Quindío protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Corporación Autónoma Regional del Quindío **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.
- La Corporación Autónoma Regional del Quindío **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Corporación Autónoma Regional del Quindío **implementará control de acceso** a la información, sistemas y recursos de red.
- La Corporación Autónoma Regional del Quindío garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Corporación Autónoma Regional del Quindío garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Corporación Autónoma Regional del Quindío **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Corporación Autónoma Regional del Quindío garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

FACTORES CRITICOS DE EXITO

La experiencia muestra que los siguientes factores suelen ser críticos para el éxito de la implantación de la seguridad de la información en una organización:

- Una política, objetivos y actividades que reflejen los objetivos de la organización;
- Un enfoque para implantar la seguridad que sea consistente con la cultura de la organización;
- El apoyo visible y el compromiso de la Dirección General;
- Una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo;
- La convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados;
- La distribución de guías sobre la política de seguridad de la información de la organización y de normas a todos los empleados y contratistas;
- La formación y capacitación adecuadas;
- Un sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información y sugerir mejoras.

INSTRUCCIONES DE INTERPRETACIÓN

La información presentada como normativa de seguridad, ha sido organizada de manera sencilla para que pueda ser interpretada por cualquier persona que ostente un cargo de empleado o terceros con un contrato de trabajo por servicios en la Corporación Autónoma Regional del Quindío, con conocimientos informáticos o sin ellos.

Las políticas fueron creadas según el contexto de aplicación, organizadas por niveles de seguridad y siguiendo un entorno de desarrollo, sobre la problemática de la institución o previniendo futuras rupturas en la seguridad, aplicada sobre los diferentes recursos o activos de la institución.

El esquema de presentación del documento consta de dos secciones, la primera que trata específicamente de las políticas de seguridad, las cuales están organizadas por niveles, dentro de éstos se engloban los dominios que se detallan en el texto subsiguiente a estas líneas.

La segunda sección esta integrada por lo que son las normas de seguridad, que tienen una relación directa, en base a la ejecución y soporte de las políticas de seguridad informática. Estas siguen el mismo enfoque organizativo que las políticas, con la salvedad de seguir un enlace figurativo sobre cada política dentro de los dominios.

Los niveles de seguridad fueron organizados constatando un enfoque objetivo de la situación real de la institución, desarrollando cada política con sumo cuidado sobre qué activo proteger, de qué protegerlo cómo protegerlo y por qué protegerlo; Los mismos se organizan siguiendo el esquema, normativo de seguridad, ISO 17799 (mejores prácticas de seguridad) y que a continuación se presenta:

Nivel de Seguridad Organizativo:

- Seguridad Organizacional
- Políticas de Seguridad
- Excepciones de Responsabilidad
- Clasificación y Control de Activos

*Responsabilidad por los Activos

*Clasificación de la Información

o Seguridad Ligada al Personal

* Capacitación de Usuarios

* Respuestas a Incidentes y Anomalías de Seguridad

Nivel de Seguridad Física:

o Seguridad Física

o Seguridad Física y Ambiental

o Seguridad de los Equipos

o Controles Generales

Nivel de Seguridad Lógico:

o Control de Accesos

o Administración del Acceso de Usuarios

o Seguridad en Acceso de Terceros

o Control de Acceso a la Red

o Control de Acceso a las Aplicaciones

o Monitoreo del Acceso y Uso del Sistema

Nivel de Seguridad Legal:

- Seguridad Legal
- Conformidad con la Legislación
- Cumplimiento de Requisitos Legales
- Revisión de Políticas de Seguridad y Cumplimiento Técnico
- Consideraciones Sobre Auditorias de Sistemas

El lector de las políticas y normas deberá enmarcar sus esfuerzos sin importar el nivel organizacional en el que se encuentre dentro de la institución, por cumplir todas las políticas pertinentes a su entorno de trabajo, utilización de los activos o recursos informáticos en los que éste se desenvuelve.

DEFINICIÓN DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA

¿Que son las Políticas de Seguridad?

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la Corporación. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que la organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

¿Que son las Normas de Seguridad?

Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red institucional.

IMPORTANCIA DE LOS MANUALES DE NORMAS Y POLÍTICAS

Como parte integral de un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), un manual de normas y políticas de seguridad trata de definir; ¿Qué?, ¿Por qué?, ¿De qué? y ¿Cómo? se debe proteger la información y sus activos. Estos engloban una serie de objetivos, estableciendo los mecanismos necesarios para lograr un nivel de seguridad adecuado a las necesidades establecidas dentro de la Corporación Autónoma Regional del Quindío. Estos documentos tratan a su vez de ser el medio de interpretación de la seguridad para toda la organización.

ORGANIZACIÓN DE LA SEGURIDAD INFORMÁTICA

DIRECCION GENERAL

Autoridad de nivel superior que integra el comité de seguridad. Bajo su administración están la aceptación y seguimiento de las políticas y normativa de seguridad.

COMITÉ DE SEGURIDAD DE LA INFORMACION

Autoridad de nivel superior conformada por personal directivo de la entidad, Bajo su administración están la aceptación y seguimiento de las políticas y normativa de seguridad.

GESTOR DE SEGURIDAD

Persona dotada de conocimiento técnico, encargada de velar por la seguridad de la información, realizar auditorías de seguridad, elaborar documentos de seguridad como, políticas, normas; y de llevar un estricto control con la ayuda de la unidad de informática referente a los servicios prestados y niveles de seguridad aceptados para tales servicios.

GRUPO DE SISTEMAS

Dependencia dentro de la institución, que vela por todo lo relacionado con la utilización de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

RESPONSABLE DE ACTIVOS

Personal dentro de las diferentes oficinas y subdirecciones de la Corporación, que velará por la seguridad y correcto funcionamiento de los activos

informáticos, así como de la información procesada en éstos, dentro de sus respectivas áreas o niveles de mando.

BASE LEGAL

La elaboración del manual de normas y políticas de seguridad informática está fundamentada bajo la norma ISO/IEC 17799, en los lineamientos establecidos en el documento de Políticas de Seguridad Informática dentro del proyecto de Gobierno Digital establecido por la Comisión Intersectorial de Políticas y Gestión de la Información para la Administración Pública, Documento CONPES 3072, Directiva Presidencial No 02 de agosto de 2000 y la Ley 1273 de 2009.

VIGENCIA.

La documentación presentada como normativa de seguridad entrará en vigencia desde el momento en que éste sea aprobado como documento técnico de seguridad informática por el Comité de Seguridad de la información de la Corporación Autónoma Regional del Quindío. Esta normativa deberá ser revisada y actualizada conforme a las exigencias y cambios que se presenten en la Corporación, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica de la Red Institucional.

VISIÓN

Constituir un nivel de seguridad, altamente aceptable, mediante el empleo y correcto funcionamiento de la normativa y políticas de seguridad informática, basado en el sistema de gestión de seguridad de la información, a través de la utilización de técnicas y herramientas que contribuyan a optimizar la administración de los recursos informáticos de la Corporación Autónoma Regional del Quindío.

MISIÓN

Establecer las directrices necesarias para el correcto funcionamiento de un sistema de gestión para la seguridad de la información, enmarcando su aplicabilidad en un proceso de desarrollo continuo y actualizable, apegado a los estándares internacionales, políticas y directrices nacionales desarrollados para tal fin.

ALCANCES Y ÁREA DE APLICACIÓN

El ámbito de aplicación del manual de normas y políticas de seguridad informática es la infraestructura tecnológica y entorno informático de la red institucional de la Corporación Autónoma Regional del Quindío. La Oficina Asesora de Planeación garantizará la ejecución y puesta en marcha de la normativa y políticas de seguridad.

POLÍTICAS DE SEGURIDAD INFORMÁTICA

OBJETIVO

Dotar de la información necesaria en el más amplio nivel de detalle a los usuarios, empleados, contratistas y directivos de la Corporación Autónoma Regional del Quindío, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la red institucional de la Corporación Autónoma Regional del Quindío, así como la información digital y/o analógica que es procesada y almacenada en estos o en otros medios.

A continuación se establecen las 12 políticas de seguridad que soportan el SGSI de La Corporación Autónoma Regional del Quindío:

• La Corporación Autónoma Regional del Quindío ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
• Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, contratistas o terceros**.

• La Corporación Autónoma Regional del Quindío protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

• La Corporación Autónoma Regional del Quindío protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• La Corporación Autónoma Regional del Quindío protegerá su información de las amenazas originadas por parte del personal.

• La Corporación Autónoma Regional del Quindío protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• La Corporación Autónoma Regional del Quindío controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• La Corporación Autónoma Regional del Quindío implementará control de acceso a la información, sistemas y recursos de red.

• La Corporación Autónoma Regional del Quindío garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• La Corporación Autónoma Regional del Quindío garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• La Corporación Autónoma Regional del Quindío garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

• La Corporación Autónoma Regional del Quindío garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

DESARROLLO DE LOS LINEAMIENTOS DEL SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Nivel 1

1. SEGURIDAD ORGANIZATIVA

1.1. SEGURIDAD ORGANIZACIONAL

1.1.1. POLÍTICAS DE SEGURIDAD

Art. 1. Los servicios de la red institucional son de exclusivo uso institucional, de investigación técnica, para gestiones administrativas y para acceso de terceros a servicios, cualquier cambio en la normativa de uso de estos, será expresa y adecuada como política de seguridad en este documento.
Art. 2. La Corporación Autónoma Regional del Quindío nombrará un **comité de seguridad,** cuyo objetivo es "asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo, tendrá las siguientes funciones:

- Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información.
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos.
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.

- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
- Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
- Gestionar y coordinar esfuerzos técnicos, humanos y financieros, por crear un plan de contingencia, que dé sustento o solución, a problemas de seguridad dentro de la Corporación. El mismo orientará y guiará a los empleados, la forma o métodos necesarios para salir avante ante cualquier eventualidad que se presente

El comité de seguridad estará integrado por los siguientes miembros:

i. Director General y/o su representante.

ii. Profesional Especializado de Sistemas.

iii. Jefe de la Oficina Asesora de Planeación

iv. Subdirectores y jefes de oficina de la entidad.

v. Jefe de la Oficina de Control Interno

vii. Jefe de la oficina Jurídica.

Art. 3. El Jefe de Oficina y/o Subdirector de cada dependencia dentro de la red institucional es el único responsable de las actividades procedentes de sus acciones.

Art. 4. El profesional especializado de sistemas es el administrador de la infraestructura tecnológica de la entidad, el encargado de coordinar el mantenimiento y el buen estado la red de comunicaciones interna y externa, la infraestructura computacional y los servidores, su configuración y administración dentro de la red institucional, además será el encargado de la implementación de las políticas de seguridad establecidas por la entidad en lo referente a los temas tecnológicos.

Art. 5. Todo usuario de la red de la Corporación Autónoma Regional del Quindío gozará de absoluta privacidad sobre su información o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en

actos ilícitos o contraproducentes para la seguridad de la red institucional, sus servicios o cualquier otra red ajena a la institución.

Art. 6. Los usuarios tendrán el acceso limitado a Internet y sus servicios (acceso a paginas *.gov, *.edu, *.org) o abierto de acuerdo a las restricciones establecidas por la entidad y con autorización de sus jefes inmediatos los cuales deberán enviar autorización por escrito al Gestor de Seguridad, siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la unidad de informática.

Art. 7. Las actividades institucionales tienen la primera prioridad, por lo que a cualquier usuario utilizando otro servicio (por ejemplo Internet, "Chat", WhatsApp, Facebook, etc) sin estos fines, se le podrá solicitar dejar libre la estación de trabajo, si así, fuera necesario o bloquearlo. Esto es importante para satisfacer la demanda de estaciones en horas pico o el uso de estaciones con software especializado y del uso del sistema de Internet.

1.1.2. EXCEPCIONES DE RESPONSABILIDAD

Art. 1. Los usuarios que por disposición de sus superiores realicen acciones que perjudiquen a otros usuarios o la información que estos procesan, y si estos no cuentan con un contrato de confidencialidad y protección de la información de la institución o sus allegados.

Art. 2. Algunos usuarios pueden estar exentos de responsabilidad, o de seguir algunas de las políticas enumeradas en este documento, debido a la responsabilidad de su cargo, o a situaciones no programadas. Estas excepciones deberán ser solicitadas formalmente y aprobadas por el comité de seguridad, con la documentación necesaria para el caso, siendo la Dirección General quien dé por sentada su aprobación final.

1.1.3. CLASIFICACIÓN Y CONTROL DE ACTIVOS

1.1.3.1. RESPONSABILIDAD POR LOS ACTIVOS

Art. 1. El Gestor de Seguridad, será el responsable por el/los activo/s crítico/s o de mayor importancia para la institución, como son las bases de datos institucionales de contabilidad, tesorería, almacén, nomina, presupuesto, Hidrología, meteorología y demás sistemas de información, al igual que el

Hardware y software del centro de cómputo como servidores, licencias de bases de datos, software de desarrollo, equipos de comunicaciones etc.

Art. 2. Cada funcionario de las oficinas o subdirecciones será responsable de la información personal o la información relacionada con su cargo o funciones y que repose en los equipos de cómputo que estén a su cargo o que utilice temporalmente, deberán mantener copias de seguridad y establecer mecanismos que garanticen su fiabilidad.

Art. 3. Los usuarios a los cuales se les asigne un computador y/o periférico será el responsable de este así como de su cuidado.

1.1.3.2. CLASIFICACIÓN DE LA INFORMACIÓN

Art. 1. De forma individual, las oficinas y/o subdirecciones de la CRQ, son responsables, de clasificar de acuerdo con el nivel de importancia, la información que en ella se procese.
Art. 2. Se tomarán como base, los siguientes criterios, como niveles de importancia, para clasificar la información:

a) Pública

b) Interna

c) Confidencial

Art. 3. Los activos de información de mayor importancia para la institución deberán clasificarse por su nivel de exposición o vulnerabilidad.

1.1.4. SEGURIDAD LIGADA AL PERSONAL

Referente a contratos:

Art. 1. Se entregará al contratado, toda la documentación necesaria para ejercer sus labores dentro de la institución, en el momento en que se dé por establecido su contrato laboral y este debe velar para que sea tratada y manejada siguiendo las normas de seguridad y limitaciones establecidas por la entidad.

Art. 2. La información procesada, manipulada o almacenada por el empleado que sea relacionada con su cargo u objeto del contrato es propiedad exclusiva

de la Corporación Autónoma Regional del Quindío y este debe velar para que sea tratada y manejada siguiendo las normas de seguridad y limitaciones establecidas por la entidad.

Art. 3. **Devolución de los Activos:** Todos los funcionarios, contratistas y/o terceros tienen la obligatoriedad de realizar la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Entidad.

1.1.4.1. CAPACITACIÓN DE USUARIOS

Art. 1. Los usuarios de la Entidad y contratistas serán capacitados en seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.

Art. 2. Se deben tomar todas las medidas de seguridad necesarias, antes de realizar una capacitación a personal ajeno o propio de la institución, siempre y cuando se vea implicada la utilización de los servicios de red o se exponga material de importancia considerable para la institución.

1.1.4.2. RESPUESTAS A INCIDENTES Y ANOMALÍAS DE SEGURIDAD

Art. 1. Se realizarán respaldos de la información, diariamente, para la información institucional de mayor importancia o críticos que se almacenen en los servidores ubicados en el centro de cómputo, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado mensualmente, el cual deberá ser guardado externamente y evitar su utilización a menos que sea estrictamente necesaria.

Art. 2. Las solicitudes de asistencia con problemas en las estaciones de trabajo, efectuados por los empleados o áreas de proceso deberán ser tramitados mediante el formulario de solicitud de soporte y deberá dárseles solución en el menor tiempo posible.

Art. 3. Cualquier situación anómala y contraria a la seguridad deberá ser documentada, posterior revisión de los registros o Log de sistemas con el objetivo de verificar la situación y dar una respuesta congruente y acorde al problema, ya sea está en el ámbito legal o cualquier situación administrativa.

Nivel 2

1.2. SEGURIDAD LÓGICA

1.2.1. CONTROL DE ACCESOS

Art. 1. El Gestor de Seguridad proporcionará toda la documentación y apoyo necesario para agilizar la utilización de los sistemas, referente a formularios, guías, controles, otros.

Art. 2. Cualquier petición de información, servicio o acción proveniente de un determinado usuario o subdirección u oficina, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por la institución, para realizar dicha acción; no dar seguimiento a esta política implica:

a) Negar por completo la ejecución de la acción o servicio.

b) Informe completo dirigido a comité de seguridad, el mismo será realizado por el subdirección u oficina al cual le es solicitado el servicio.

c) Sanciones aplicables por autoridades de nivel superior, previamente discutidas con el comité de seguridad.

1.2.1.1. ADMINISTRACIÓN DEL ACCESO DE USUARIOS

Art. 1. Son usuarios de la red institucional los funcionarios de planta, administrativos, secretarias, técnicos y toda aquella persona que tenga vinculo contractual con le Entidad y se le otorgue autorización para que utilice los servicios de la red institucional.

Art. 2. Se asignará una cuenta de acceso a los sistemas de la intranet, cuenta de correo electrónico y a internet, a todo usuario de la red institucional, siempre y cuando el jefe de oficina y/o subdirector lo solicite por escrito y se identifique previamente el objetivo de su uso o permisos explícitos a los que este accederá, junto a la información personal del usuario.

Art. 3. Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con la institución fuera del ámbito de

empleado/contratista y siempre que tenga una vinculación con los servicios de la red institucional.
Art. 4. El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia la institución y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

Art. 5. No se proporcionará el servicio solicitado por un usuario, subdirección y oficina, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

Art. 6. Se creará una cuenta temporal del usuario, en caso de olvido o extravío de información de la cuenta personal, para brindarse al usuario que lo necesite.

Art. 7. La longitud máxima de caracteres permisibles en una contraseña se establece en 8 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales.

Art. 8. El tiempo Máximo de uso de una contraseña es de un mes, al final de este periodo el usuario deberá nuevamente cambiar la contraseña.

Art. 9. Al cabo de 7 intentos fallidos de uso de la cuenta de usuario y/o de contraseña, el sistema bloqueará la cuenta, para su nueva activación se deberá solicitar al Gestor de Seguridad se reactivación.

