

POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA



**GA-PR SOPORTE EN SISTEMAS
ÁREA DE SISTEMAS
Versión 2.0
2014**

I. INTRODUCCIÓN

Con la definición de las políticas y estándares de seguridad informática se busca establecer en el interior de la Corporación Autónoma Regional De Los Valles Del Sinú y San Jorge una cultura de calidad operando en una forma confiable.

La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de la Corporación Autónoma Regional De Los Valles Del Sinú y San Jorge en materia de seguridad.

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 de la información y los servicios prestados por la red a los usuarios finales.

El documento que se presenta como políticas de seguridad, pretende, ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la Corporación, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias.

Toda persona que utilice los servicios que ofrece la red y los dispositivos informáticos, 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.

En la actualidad la cultura informática que se ha creado como consecuencia de la mayor disponibilidad de recursos informáticos, ha creado nuevas necesidades y han hecho ver las posibilidades que se tienen al utilizar las herramientas computacionales para facilitar el cumplimiento misional de la CVS, pero también esta expansión ha mostrado que se debe hacerse de una manera planificada con el fin de optimizar los recursos en el presente y proyectarlos para que cumplan su objetivo final en el futuro.

En términos generales el manual de normas y políticas de seguridad informática, engloba los procedimientos más adecuados, tomando como lineamientos principales seis (6) criterios, que se detallan a continuación:

- Seguridad Institucional y Organizacional
- Seguridad física y del medio ambiente
- Seguridad lógica y control de acceso
- Manejo y control Centro de Cómputo
- Control de usuarios
- Lineamientos legales.

Seguridad Institucional y Organizacional

Dentro de este, se establece el marco formal de seguridad que debe sustentar la Corporación, 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 Física y Del Medio Ambiente

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 y cuidando el entorno y el medio ambiente donde se labora o se realizan las actividades diarias.

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 la gestión de soporte en 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 Manejo y Control Centro de Cómputo

Aquí se dan el conjunto de métodos, documentos, programas y dispositivos físicos destinados a lograr que los recursos de cómputos disponibles sean administrados de buena forma en un ambiente dado, sean accedidos y exclusivamente por quienes tienen la autorización para hacerlo. Por ser este el núcleo de la organización su principal objetivo es satisfacer las necesidades de la información de la Corporación de manera veraz, oportuna, y en tiempo y forma.

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 en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país y contrataciones externas.

II. GENERALIDADES

INTRODUCCIONES DE INTERPRETACION

La información presentada como normativa de seguridad, ha sido organizada de manera sencilla para que pueda ser interpretada por cualquier persona independientemente del rango o tipo de vinculación laboral que preste a la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS, con conocimientos informáticos o sin ellos.

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC's de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el Área de Sistemas.

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge – CVS. Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por el **Área de Sistemas** al personal, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

EVALUACION DE LAS POLITICAS

Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

BENEFICIOS

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC's) en la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge – CVS.

ESQUEMA

El esquema de presentación del documento trata específicamente de las políticas de seguridad, las cuales están organizadas por los seis niveles anteriormente descritos estableciendo cada política dentro del dominio CVS.

Los niveles de seguridad fueron organizados constatando un enfoque objetivo de la situación real de la Corporación, 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

- Seguridad Ligada al Personal
 - Capacitación de Usuarios
 - Respuestas a Incidentes y Anomalías de Seguridad

❖ Nivel de Seguridad Física y Del Medio Ambiente:

- Seguridad Física
- Seguridad Física y Ambiental
- Seguridad de los Equipos

- Controles Generales

❖ **Nivel de Seguridad Lógico:**

- Control de Accesos
- Administración del Acceso de Usuarios
- Seguridad en Acceso de Terceros
- Control de Acceso a la Red
- Control de Acceso a las Aplicaciones
- Monitoreo del Acceso y Uso del Sistema.

❖ **Nivel de Seguridad Manejo y Control Centro de Cómputo:**

- Políticas del Centro de Cómputo
- Uso de Medios de Almacenamiento
- Adquisición de Software
- Licenciamiento de Software
 - Identificación de Incidentes.

❖ **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 Corporación, 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 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.

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 organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

*Por el desarrollo sostenible
del departamento de Córdoba*

IMPORTANCIA DE LOS MANUALES DE NORMAS Y POLÍTICAS

Como parte integral de un Sistema de Gestión de Seguridad 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. 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. 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

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 en concordancia con las autoridades de nivel superior.

COORDINADOR DE SISTEMAS

Persona dotada de conciencia técnica, 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.

CORPORACION
AUTONOMA REGIONAL
DE LOS VALLES DEL
SINU Y DEL SAN JORGE
UNIDAD DE SISTEMAS

Entidad o Departamento dentro de la Corporación, 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.

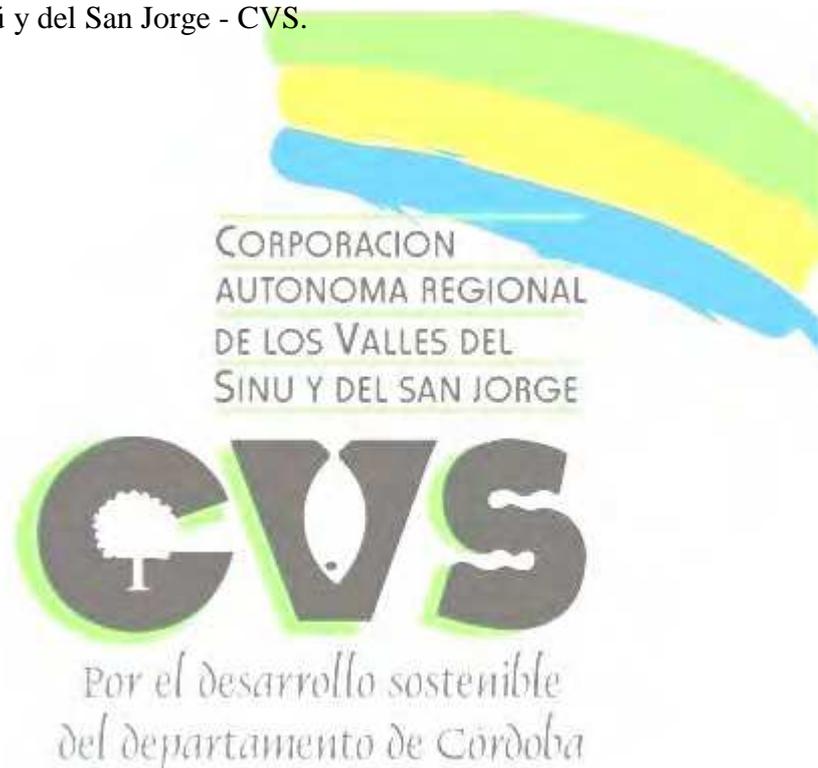
Por el desarrollo sostenible
del departamento de Córdoba

RESPONSABLE DE ACTIVOS

Personal dentro de los diferentes departamentos administrativos 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. (Líderes de Procesos).

III. MARCO LEGAL

La elaboración del manual de normas y políticas de seguridad informática, está fundamentado bajo la norma ISO/IEC 17799, unificada al manual interno de trabajo y el manual de normas y políticas de recurso humano de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS.



IV. 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 la alta dirección de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS. Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la Corporación, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica de la Red Institucional.



V. 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 de los Valles del Sinú y del San Jorge - CVS.

VI. 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 desarrollados para tal fin.



VII. 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 de los Valles del Sinú y del San Jorge - CVS.

El ente que garantizará la ejecución y puesta en marcha de la normativa y políticas de seguridad, estará bajo el cargo del proceso **GESTIÓN DE SOPORTE EN SISTEMAS**, siendo el responsable absoluto de la supervisión y cumplimiento, el **Coordinador de Sistemas**, supervisados por la Subdirección de Planeación.



VIII. GLOSARIO DE TERMINOS

Activo: Es el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la Corporación. 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 Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS, a través de terminales o equipos remotos, físicamente separados del usuario final.

Amenaza: Es un evento que puede desencadenar un incidente en la empresa, 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.

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

Impacto: consecuencia de la materialización de una amenaza.

ISO: (Organización Internacional de Estándares) Corporación 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: (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 Corporación.

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

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

SGSI: Sistema de Gestión de Seguridad 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 Corporación.

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

Terceros: proveedores de software, que tengan convenios o profesionales con la Corporación.