Art. 10. El Jefe de Oficina y/o Subdirector deberá enviar por escrito al gestor de seguridad la cancelación de la cuenta de un usuario tan pronto tenga información de su retiro de la institución.

Art. 11. La Entidad cuenta con un servicio de acceso a servicio de Internet por parte de usuarios externos, el gestor de seguridad con el apoyo del comité de seguridad deberá implementar y mantener la seguridad necesaria para evitar el ingreso de terceros a la red y servicios institucionales

Art. 12. El acceso remoto a la red informática institucional será restringido y solo mediante autorización del gestor de seguridad se podrá autorizar para fines de soporte y mantenimiento de los sistemas de información y tecnológicos.

1.2.1.2. RESPONSABILIDADES DEL USUARIO

Art. 1. El usuario es responsable exclusivo de mantener a salvo su contraseña.

Art. 2. El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios.

Art. 3. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta se guardada en un lugar seguro.

Art. 4. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Gestor de Seguridad, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

Art. 5. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.

Art. 6. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en el.

Art. 7. Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos de la institución, está obligado a reportarlo a los administradores del sistema o gestor de seguridad.

Art. 8. Los funcionarios de planta y/o contratistas, son responsables de guardar sus trabajos en discos flexibles, CDs, USB etc como copias de seguridad.

Art.9. Ningún usuario podrá utilizar la cuenta de acceso de otro funcionario.

Art.10. A los usuarios les está prohibido ingerir alimentos y bebidas cerca de los equipos de cómputo.

Art. 11. A los usuarios les esta terminantemente prohibido conectar computadores portátiles, celulares u otros dispositivos a la red de comunicaciones de la entidad sin el permiso del gestor de seguridad.

Art.12 Los usuarios utilizaran los servicios informáticos y la red de comunicaciones de la entidad para uso exclusivo de sus labores y no para acciones personales.

Art.13. Los funcionarios que por sus funciones deben usar los navegadores WEB para pagos, consignaciones, traslados financieros etc., deberán usar las contraseñas con responsabilidad, hacer link a las páginas bancarias directamente usando la dirección URL que el banco haya asignado, no hacer transacciones desde dispositivos móviles o hacer enlaces desde cuentas de correo electrónico, no abrir correos electrónicos o archivos adjuntos de desconocidos.

Art.14 Los funcionarios no podrán descargar e instalar ningún software propio o de terceros sin autorización del gestor de seguridad, la violación a esta norma generara una investigación disciplinaria y el usuario será responsable de los perjuicios que se deriven de esta infracción.

Uso de correo electrónico:

Art. 1. El servicio de correo electrónico es un servicio gratuito, se debe hacer uso acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

Art. 2. El correo electrónico es de uso exclusivo para los funcionarios de la Corporación Autónoma Regional del Quindío.

Art. 3. Todo uso indebido del servicio de correo electrónico será motivo de suspensión temporal de su cuenta de correo.

Art. 4. El usuario será responsable de la información que sea enviada con su cuenta.

Art. 5. El comité de seguridad, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.

Art. 6. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

1.2.1.3. SEGURIDAD EN ACCESO DE TERCEROS

Art. 1. El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual deberá estar firmado por las entidades involucradas en el mismo.

Art. 2. Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatar las responsabilidades que devengan de la utilización de este.

Art. 3. Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno de la institución, además de los requisitos expuestos en su contrato con la CRQ.

1.2.1.4. CONTROL DE ACCESO A LA RED

Unidad de Informática y afines a ella.

Art. 1. El acceso a la red interna se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido mediante un mecanismo de autenticación.

Art. 2. Se debe eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo implicado en el proceso.

Art. 3. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoria de seguridad.

Art. 4. El área de informática deberá emplear dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

Art.5. Se registrará todo acceso a los dispositivos de red, mediante archivos de registro o Log, de los dispositivos que provean estos accesos.

Art. 6. Se efectuará una revisión de Log de los dispositivos de acceso a la red cuando se presente fallas en la seguridad.

Art. 7. Los funcionarios de planta y/o contratistas no podrán instalar equipos portátiles y/o utilizar los servicios de red sin autorización del gestor de seguridad, lo anterior con el fin de evitar ingreso de virus y/o sustracción de información institucional.

Art. 8. El gestor de seguridad será el funcionario encargado de la autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas tanto para el ingreso a la red informática como a los sistemas de información de la entidad.

Art. 9 La subdirección administrativa y financiera a través del área de talento humano deberá reportar periódicamente la salida de personal de planta y contratistas de la entidad al gestor de seguridad con el fin de mantener actualizada la lista de funcionarios que pueden tener acceso a la red de comunicaciones y a los aplicativos de la entidad.

1.2.1.4. CONTROL DE ACCESO AL SISTEMA OPERATIVO

Art. 1. Se deshabilitarán las cuentas creadas por ciertas aplicaciones con privilegios de sistema, (cuentas del servidor de aplicaciones, cuentas de herramientas de auditoría, cuentas de administrador, etc.) evitando que estas ejecuten sus servicios con privilegios nocivos para la seguridad del sistema.

Art. 2. Al terminar una sesión de trabajo en las estaciones, los operadores o cualquier otro usuario, evitaran dejar encendido el equipo, pudiendo proporcionar un entorno de utilización de la estación de trabajo.

Art. 3. El acceso a la configuración del sistema operativo de los servidores es únicamente permitido al usuario administrador.

Art. 4. Los administradores de servicios tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

Art. 5 La instalación y configuración de los sistemas operativos y aplicativos de los computadores será responsabilidad del grupo de sistemas.

1.2.1.5. CONTROL DE ACCESO A LAS APLICACIONES

Art. 1. Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso específicas para cada usuario del entorno operativo de la aplicación, las prestaciones de la aplicación.

Art. 2. Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo con el nivel de ejecución o criticidad de las aplicaciones o archivos, y haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.

Art. 3. Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones, de forma aleatoria, sobre distintas fases, antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información u otras anomalías.

Art. 4. Las salidas de información de las aplicaciones, en un entorno de red, deberán ser documentadas, y especificar la terminal por la que deberá ejecutarse exclusivamente la salida de información.

Art. 5. Se deberá llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

Art.6. Todo acceso a uno o varios módulos de una aplicación deberá ser autorizado por el jefe de oficina o subdirección mediante documento enviado al Gestor de seguridad, donde se especifique claramente los permisos que tendrá el usuario sobre el aplicativo y / o la información.

1.2.1.6. MONITOREO DEL ACCESO Y USO DEL SISTEMA

Art. 1. Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

Art. 2. Los archivos Log almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros.

Art. 3. Se efectuará una copia automática de los archivos de Log, y se conducirá o enviará hacia otra terminal o servidor, evitando se guarde la copia localmente donde se produce.

1.3. GESTIÓN DE OPERACIONES Y COMUNICACIONES

1.3.1. RESPONSABILIDADES Y PROCEDIMIENTOS OPERATIVOS

Art. 1. El personal administrador de algún servicio es el responsable absoluto por mantener en óptimo funcionamiento ese servicio, coordinar esfuerzos con el gestor de seguridad, para fomentar una cultura de administración segura y servios óptimos.

Art. 2. Las configuraciones y puesta en marcha de servicios son normadas por el área de informática, y el comité de seguridad.

Art. 3. El personal responsable de los servicios llevará archivos de registro de fallas de seguridad del sistema, revisara, estos archivos de forma frecuente y en especial después de ocurrida una falla.

1.3.2. PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

Art. 1. El área de informática, o personal de la misma dedicado o asignado en el área de programación o planificación y desarrollo de sistemas, efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para la Corporación Autónoma Regional del Quindío

Art. 2. La aceptación del software se hará efectiva por la interventoría de la institución, previo análisis y pruebas efectuadas por el personal de informática.

Art. 3. Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad.

Art. 4. La aceptación y uso de los sistemas no exonera, de responsabilidad alguna sobre el gestor de seguridad, para efectuar pruebas o diagnósticos a la seguridad de estos.

Art. 5. El software diseñado localmente o llámese de otra manera desarrolladas por programadores internos, deberán ser analizados y aprobados, por el gestor de seguridad, antes de su implementación.

Art. 6. Es tarea de programadores el realizar pruebas de validación de entradas, en cuanto a:

- Valores fuera de rango.
- Caracteres inválidos, en los campos de datos.
- Datos incompletos.
- Datos con longitud excedente o valor fuera de rango.
- Datos no autorizados o inconsistentes.
- Procedimientos operativos de validación de errores
- Procedimientos operativos para validación de caracteres.
- Procedimientos operativos para validación de la integridad de los datos.
- Procedimientos operativos para validación e integridad de las salidas.

Art. 7 Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.

Art.8. Cuando se contrate desarrollo de software con terceros, se dejará en el contrato cláusula en la cual se establezca que los derechos de autor e intelectuales serán de la Corporación Autónoma Regional del Quindío.

Art.9. La contratación de software y/o de elaboración de cartografía debe ser concertada con el grupo de sistemas para definir los parámetros y necesidades técnicas respectivas.

1.3.3. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Art. 1. Se adquirirá y utilizará software únicamente de fuentes confiables.