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

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



1. POLITICA DE SEGURIDAD INFORMÁTICA

1.1. OBJETIVO

Dotar de la información necesaria en el más amplio nivel de detalle a los usuarios, empleados y gerentes de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS, 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 de los Valles del Sinú y del San Jorge - CVS, así como la información que es procesada y almacenada en estos.

1.2. DESARROLLO GENERAL

1.2.1 APLICACIÓN

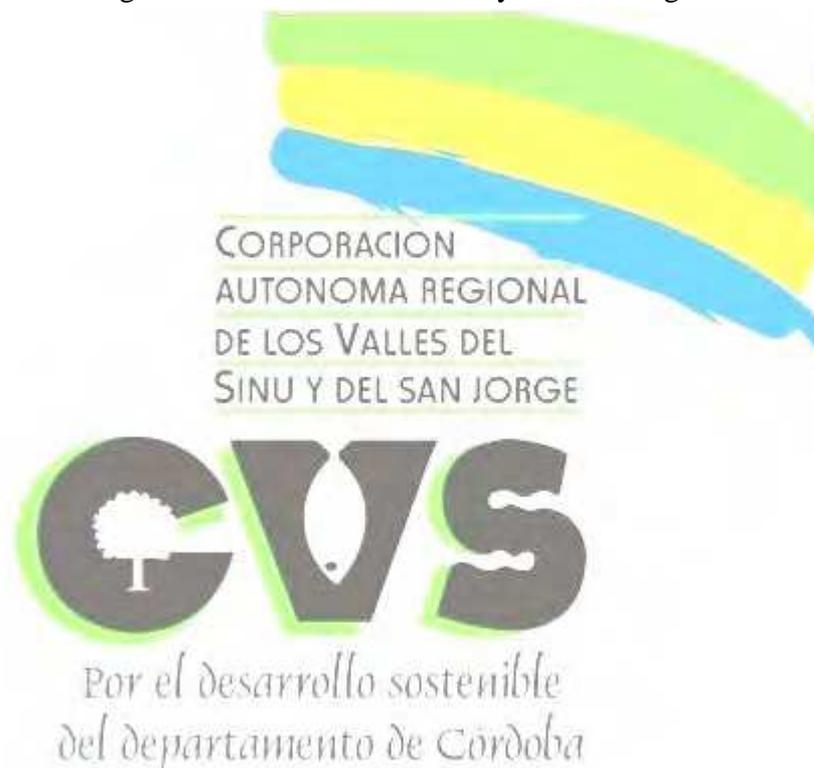
Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC's de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el Área de Sistemas. También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS. Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por el Área de Sistemas personal, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

1.2.2 EVALUACION DE LA POLITICA

Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias.

1.2.2 EVALUACION DE LA POLITICA

Las políticas y estándares de seguridad informática establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información de las Tecnologías de Información y Comunicaciones (TIC's) en la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS.



Nivel 1: SEGURIDAD ORGANIZATIVA

1.2. SEGURIDAD ORGANIZACIONAL

1.2.1. POLÍTICAS DE SEGURIDAD

- Los servicios de la red institucional son de exclusivo uso académico, de investigación, técnicos y para gestiones administrativas, cualquier cambio en la normativa de uso de los mismos, será expresa y adecuada como política de seguridad en este documento.
- La Dirección de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS delegara al proceso **GS-GESTIÓN DE SOPORTE EN SISTEMAS** para que de seguimiento al cumplimiento de la normativa y propicie el entorno necesario para crear un SGSI, el cual tendrá entre sus funciones:
 - a) Velar por la seguridad de los activos informáticos
 - b) Gestión y procesamiento de información.
 - c) Cumplimiento de políticas.
 - d) Elaboración de planes de seguridad.
 - e) Capacitación de usuarios en temas de seguridad.
 - f) Gestionar y coordinar esfuerzos, 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 adelante ante cualquier eventualidad que se presente.
 - g) Informar sobre problemas de seguridad a la alta gerencia.
 - h) Poner especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.
 - i) El Líder de proceso de cada unidad organizativa dentro de la red institucional es el responsable de las actividades procedentes de sus acciones.
 - j) El administrador de sistemas es el encargado de mantener en buen estado los servidores dentro de la red institucional.

k) Toda persona que ingresa como usuario nuevo de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

l) Todo el personal nuevo de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS, deberá ser notificado al o Área de Sistemas, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo, Cuentas de correos Institucional) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

m) Todo usuario de la red institucional de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS, 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 Corporación.

n) Los usuarios tendrán el acceso a Internet, 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.

1.2.2. EXCEPCIONES DE RESPONSABILIDAD

- a) 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 Corporación o sus allegados.
- b) 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 la subdirección de planeación y supervisadas por la unidad de sistemas, con la documentación necesaria para el caso, siendo la gerencia quien dé por sentada su aprobación final.



1.2.3. CLASIFICACIÓN Y CONTROL DE ACTIVOS

1.2.3.1. RESPONSABILIDAD POR LOS ACTIVOS

- ✓ Cada área, tendrá un responsable por el/los activo/s crítico/s o de mayor importancia para la corporación.
- ✓ La persona responsable de los activos de cada unidad organizativa o área de trabajo, velará por la salvaguarda de los activos físicos (hardware y medios magnéticos, aire acondicionado, mobiliario.), activos de información (Bases de Datos, Archivos, Documentación de sistemas, Procedimientos Operativos, configuraciones), activos de software aplicaciones, software de sistemas, herramientas y programas de desarrollo).
- ✓ Los administradores de los sistemas son los responsables de la seguridad de la información almacenada en esos recursos.

1.2.3.2. CLASIFICACIÓN DE LA INFORMACIÓN

- ✓ De forma individual, los departamentos de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS, son responsables, de clasificar de acuerdo al nivel de importancia, la información que en ella se procese.
- ✓ Se tomarán como base, los siguientes criterios, como niveles de importancia, para clasificar la información:
 - a) PUBLICA
 - b) INTERNA
 - c) CONFIDENCIAL.
- ✓ Los activos de información de mayor importancia para la Corporación deberán clasificarse por su nivel de exposición o vulnerabilidad.

1.2.4. SEGURIDAD LIGADA AL PERSONAL

Referente a contratos:

- ✓ Se entregará al contratado, toda la documentación necesaria para ejercer sus labores dentro de la Corporación, en el momento en que se de por establecido su contrato laboral.

El empleado:

- ✓ La información procesada, manipulada o almacenada por el empleado es propiedad exclusiva de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS.
- ✓ Es responsabilidad de los empleados de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Empleados del presente Manual.
- ✓ La Corporación Autónoma Regional de los Valles del Sinú y del San Jorge- CVS no se hace responsable por daños causados provenientes de sus empleados a la información o activos de procesamiento, propiedad de la Corporación, daños efectuados desde sus instalaciones de red a equipos informáticos externos.

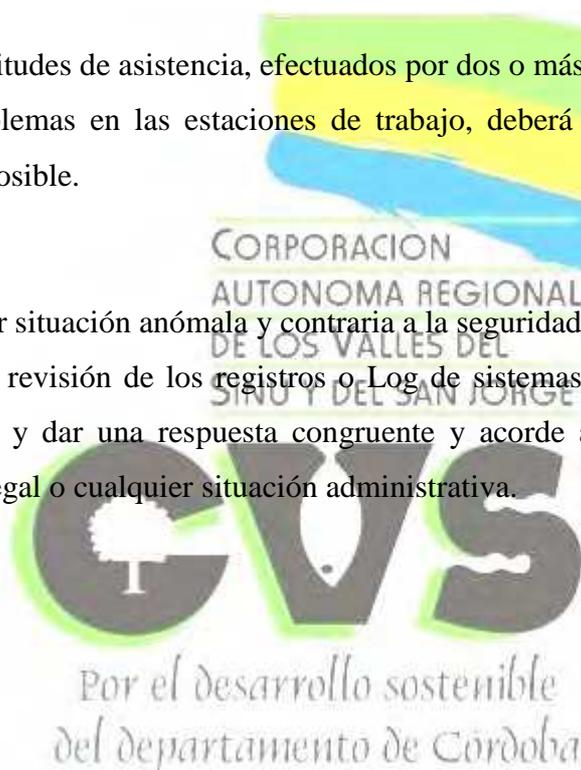
1.2.4.1. CAPACITACIÓN DE USUARIOS

- ✓ Los usuarios de la red institucional, serán capacitados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.
- ✓ Todo servidor o funcionario nuevo en la Corporación deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.
- ✓ Se deben tomar todas las medidas de seguridad necesarias, antes de realizar una capacitación a personal ajeno o propio de la Corporación, siempre y cuando se vea

implicada la utilización de los servicios de red o se exponga material de importancia considerable para la Corporación.