Art. 2. En caso de ser necesaria la adquisición de software de fuentes no confiables, este se adquirirá en código fuente.

Art. 3. Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

Art. 4 El personal del área de sistemas, periódicamente realizara auditoria de sistemas para verificar la instalación de software pirata, en caso de encontrarse alguno(s) instalados, se desinstalarán inmediatamente.

1.3.4. MANTENIMIENTO

Art. 1. El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal del área de sistemas, o del personal de soporte técnico.

Art. 2. El cambio de archivos de sistema no es permitido, sin una justificación aceptable y verificable por el gestor de seguridad.

Art. 3. Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

1.3.5. MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

Art. 1. Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la institución, serán etiquetados de acuerdo con la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.

Art. 2. Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.

Art. 3. Se llevará un control, en el que se especifiquen los medios de almacenamiento en los que se debe guardar información y su uso.

Nivel 3

SEGURIDAD FÍSICA

1.4. SEGURIDAD FÍSICA Y AMBIENTAL

1.4.1. SEGURIDAD DE LOS EQUIPOS

Art. 1. El cableado estructurado de la red se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias y siguiendo los estándares Internacionales establecidos.

Art. 2. Los servidores, sin importar al grupo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.

Art. 3. Los equipos o activos críticos de información y proceso deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el gestor de seguridad y las personas responsables por esos activos, quienes deberán poseer su debida identificación.

Art. 4. El ingreso al área física donde se encuentran los servidores y equipos de comunicaciones de la entidad debe estar protegida con un sistema de alarma cuyas claves las deben manejar el Jefe de la oficina de Planeación, el Gestor de seguridad y el técnico de sistemas.

Art. 5. El área de sistemas de la entidad debe tener instalado aire acondicionado y unidad de UPS de acuerdo con las normas internacionales para este tipo de área de trabajo.

1.4.2. CONTROLES GENERALES

Art. 1. Las estaciones o terminales de trabajo, con procesamientos críticos no deben de contar con medios de almacenamientos extraíbles, que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información o el ingreso de virus a través de estos a la red de la entidad, en caso de requerirse la utilización de estos deberán contar con la aprobación del gestor de seguridad.

Art. 2. En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.

Art. 3. Deberá llevarse un control exhaustivo del mantenimiento preventivo y otro para el mantenimiento correctivo que se les haga a los equipos.

Art. 4. Toda oficina o área de trabajo debe poseer entre sus inventarios, herramientas auxiliares (extintores, alarmas contra incendios, lámpara de emergencia), necesarias para salvaguardar los recursos tecnológicos y la información.

Art. 5. Toda visita a las oficinas de tratamiento de datos críticos e información (unidad de informática, sala de servidores entre otros) deberá ser registrada mediante el formulario de accesos a las salas de procesamiento crítico, para posteriores análisis de este.

Art. 6. La sala o cuarto de servidores, deberá estar separada de las oficinas administrativas, mediante una división en el área de sistemas, recubierta de material aislante o protegido contra el fuego, Esta sala deberá ser utilizada únicamente por las estaciones prestadoras de servicios y/o dispositivos a fines.

Art. 7. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

Art. 8. El suministro de energía eléctrica debe estar debidamente polarizado, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente, si no que debe existir una red de polarización.

Art. 9. Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

Art. 10. Los funcionarios, contratistas o terceros pueden tener acceso a las redes inalámbricas que se encuentran instaladas en las dependencias de la Corporación Autónoma Regional del Quindío como apoyo a sus labores contractuales, la Corporación Autónoma Regional del Quindío no se hace responsable por el mal uso que terceros hagan de estas redes de comunicaciones.

Nivel 4

SEGURIDAD LEGAL

1.5. SEGURIDAD LEGAL

1.5.1. CONFORMIDAD CON LA LEGISLACIÓN

1.5.1.1. CUMPLIMIENTO DE REQUISITOS LEGALES

Licenciamiento de Software:

Art. 1. La Corporación Autónoma Regional del Quindío, se reserva el derecho de respaldo, a cualquier funcionario de la institución, ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.

Art. 2. Todo el software comercial que utilice la Corporación Autónoma Regional del Quindío deberá estar legalmente registrado, en los contratos de arrendamiento de software con sus respectivas licencias.

Art. 3. La adquisición de software por parte de personal que labore en la institución no expresa el consentimiento de la institución, la instalación del mismo no garantiza responsabilidad alguna para la Corporación Autónoma Regional del Quindío, por ende la institución no se hace responsable de las actividades de sus empleados.

Art. 4. Tanto el software comercial como el software libre son propiedad intelectual exclusiva de sus desarrolladores, la Corporación Autónoma

Regional del Quindío respeta la propiedad intelectual y se rige por el contrato de licencia de sus autores.

Art. 5. El software comercial licenciado a la Corporación Autónoma Regional del Quindío es propiedad exclusiva de la institución, la misma se reserva el derecho de reproducción de éste, sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.

Art. 6. En caso de transferencia de software comercial a terceros, se harán las gestiones necesarias para su efecto y se acatarán las medidas de licenciamiento relacionadas con la propiedad intelectual.

Art. 7. Las responsabilidades inherentes al licenciamiento de software libre son responsabilidad absoluta de la Corporación Autónoma Regional del Quindío.

Art. 8. Cualquier cambio en la política de utilización de software comercial o software libre, se hará documentado y en base a las disposiciones de la respectiva licencia.

Art. 9. El software desarrollado internamente, por el personal que labora en la institución es propiedad exclusiva de la Corporación Autónoma Regional del Quindío.

Art. 10. La adquisición del software libre o comercial deberá ser gestionado con las autoridades competentes y acatando sus disposiciones legales, en ningún momento se obtendrá software de forma fraudulenta.

Art. 11. Los contratos con terceros, en la gestión o prestación de un servicio, deberán especificar, las medidas necesarias de seguridad, nivel de prestación del servicio, y/o el personal involucrado en tal proceso.

Art. 12. La información entregada por terceros a la Corporación Autonomía Regional del Quindío en calidad de préstamo para labores misionales será custodiada por el gestor de seguridad y no podrá ser entregada a funcionarios y/o contratistas sin la autorización escrita de la institución propietaria de la misma.

1.5.1.2. REVISIÓN DE POLÍTICAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

Art. 1. Toda violación a las políticas de licenciamiento de software será motivo de sanciones de acuerdo a la Ley aplicables al personal que incurra en la violación.

Art. 2. El documento de seguridad será elaborado y actualizado por el gestor de seguridad, junto al comité de seguridad, su aprobación y puesta en ejecución será responsabilidad de la Dirección General.

Art. 3. Cualquier violación a la seguridad por parte del personal que labora, para la Corporación Autónoma Regional del Quindío, así como terceros que tengan relación o alguna especie de contrato con la institución se harán acreedores a sanciones aplicables de acuerdo con la ley 200 (código disciplinario) y a la Ley 734 De 2011.

1.5.1.3. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS

Art. 1. Se debe efectuar una auditoria de seguridad a los sistemas de acceso a la red anualmente o cuando se requiera, enmarcada en pruebas de acceso tanto internas como externas, desarrolladas por personal técnico especializado o en su defecto personal capacitado en el área de seguridad.

Art. 2. Toda auditoria a los sistemas, estará debidamente aprobada, y tendrá el sello y firma de la Dirección General.

Art. 3. Cualquier acción que amerite la ejecución de una auditoria a los sistemas informáticos deberá ser documentada y establecida su aplicabilidad y objetivos de esta, así como razones para su ejecución, personal involucrada en la misma y sistemas implicados.

Art. 4. La auditoría no deberá modificar en ningún momento el sistema de archivos de los sistemas implicados, en caso de haber necesidad de modificar algunos, se deberá hacer un respaldo formal del sistema o sus archivos.

Art. 5. Las herramientas utilizadas para la auditoria deberán estar separadas de los sistemas de producción y en ningún momento estas se quedarán al alcance de personal ajeno a la elaboración de la auditoria.

2. NORMAS DE SEGURIDAD INFORMÁTICA

2.1. OBJETIVO

Proporcionar las directrices necesarias para la correcta administración del Sistema de Gestión de Seguridad y privacidad de la Información, bajo un entorno normativamente regulado e interpretable por los usuarios de la red institucional y ajustada a las necesidades de la Corporación Autónoma Regional del Quindío.

2.2. SEGURIDAD ORGANIZACIONAL

2.2.1. EN CUANTO A POLÍTICAS GENERALES DE SEGURIDAD

Área de Sistemas:

Art. 1 El usuario acatará las disposiciones expresas sobre la utilización de los servicios informáticos de la red institucional.

Art.2 El Gestor de seguridad hará respaldos periódicos de la información institucional almacenada en los servidores así como la depuración de los discos duros.

Art. 3 El gestor de seguridad y/o administrador de sistemas, realizarán auditorias periódicas en el sistema con el fin de localizar intrusos o usuarios que estén haciendo mal uso de los recursos de un servidor.

Art. 4 Se revisará el tráfico de paquetes que se estén generando dentro de un segmento de red, a fin de determinar si se está haciendo mal uso de la red o se está generando algún problema que pueda llevar a que se colapsen los sistemas.

Art.5. El gestor de seguridad dará de alta y baja a usuarios y revisará las cuentas periódicamente para estar seguros de que no hay usuarios ficticios.

Art. 6. Recomendar sobre el uso e implementación de nuevas tecnologías para administración de los sistemas y la red.

Art. 7. Reportar a las autoridades de la institución, las fallas en el desempeño de la red. Solucionar junto al gestor de seguridad, los problemas que se generen en su red local.

Art. 8. La Corporación Autónoma Regional del Quindío se guarda el derecho de divulgación o confidencialidad de la información personal de los usuarios de la red institucional, si estos se ven envueltos en actos ilícitos.

Art. 9. El gestor de seguridad monitoreara las acciones y tareas de los usuarios de la red institucional.

Art. 10. Se prestará el servicio de Internet, siempre que se encuentren presentes los requisitos de seguridad mínimos.

Art. 11. El usuario no tiene derecho sobre el servicio de Internet sino es mediante la aceptación de la normativa de seguridad.

2.2.2. EXCEPCIONES DE RESPONSABILIDAD

Art. 1. La institución debe establecer con sus empleados un contrato de confidencialidad de común acuerdo.

Art. 2. Toda acción debe seguir los canales de gestión necesarios para su ejecución.

Art. 3 El comité de seguridad proveerá la documentación necesaria para aprobar un acuerdo de no responsabilidad por acciones que realicen dentro de la red institucional.

Art. 4 Las gestiones para las excepciones de responsabilidad son acordadas bajo común acuerdo de la Dirección General y el comité de seguridad.

2.2.3. CLASIFICACIÓN Y CONTROL DE ACTIVOS

2.2.3.1. RESPONSABILIDAD POR LOS ACTIVOS

Art.1 Los jefes de cada oficina y subdirección de la institución, son responsables de mantener o proteger los activos de mayor importancia.

2.2.3.2. CLASIFICACIÓN DE LA INFORMACION

Art. 1 Cada jefe de oficina o subdirección dará importancia a la información en base al nivel de clasificación que demande el activo.

Art. 2 La información pública puede ser visualizada por cualquier persona dentro o fuera de la institución a través de la página Web y siguiendo las directrices del gobierno Digital.

Art. 2 La información interna, es propiedad de la institución, en ningún momento intervendrán personas ajenas a su proceso o manipulación.

Art. 3 La información confidencial es propiedad absoluta de la institución, el acceso a ésta es permitido únicamente a personal administrativo.

Art. 4 Los niveles de seguridad se detallan como nivel de seguridad bajo, nivel de seguridad medio y nivel de seguridad alto.

Art.5. La información generada, producida o desarrollada por la Corporación Autónoma Regional del Quindío es de su propiedad intelectual y de sus derechos de autor, para entregar esta información a terceros, las dependencias deberán solicitar por escrito autorización al jefe de la oficina asesora de planeación y se deberá firmar un contrato de responsabilidad con terceros.

Art.16 La información que otras instituciones entreguen a la CRQ para procesos misionales no deberá ser entregada a terceros sin previa autorización escrita de sus propietarios.

2.2.4. SEGURIDAD LIGADA AL PERSONAL

Referente a contratos.

El empleado.

Art. 1 El empleado no tiene ningún derecho de autor ni intelectual sobre la información que procese dentro de las instalaciones de la red institucional y en cumplimiento del contrato externo o laboral.

Art. 2 La información que maneja o manipula el empleado, no puede ser divulgada a terceros o fuera del ámbito de laboral.

Art. 3 El usuario se regirá por las disposiciones de seguridad informática de la Corporación Autónoma Regional del Quindío.

Art. 4 Los usuarios son responsables de las acciones causadas por sus operaciones con el equipo de la red institucional.

Art 5. Los empleados, contratistas y cualquier otro usuario vinculado con la CRQ respetaran los derechos de autor y la propiedad intelectual de la información que reciban o procesen de la entidad o de otras entidades para desarrollar sus trabajos.

2.2.4.1. CAPACITACIÓN DE USUARIOS

Art. 1 El comité de seguridad capacitará los usuarios de la red institucional en las normas de seguridad informática.

Art. 2 El comité de seguridad proporcionara las fechas en que se impartirán las capacitaciones.

Art. 3 El material de apoyo (manuales, guías, etc.) será entregado minutos antes de iniciar la capacitación, en la sala donde será efectuada la capacitación.

Art. 4 Las capacitaciones deben realizarse fuera de áreas de procesamiento de información.

Art. 5 Entre los deberes y derechos de los empleados institucionales y personal denotado como tercero, se encuentran acatar o respetar las disposiciones sobre capacitaciones y por ende asistir a ellas sin excepción alguna, salvo casos especiales.

Art 6. Los empleados, contratistas deberán estar apropiadamente informados sobre sus roles y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información

2.2.4.2. RESPUESTA A INCIDENTES Y ANOMALIAS DE SEGURIDAD

Art. 1 Los respaldos de información institucional deberán ser almacenados en un sitio aislado y libre de cualquier daño o posible extracción por terceros dentro de la institución y una copia fuera de la institución.

Art.2 Los respaldos se utilizarán únicamente en casos especiales ya que su contenido es de suma importancia para la institución.

Art. 3 La institución debe contar con respaldos de la información institucional ante cualquier incidente.

Art. 4 Generar procedimientos manuales de respaldo de información.

Art.5 El área de sistemas tendrá la responsabilidad, de priorizar una situación de la otra en cuanto a los problemas en las estaciones de trabajo.

Art. 6 En situaciones de emergencia que impliquen áreas como atención al cliente entre otros, se da prioridad en el orden siguiente.

a. Atención al cliente

b. Subdirección operativa, administrativa y financiera, Dirección General

c. Subdirección de Control y seguimiento ambiental y Subdirección de ejecución de políticas ambientales

d. Oficina Jurídica y Oficina de Control Interno

Art.7 El documento de seguridad se elaborará, tomando en cuenta aspectos basados en situaciones pasadas, y enmarcarlo en la pro actividad de situaciones futuras.

Art. 8 Se prioriza la información de mayor importancia para la institución.

Art. 9 Se evacua la información o activo de los niveles confidenciales de la institución.

Art. 10. Llevar un registro manual de las actividades sospechosas de los empleados.

2.3. **SEGURIDAD LÓGICA**

2.3.1. CONTROL DEL ACCESO DE USUARIOS A LA RED INSTITUCIONAL

Art. 1 La documentación de seguridad será resguardada por el gestor de seguridad, esto incluye folletos, guías, formularios, controles entre otros.

Art.2 Los canales de gestión y seguimiento para realizar acciones dentro de la red institucional, no pueden ser violentados en ninguna circunstancia.

Art. 3 El personal encargado de dar soporte a la gestión de comunicaciones entre servicios y la prestación de este, no está autorizado a brindar ninguna clase de servicios, mientras no se haya seguido todos y cada uno de los canales de gestión necesarios.
Art 4. La oficina de recursos humanos informara oportunamente y por escrito al gestor de seguridad sobre el retiro de personal de planta o contratista para desactivar sus cuentas y derechos de acceso a la información.
Art 5. El gestor de seguridad una vez informado del retiro de personal deberá cambiar o anular las claves de acceso que el empleado tenía en software, correos electrónicos, equipos etc.

2.3.1.1. ADMINISTRACIÓN DEL ACCESO DE USUARIOS A LOS SERVICIOS INFORMÁTICOS DE LA INSTITUCION.

Art. 1 Sin excepción alguna se consideran usuarios de la red institucional de la CRQ todos y cada uno del personal que se encuentra denotado en la política de administración de acceso de usuarios.

Art. 2 El acceso a los sistemas y servicios de información, es permitido únicamente a los usuarios que dispongan de los permisos necesarios para su ejecución.

Art. 3 El usuario deberá proveer toda la información necesaria para poder brindarle los permisos necesarios para la ejecución de los servicios de la red institucional.

Art. 4 El acceso a la Internet por parte de los usuarios esta sujeto a la normativa desarrollada por cada Jefe de Oficina y/o Subdirector y sus disposiciones generales, estos usuarios no necesitan la aprobación del gestor o del comité de seguridad, para tener acceso.

Art. 5 Las necesidades y aprobación de acceso, de los funcionarios a los servicios de la red institucional, deberá ser documentada y actualizada su información, en la política que norma su uso.

Art. 6 La identificación del usuario se hará a través autorización escrita enviada por el Jefe de Oficina y/o Subdirector quien se la enviara el Gestor de Seguridad, y se autenticara, mediante la firma impresa de la persona que tendrá acceso al sistema o se acreditará con su cuenta de usuario

Art. 7 Cualquier petición de servicio, por parte de personal de la institución o ajeno a la misma, no se concederá sino es mediante la aprobación de la política de acceso y prestación de servicio.

Art. 8 La cuenta temporal es usada únicamente con propósitos legales y de ejecución de tareas, por olvido de la información de la cuenta personal.

Art. 9 La cuenta temporal es únicamente acreditable, si se proporciona la información necesaria para su uso.

Art. 10 Toda cuenta nula u olvidada, se eliminará del/los sistema/s, previa verificación o asignación de una nueva cuenta, al usuario propietario de la cuenta a eliminar.