1.2.4.2. RESPUESTAS A INCIDENTES Y ANOMALÍAS DE SEGURIDAD

- ✓ Se realizarán respaldos de la información, diariamente, para los activos de mayor importancia o críticos, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado semestralmente, el cual deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria.
- ✓ Las solicitudes de asistencia, efectuados por dos o más empleados o áreas de proceso, con problemas en las estaciones de trabajo, deberá dárseles solución en el menor tiempo posible.
- ✓ 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 : SEGURIDAD LÓGICA

1.3. SEGURIDAD LOGICA

POLÍTICAS DE SEGURIDAD

Cada usuario y funcionario son responsables de los mecanismos de control de acceso que les sean proporcionado; esto es, de su “ID” login de usuario y contraseña necesarios para acceder a la red interna, aplicativos y correos institucionales y a la infraestructura tecnológica La Corporacion Autónoma Regional de los Valles del Sinú y del San Jorge- CVS por lo que se deberá mantener de forma confidencial.

1.3.1. CONTROL DE ACCESOS

- ✓ El Coordinador de sistemas proporcionará toda la documentación necesaria para agilizar la utilización de los sistemas, referente a formularios, guías, controles, otros, localizados en el sistema de gestión de la calidad de la corporación.
- ✓ Cualquier petición de información, servicio o acción proveniente de un determinado usuario o líder de proceso, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por la Corporación, 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, mismo será realizado por la persona o el departamento al cual le es solicitado el servicio.
 - c) Sanciones aplicables por autoridades de nivel superior, previamente discutidas con el comité de seguridad.

1.3.1.1. ADMINISTRACIÓN DEL ACCESO DE USUARIOS

- ✓ Son usuarios de la red institucional los empleados de planta, administrativos, secretarías, contratistas, y toda aquella persona, que tenga contacto directo y utilice los servicios de la red institucional de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS.

- ✓ Se asignará una cuenta de acceso a los sistemas de la intranet, a todo usuario de la red institucional, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que este accederá, junto a la información personal del usuario.

- ✓ Los usuarios externos, son usuarios limitados, estos tendrán acceso únicamente a los servicios de Internet y recursos compartidos de la red institucional, cualquier cambio sobre los servicios a los que estos tengan acceso, será motivo de revisión y modificación de esta política, adecuándose a las nuevas especificaciones.

- ✓ Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con la Corporación fuera del ámbito de empleado/contratista y siempre que tenga una vinculación con los servicios de la red institucional.

- ✓ 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 Corporación y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

- ✓ No se proporcionará el servicio solicitado por un usuario, o área de trabajo, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución según el sistema de gestión de la calidad.

- ✓ 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, siempre y cuando se muestre un documento de identidad personal.
- ✓ La longitud mínima de caracteres permisibles en una contraseña se establece en 6 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales.
- ✓ La longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

1.3.1.2. RESPONSABILIDADES DEL USUARIO

- ✓ El usuario es responsable exclusivo de mantener a salvo su contraseña.
- ✓ El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios, so pena de incurrir en una denuncia penal por mal uso de los servicios informáticos de la corporación.
- ✓ 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.
- ✓ El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Administrador de la red, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.
- ✓ 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.

- ✓ El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en el, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.
- ✓ Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos de la Corporación, está obligado a reportarlo a los administradores del sistema o gestor de seguridad.

Uso de correo electrónico(CORREO INSTITUCIONAL):

- ✚ El servicio de correo electrónico, es un servicio gratuito, y no garantizable, se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.
- ✚ El correo electrónico es de uso exclusivo, para los empleados y contratistas de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge - CVS.
- ✚ Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.
- ✚ El usuario será responsable de la información que sea enviada con su cuenta.
- ✚ El Administrador de la red corporativa, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.
- ✚ 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.

- ✚ El usuario debe tener en cuenta que el correo institucional por capacidad solo envía archivos de capacidad máximo de 10 MB por lo que hace no optimo el envío del mismo; como también es responsabilidad del usuario hacerle el mantenimiento periódico de su cuenta como borrar archivos demasiado viejos (historial), carpetas enviadas, temporales etc.