Art. 11 El par usuario/contraseña temporal, será eliminada del sistema como tal, por el gestor de seguridad, en el preciso momento en que sea habilitada una cuenta personal para el usuario que haya solicitado su uso.

Art. 12 El sistema no aceptará contraseñas con una longitud menor a la expresada en la política de creación de contraseñas.

Art. 13 Los usuarios darán un seguimiento estricto sobre las políticas de creación de contraseñas, acatando sus disposiciones en su totalidad.

Art. 14 El sistema revocará toda contraseña con una longitud mayor a la expresada en la política de creación de contraseñas.

Art. 17 El usuario se responsabiliza en crear una contraseña fuerte y difícil de conocer.

2.3.1.2. RESPONSABILIDADES DEL USUARIO

Art. 1 El usuario deberá estar consiente de los problemas de seguridad que acarrea la irresponsabilidad en la salvaguarda y uso de su contraseña.

Art. 2 El usuario deberá ser precavido al manipular su cuenta de acceso a los sistemas, tomando medidas de seguridad que no pongan en riesgo su integridad como persona.

Art.3 Las cuentas de usuario son personales, en ningún momento deben ser utilizadas por personal ajeno al que le fue asignada.

Art. 4 La práctica de guardar las contraseñas en papel adherido al monitor o áreas cercanas al equipo de trabajo, es una falta grave y sancionable.

Art. 5 Las contraseñas deben ser memorizadas desde el mismo momento en que le es asignada.

Art. 6 Se desechará, toda documentación que tenga que ver con información relacionada a su cuenta de usuario, minutos después de habérsele entregado y siempre que haya sido memorizada o resguarda su información

Art. 7 Es importante que el usuario establezca contraseñas fuertes y desligadas de su vida personal o de su entorno familiar o no emplean do formatos comunes de fechas.

Art.8 El usuario es parte esencial en la seguridad de la red institucional, su experiencia como operador en las estaciones de trabajo es de suma importancia para el comité de seguridad.

Art. 9 Toda falla en el equipo debe ser documentado por el operador de las estación de trabajo.

Art. 10 El usuario hará copias de seguridad de la información que procesan en discos flexibles o unidades USB.

Art. 11. El usuario que tiene a cargo las transacciones financieras de la entidad está obligado a realizarlas en los equipos de cómputo de la entidad, está prohibido hacerlo desde computadores portátiles o personales, de igual manera

deberá hacer los links desde la dirección URL de las páginas oficiales de los bancos y no desde un navegador o correo electrónico.

Art.12 El usuario que tiene a cargo las transacciones financieras de la entidad está obligado a tomar medidas seguras en el lugar físico donde se encuentran los equipos de cómputo para que no haya ingresos de personas no autorizadas.

Normativa del Uso del Correo electrónico.

Art. 1 El correo electrónico es un medio de comunicación directo y confidencial, entre el emisor del mensaje y el receptor o receptores del mismo, por ende deberá ser visto o reproducido por las personas implicadas en la comunicación.

Art. 2 Ningún usuario externo a la institución, puede usar los servicios de correo electrónico proporcionado por la red institucional.

Art. 3 Es responsabilidad del usuario hacer un correcto empleo del servicio de correo electrónico.

Art. 4 Las cuentas de correo que no cumplan con la normativa de seguridad o los fines institucionales o de investigación para lo que fueron creadas, pierden automáticamente su característica de privacidad.

Art. 5 La cuenta de usuario que mostrase un tráfico excesivo y que almacenare software de forma ilegal serán deshabilitadas temporalmente.

Art. 6 La información y el software tienen la característica de ser propiedad intelectual, la CRQ no se responsabiliza por el uso del correo electrónico de parte de sus empleados violentando la ley de derechos de autor.

2.3.1.3. SEGURIDAD EN ACCESO DE TERCEROS

Art. 1 Los requisitos mínimos de seguridad se expresan, en cuestión del monitoreo y adecuación de un servicio con respecto a su entorno o medio de operación.

Art. 2 El gestor de seguridad tomará las medidas necesarias para asignar los servicios a los usuarios externos.

Art. 3 El no cumplimiento de las disposiciones de seguridad y responsabilidad sobre sus acciones por parte de los usuarios de la red institucional, se obliga a la suspensión de su cuenta de usuario de los servicios.

2.3.1.4. CONTROL DE ACCESO A LA RED

Art. 1 El administrador de sistemas diseñará los mecanismos necesarios para proveer acceso a los servicios de la red institucional.

Art. 2 Los mecanismos de autenticación y permisos de acceso a la red, deberán ser evaluados y aprobados por el gestor de seguridad.

Art. 3 El administrador de sistemas, verificará que el tráfico de red sea, estrictamente normal, la variación de este sin ninguna razón obvia, pondrá en marcha técnicas de análisis concretas.

Art. 4. Los dispositivos de red estarán siempre activos, y configurados correctamente para evitar anomalías en el tráfico y seguridad de información de la red institucional.

Art. 5. Se utilizarán mecanismos y protocolos de autenticación como, ssh, IPsec, Claves públicas y privadas, autenticación usuario/contraseña, cualquiera de ellos será válido para la autenticación.

Art. 6. Los archivos de registro o logs de los dispositivos de red deberán estar activados y configurados correctamente, en cada dispositivo.

2.3.1.5. MONITOREO DEL ACCESO Y USO DEL SISTEMA

Personal de Informática:

Art.1 El administrador de sistemas tendrá especial cuidado al momento de instalar aplicaciones en los servidores, configurando correctamente cada servicio con su respectivo permisos de ejecución.

Art. 2 La finalización de la jornada laboral, termina con cualquier actividad desarrolla en ese momento, lo cual implica guardar todo cuanto se utilice y apagar equipos informáticos antes de salir de las instalaciones.

Art. 3. No le está permitido al usuario operador, realizar actividades de configuración del sistema, bajo ninguna circunstancia.

Art. 4. Los servidores estarán debidamente configurados, evitando el abuso de personal extraño a la administración estos.

Art. 5. En el caso de haber la necesidad de efectuar configuración de servicios por más de un usuario administrador de estos, se concederá acceso exclusivo mediante una cuenta referida al servicio.

Art. 6. La cuenta administrativa, es propiedad exclusiva del administrador de sistemas y una copia de la contraseña deberá tenerla el jefe de la oficina de planeación.

Art. 7 Las aplicaciones prestadoras de servicios correrán con cuentas restrictivas y jamás con privilegios tan altos como los de la cuenta administrativa.

Art 8. El personal de sistemas encargado de la administración de los equipos de cómputo y del software de apoyo podrá realizar labores de mantenimiento a través de sistemas remotos.

2.3.1.6. CONTROL DE ACCESO A LAS APLICACIONES

Art. 1 Las aplicaciones deberán contar con su respectiva documentación, la cual será entregada a cada empleado de la institución que la utilice.

Art. 2 El usuario tendrá los permisos de aplicaciones necesarios para ejercer su trabajo.

Art. 3 Tienen acceso total a las aplicaciones y sus archivos, los usuarios que lo ameriten por su cargo dentro de la institución, siempre que sea aprobado por el Jefe de Oficina y/o Subdirector.

Art. 4 Los niveles de privilegio son definidos por Jefe de Oficina y/o Subdirector, en base a lo importante o critico de la información que procesará el usuario.

Art. 5 Antes de ser puestas en ejecución, las aplicaciones recibirán una auditoria sobre fallos o información errónea que puedan procesar.

Art. 6 Se hace énfasis en la importancia que tienen las salidas de información provistas por una aplicación, sin importar el medio de salida.

Art. 7 En el registro de sucesos del sistema se registran todas las actividades realizadas por un determinado usuario, sobre las aplicaciones.

Art. 8 Se verifica constantemente la operatividad de los registros de logs, que no sean alterados de forma fraudulenta.

2.3.1.7. MONITOREO DEL ACCESO Y USO DEL SISTEMA

Art. 1 Los archivos de registro de sucesos de los sistemas de aplicación y de operación, se mantienen siempre activos y en ningún momento deberán ser deshabilitados.

Art. 2 De ser necesarios, se crearán archivos de ejecución de comandos por lotes para verificar que se cumpla el grabado completo de la información a la que es accedida por los usuarios, aplicaciones, sistemas, y para los dispositivos que guardan estos archivos.

Art. 3 Es necesario efectuar un respaldo de los archivos de registro o logs, fuera de los dispositivos que les creen.

Art. 4 Los archivos de logs deben ser respaldados en tiempo real, sus nombres deben contener la hora y la fecha en la que fueron creados sus originales.

2.3.2. GESTIÓN DE OPERACIONES Y COMUNICACIONES

2.3.2.1. RESPONSABILIDADES DEL USUARIO SOBRE LOS PROCEDIMIENTOS OPERATIVOS.

Art. 1 Es la oficina de sistemas quien crea las reglas para la ejecución de algún servicio.

Art. 2 Es el comité de seguridad quien aprueba la normas creadas para la ejecución de los servicios.

Art. 3 Los sistemas son configurados para responder de forma automática, con la presentación de un informe que denote las características propias de un error en el sistema.

2.3.2.2. PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

Art. 1 Ninguna otra persona que no sea la expresada en la política de aceptación y creación de sistemas puede intervenir, sino es por petición expresa de alguna de estas.

Art.2 Ninguna persona que labore para la institución, está facultada para instalar software en las estaciones de trabajo, sin antes haberse aprobado su utilización.

Art. 3 Sin importar el origen del software y la utilización de este dentro de la institución, éste será evaluado por el área de sistemas, haya sido o no aprobada su utilización.

Art. 4 Ninguna clase de código ejecutable será puesto en marcha sin antes haber pasado el control de análisis sobre seguridad de este.

Art. 5 Antes de efectuar cualquier análisis o prueba sobre los sistemas de producción, se realizarán Backus generales, de la información que en ellos se procesa y del sistema en sí.

Art. 6 Los sistemas o dispositivos que aún están conectados a la red, pero que no tienen utilización productiva alguna para la institución, se les deberá eliminar cualquier rastro de información que hayan contenido.

Art. 7 El gestor de seguridad deberá mantener actualizado un manual sobre el plan de contingencia de la empresa en caso de desastre natural y/o entrópico.

2.3.2.3. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Art. 1 El software que venga de empresas no reconocidas o acreditadas como no confiables, no tendrá valor alguno para la institución siempre que esta sea en formato ejecutable.

Art. 2 El gestor de seguridad supervisará la instalación y correcta configuración de software antivirus en todas y cada una de las estaciones de trabajo de la institución.

Art. 3. La entidad deberá tener un servidor antivirus actualizado y funcionando óptimamente, la administración de este estará a cargo del gestor de seguridad.

Art. 4. A los equipos clientes se les podrá suspender los puertos USB, Serial u otro que permitan la conexión de dispositivos externos y que pongan en riesgo la seguridad de la información e infraestructura institucional.

Art. 5. Los usuarios estarán en la obligación de realizar revisión de virus a todo dispositivo externo que se vaya a usar en su computador.

2.3.2.4. MANTENIMIENTO DE SISTEMAS Y EQUIPO DE CÓMPUTO

Art. 1 El usuario no está facultado a intervenir física o lógicamente ninguna estación de trabajo, que amerite reparación.

Art. 2 En ningún momento es aceptable la modificación de archivos en los equipos informáticos, sino es bajo circunstancias especiales, en las que de no hacerse de esa manera el sistema queda inutilizable.

Art. 3. El personal de sistemas no se hará responsable de la información existente en los equipos de cómputo de los usuarios en el momento de realizar mantenimiento preventivo y/o correctivo.

Art. 4 Se deberá haber una bitácora completa, en cuanto a las versiones de actualización del software y de las revisiones instaladas en los sistemas.

Art. 5. Los funcionarios de sistemas son los únicos responsables del mantenimiento preventivo y correctivo de los computadores y redes de comunicación.

Art. 6. La oficina de sistemas avisará con anticipación a cada usuario sobre el mantenimiento preventivo que se realizará a su computador y el usuario deberá hacerse responsable de sacar copias de seguridad.

Art.7. La oficina de sistemas llevara hojas de vida e inventario de cada computador donde se detallen sus características, mantenimientos efectuados.

Art 8. La oficina de sistemas realizará mantenimientos físico y lógico de los computadores y servidores de la entidad, deberá llevar un registro en la hoja de vida de estos y además mantener las actualizaciones de los sistemas operativos al día.

2.3.2.5. SEGURIDAD EN EL MANEJO DE LOS MEDIOS DE ALMACENAMIENTO

Art. 1 La clasificación e identificación de los medios de almacenamiento, es acorde al propósito u objetivo por el cual se respalda.

Art. 2 Es totalmente prohibido para los usuarios de la red institucional el intervenir con las labores de respaldo del personal de informática.

Art. 3 En ninguna circunstancia se dejarán desatendidos los medios de almacenamiento, o copias de seguridad de los sistemas.

Art. 4 Todo medio de almacenamiento deberá ser documentado e inventariado en un registro específico y único sobre medios de almacenamiento.

Art. 5 La ubicación de los medios de almacenamiento deberá estar alejada del polvo, humedad, o cualquier contacto con material o químicos corrosibles.

Art. 6 Entre la documentación de seguridad deberá existir un control para la clasificación y resguardo de los medios de almacenamiento

2.4. **SEGURIDAD FÍSICA**

2.4.1. LA SEGURIDAD EN LOS DIFERENTES DEPARTAMENTOS DE PROCESAMIENTO DE INFORMACIÓN

2.4.1.1. RESGUARDO DE LOS EQUIPOS DE CÓMPUTO

Usuarios comunes y administrativos:

Art. 1 El área de sistemas será la responsables del diseño, implementación y mantenimiento toda la red de comunicaciones y sus características técnicas de la institución siguiendo la normativa y estándares internacionales de cableado estructurado.

Art. 2 Es totalmente prohibido, salvo autorización o supervisión expresa del área de sistemas, la intervención física de los usuarios sobre los recursos de la red institucional (cables, enlaces, estaciones de trabajo, dispositivos de red).

Art. 3 Solo el personal autorizado es el encargado exclusivo de intervenir físicamente los recursos de la red institucional.

Art.4 Solo el personal de sistemas tendrá acceso a los centro de comunicaciones, área de servidores y de comunicaciones de la entidad, cualquier persona externa será autorizada por el gestor de seguridad cuando

Personal de Informática:

Art. 1 El soporte técnico a las estaciones de trabajo y servidores, es responsabilidad del área de sistemas, por tanto deben tomarse todas las medidas de seguridad necesarias para evitar cualquier anomalía por manipulación errónea efectuada por terceros.

Art. 2 Las estaciones de trabajo, servidores y equipos de comunicaciones, deben operar en óptimas condiciones, efectuando un mantenimiento constante y acorde a las especificaciones de los fabricantes del equipo.

Art. 3 Se deberá proteger las salas que contengan los servidores, o equipos de información críticos, con paredes recubiertas de material aislante o antiincendios.

Art. 4 Las líneas de alimentación de energía externa deberán estar protegidas con filtros de protección para rayos.

Art. 5 Los centros de procesamiento de datos o unidades de procesos críticos, son zonas restringidas, únicamente accesibles por personal autorizado o que labore en dichas instalaciones.

Art. 6 Al permanecer en las instalaciones de procesamiento de información, se dedicará única y exclusivamente a los procesos relacionados con las actividades propias del centro de procesamiento, evitando cualquier actividad contraria a los objetivos para los que fue diseñada.

Art. 7 Cada estación de procesamiento crítico de información deberá estar protegido con un dispositivo de alimentación ininterrumpida, que deberá ser de uso exclusivo para dicha estación.

Art. 8. La institución deberá tener sistemas alternos de respaldo (servidores secundarios) de los servidores principales con el fin de evitar fallas por tiempos largos en caso de que los servidores principales fallen por cualquier circunstancia.

2.4.1.2. CONTROLES FÍSICOS GENERALES

Art. 1 Los respaldos de información de los servidores de procesos críticos, solo lo realizara el administrador de sistemas.

Art. 2 Las lectoras de CD y USB deberán deshabilitarse en aquellas máquinas en que no se necesiten.

Art. 3 Cada empleado de la institución, velará por la correcta salvaguarda de la información, el dejar información desatendida sin ningún medio de seguridad verificable es una práctica prohibida y sancionable.

Art. 4 Se debe establecer los periodos de mantenimiento preventivo.

Art. 5 No se permite el ingreso a las instalaciones de procesos críticos, sin antes haberse completado el proceso de registro de información, en el documento especificado para ese uso.

Art. 6 Dentro de las instalaciones de la unidad de informática, habrá un espacio dedicado única y exclusivamente al área de servidores, la cual se mantiene separado mediante una división de pared y protegido su acceso bajo llave y alarma.

Art. 7 Cualquier actividad anómala, efectuada dentro de las instalaciones físicas de procesamiento de información será cancelada en el momento en que se constatase la actividad.

Art.8 Al ingresar a las áreas de procesamiento de información, se da por aceptada la normativa de permanencia en las instalaciones, desarrollada bajo la política de acceso y permanencia a las áreas de procesamiento de datos.

Art. 9 Los equipos de oficina, como cafeteras, aires acondicionados, entre otros no deben estar conectados al mismo circuito que los sistemas informáticos.

Art. 10 Se hará una revisión periódica de los equipos de respaldo de energía o UPS, constatando su capacidad y correcto funcionamiento, se registrara cada revisión en una bitácora de control y funcionamiento de los equipos.

Art. 11 Los UPS son de uso exclusivo de cada estación de trabajo.

Art. 12 Es responsabilidad de los usuarios la correcta utilización de los UPS.

Art. 13 Al finalizar con la jornada laboral es necesario que cada usuario de las estaciones de trabajo verifique el apagado correctamente el equipo y dispositivo UPS.

Art. 14 Se debe efectuar una revisión periódica de los circuitos.

Art 15. La entidad deberá garantizar la seguridad física del centro de cómputo, para lo cual adecuará las oficinas con los materiales y la seguridad física necesaria que garantice la restricción a este lugar.

2.4.1.3. ACCESO Y PERMANENCIA EN EL CENTRO DE CÓMPUTO

Art. 1 Los encargados o administradores del centro de cómputo son los responsables del desarrollo de la normativa reguladora de las actividades en dicho centro.

Art. 2 Las normas desarrolladas para dicha instalación deberán estar en pleno acuerdo y relación, de las normas generales de seguridad informática.

Art. 3 El acceso del usuario al centro de cómputo, deberá tomarse como aceptación implícita de la normativa relacionada con dicha actividad.

2.4.2. ACTIVIDADES PROHIBITIVAS

Art. 1 Está prohibido el consumo de bebida(s) o alimento(s) de cualquier tipo en los lugares cercanos a los equipos de cómputo.

Art. 2 Se prohíbe a los usuarios utilizar equipos informáticos, herramientas o servicios provistos por la CRQ, para un objetivo distinto del que están destinadas o para beneficiar a personas ajenas a la institución.

Art. 3 No se deben alterar documentos, expedientes o registros, mediante tratamiento electrónico, proporcionando datos falsos, que pueden perjudicar la correcta operatividad de la Corporación Autónoma Regional del Quindío.

2.5. **SEGURIDAD LEGAL**

2.5.1. CONFORMIDAD CON LA LEGISLACIÓN

2.5.1.1. CUMPLIMIENTO DE REQUISITOS LEGALES

Art.1 Las acciones de los empleados de la Corporación Autónoma Regional del Quindío, referente a la utilización de software pirata dentro de las instalaciones de la CRQ, no son propias de la institución.

Art. 2 la institución se reserva todo derecho al utilizar software licenciado en sus equipos de producción, bajo ninguna circunstancia se aprueba la utilización de software sin licencia en la Entidad.

Art. 3 El área de sistemas, llevará un control detallado sobre los inventarios de software referente a sus licencias y contratos firmados para ser utilizados en la infraestructura tecnológica de la red institucional.

Art. 4 Las copias de los contratos de arrendamiento de software, será resguardado por el área de sistemas.

Art. 5 La institución no participa con sus empleados en la adquisición de software de forma no legal.

Art. 6 La institución no respalda que sus empleados puedan instalar software no licenciado en los equipos de trabajo, los cuales son propiedad exclusiva de la CRQ.

Art. 7 La institución deshecha por completo la utilización de software pirata o no licenciado, en las estaciones de trabajo, servidores, y equipo informático personalizado, que sea parte de sus inventarios informáticos.

Art. 8 El contrato de licencia de usuario final tanto de software comercial con derechos de copyright, como de software libre con derechos de copyleft, son respetados en su totalidad por la CRQ, sus empleados no pueden utilizar software de este tipo sin su respectiva licencia.

Art. 9 La institución a razón de seguridad de sus activos, realizará copias de seguridad de las unidades de software que le son licenciadas en el contrato de arrendamiento, con el objetivo de resguardar la licencia original y su medio físico.

Art. 10 Las copias que se hagan del software original serán que se utilicen para las instalaciones en toda la red institucional.

Art. 11 La transferencia de software comercial a terceros, es una actividad únicamente permisible, por un derecho concedido a la institución por el propietario intelectual del software o licencia en cuestión.

Art. 12 La institución no hace uso indebido de estas licencias, obteniendo provecho por su distribución si no es acordado por su contrato de licencia de derechos de autor.

Art. 13 El software libre, es regido por la licencia GPL (licencia Publica), y concedido a la institución con derechos de copyleft (comprende a un grupo de derechos de autor caracterizados por eliminar las restricciones de distribución o modificación impuestas por el copyright, con la condición de que el trabajo derivado se mantenga con el mismo régimen de derechos de autor que el original) , por tanto, no es permitido en ningún momento la distribución ilegal de este software, haciéndose acreedor la institución o empleados de los derechos de propiedad intelectual.

Art.14 Al laborar para la institución, cualquier información, código u otros, producida, mediante tratamiento electrónico dentro de sus instalaciones, es propiedad irrevocable de la CRQ

Art. 15 Ningún funcionario o contratista de la CRQ está facultado a obtener software para la institución, sino es mediante los canales de gestión necesarios.

Art. 16. Los supervisores de contratos de hardware, software y comunicaciones deberán informar al gestor de seguridad sobre los objetos y el desarrollo de estos y coordinar con este la implementación de las tecnologías contratadas.

Art.16. **Principios del tratamiento de datos personales:** Los siguientes son los principios que regirán el tratamiento de datos personales de las bases de datos institucionales y los contemplados en la Ley 1581 de 2012:

- Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
- Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento
- Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información

Área de Sistemas:

2.5.1.2. CUMPLIMIENTO TÉCNICO DE LA REVISIÓN Y ACTUALIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Art.1 La documentación de seguridad acá provista, podrá ser actualizada respetando todas y cada una de las políticas que demandan su correcto diseño y aplicabilidad.

Art.2 En ningún momento personal ajeno a los mencionados responsables de la actualización y aprobación de esta documentación, deberán ser designados como propietarios de los cargos de actualización y aprobación de los mismos, sin antes haber aprobado una preparación técnica para tales efectos.

Art. 3 El personal o usuarios de la red institucional deberán tener pleno conocimiento de la documentación de seguridad, apegarse a ella en todo caso o gestión.

Art. 4 El medio exclusivo de soporte para la seguridad en el tratamiento de la información de la institución, lo constituyen las políticas de seguridad informática y toda su reglamentación técnica, esto incluye un sistema de gestión de seguridad de la información.

Art. 5 Se iniciará proceso disciplinario, por incumplimiento de la normativa de seguridad informática o de protección de datos en los casos en los que el(los) problema(s) ocasionado(s), sea(n) crítico(s) y vital(es), para el correcto funcionamiento de la Corporación Autónoma Regional del Quindío.

Art.6 El único caso en el que personal ajeno o propio de la institución no será sancionado por violación a la seguridad informática de la institución, serán, los motivos previstos en la política de excepciones de responsabilidad.

2.5.1.3. NORMATIVA SOBRE AUDITORIAS A LOS SISTEMAS DE INFORMACIÓN

Art. 1 La ejecución de una auditoria a los sistemas informáticos, ameritará la planificación de esta, herramientas a utilizar en la auditoria, objetivos de la

auditoría, implicaciones legales, contractuales, requisitos y conformidad con la Dirección General.

Art. 2 De no existir personal técnicamente preparado para efectuar auditorías a la seguridad de la información, estos deberán ser capacitados por personal especializado en el área.

Art. 3 Salvo casos especiales toda auditoría, deberá estar respaldada por la Direccion General.

Art. 4 La implicación de casos especiales, en los cuales sea necesario de inmediato, amerita realizar auditorías sin una fecha planificada.

Art. 5 Sin importar la razón de la auditoría, se llevará un control exhaustivo, se tomará registro de cada actividad relaciona con ésta, quiénes la realizan, fechas, horas y todo lo que tenga que ver con la auditoría en sí.

Art. 6 El personal de auditoría no está facultado a realizar cambios en los sistemas informáticos, ya sea de los archivos que integran el sistema o de la información que en ellos se procesa.

Art. 7 Salvo caso especial, cualquier cambio efectuado al sistema de archivos, será motivo de sanción.

Art. 8 Las auditorías a los sistemas, serán realizadas con equipos móviles (Laptops) conectados a la red, en ningún momento el sistema de producción mantendrá instalado software para auditoría en su disco duro.

Art. 9 Toda aplicación para la auditoría será instalado correctamente y supervisado su uso, desde las terminales remotas en el mismo segmento de red.

3. RECOMENDACIONES

- Crear un Sistema de Gestión de Seguridad y privacidad de la Información, que supervise y normalice, toda actividad relacionada con la seguridad informática.

- Aprobar y poner en marcha el manual de políticas y normas de seguridad informática.

- Actualizar de forma constante, transparente y de acuerdo a las necesidades existentes al momento, el manual de normas y políticas de seguridad informática.

- Asignar presupuesto para la gestión de seguridad y privacidad de la información, independiente del proyecto para sistemas de información.

- Involucrar tanto personal técnico, como directivos de la institución, o a la Dirección General en temas de seguridad.

- Fijar objetivos para la salvaguarda de la información.

- Concienciar los usuarios, en temas de seguridad, hacerles sentirse responsables y parte de la institución.

- Dar seguimiento a estándares internacionales sobre temas de seguridad de la información.

- Realizar pruebas de intrusión, locales y externas por personal de la institución, de forma periódica.

- Contratar los servicios de terceros (Hacking ético), para ejecutar pruebas completas de intrusión a los sistemas de la red institucional.

- Capacitar los empleados de la institución, en temas de seguridad, adoptando un estricto control de las técnicas más comunes de persuasión de personal (Ingeniería Social).

- Contratar con empresas especializadas un estudio que nos indique el diagnostico de seguridad en la entidad y el plan de trabajo a seguir para reducir los riesgos informáticos en la entidad.

REFERENCIAS

Referencias Complementarias.

[1]. ISO/IEC 17799 Code of Best Practice for Information Security Management

[2]. Certified Information Systems Security Professional (CISSP)

[3]. RFC 1244, Site Security Handbook

[4]. Manual de Políticas y Seguridad Informática – Universidad de Oriente

[5]. Gobierno en Línea – Políticas de Seguridad Informática

[6]. Estándares de la ISO/IEC http://www.iso.org