Uso de mensajero interno cvs (SPARK):

- ✚ El servicio de mensajería interna (spark) se creó en la Corporación con el fin de agilizar la comunicación entre Sedes y Dependencias adscritas a la Corporación; además de esto es un fundamental entre la comunicación de funcionarios de la misma.
- ✚ La creación de cuentas y usuarios para acceder a este servicio debe ser supervisada y aprobada por el Área de sistemas para sus fines pertinentes.
- ✚ Todo uso indebido del servicio de mensajería interna (spark) será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.
- ✚ Las cuentas de mensajería de la modalidad de PRACTICANTES-PASANTES dentro de la Corporación se le creará una cuenta referenciando el área hacen sus actividades y proporcional al número de practicantes asignados al donde Área previo consentimiento del Área de Sistemas.
- ✚ El usuario será responsable de la información que sea enviada con su cuenta.
- ✚ El Administrador de la red corporativa, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.

Uso del Servicio de Internet:

- ✚ El acceso a Internet provisto a los usuarios y funcionarios de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

- ✚ Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el Área de Sistemas.

- ✚ Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:
 - *Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.*
 - *Saben que existe la prohibición de descarga de software sin la autorización del Área de Sistemas.*
 - *La utilización de Internet es para el desempeño de sus funciones y cargo en Corporación Autónoma Regional de los Valles del Sinú y del San Jorge y no para propósitos personales.*

- ✓ El acceso a Internet puede ser Gestionado, limitado y Personalizado por el Área de Sistemas siempre y cuando la situación lo amerite y casos especiales de trabajo para los usuarios y funcionarios de Corporación Autónoma Regional de los Valles del Sinú y del San Jorge. Es decir se pueden bloquear y denegar algunos accesos a paginas para Optimizar el ancho de banda de Internet para su total aprovechamiento.

1.3.1.3. SEGURIDAD EN ACCESO DE TERCEROS

- ✓ 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.
- ✓ 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 del mismo.
- ✓ Los servicios accedidos por terceros acatarán las disposiciones generales de acceso a servicios por el personal interno de la Corporación, además de los requisitos expuestos en su contrato/convenio con la Corporación.

1.3.1.4. CONTROL DE ACCESO A LA RED

Unidad de Sistemas y afines a ella.

- ✓ 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.
- ✓ Se debe eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo implicado en el proceso.
- ✓ 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 auditoría de seguridad.

- ✓ El departamento 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.
- ✓ Los accesos a la red interna o local desde una red externa de la Corporación o extranet, se harán mediante un mecanismo de autenticación seguro y el tráfico entre ambas redes o sistemas será cifrado con una encriptación de 128 bits.
- ✓ Se registrara todo acceso a los dispositivos de red, mediante archivos de registro o Log, de los dispositivos que provean estos accesos.
- ✓ Se efectuara una revisión de Log de los dispositivos de acceso a la red en un tiempo máximo de 48 horas.

Uso de Unidad de Almacenamiento (Carpeta Pública):

- ✓ Es un servidor localizado en la oficina de sistemas que tiene un directorio compartido en la red (\\servidor\publica), para la utilización de espacio virtual en forma general por todos en la corporación. Este espacio es limitado ya que la capacidad de almacenamiento del disco duro en ese servidor es de 824 GB.
- ✓ La información contenida en este directorio es responsabilidad del usuario a quien pertenece, por lo tanto se debe de tener copias de seguridad de la misma en el equipo local que usa para en caso de pérdida poder ser recuperada. El Área de sistemas no se hace responsable de la información y pérdida contenida en esta carpeta, ya que se está depurando constantemente para su buen uso y excelente funcionamiento.
- ✓ Solo se realizan copias de seguridad a los directorios críticos. (SGC), las otras copias de seguridad en este directorio son realizadas por petición de los usuarios.

- ✓ No es permitido tener en el directorio pública, debido al poco espacio disponible: instaladores de programas que no estén debidamente licenciados Archivos MP3, Fotos digitales y videos que no sean de uso corporativo. Al ser detectados en la red, estos se procederán a borrar, previo aviso al usuario en la cual reposa esta información.

- ✓ La estructura general del directorio pública debe ser respetada para mantener una organización optima del mismo, en tal caso de que si se encuentra algún archivo fuera de los directorios asignados, este será movido a el directorio llamado Raíz de publica y posteriormente eliminado.

- ✓ El usuario en la corporación puede tener música, videos, fotos en los computadores de uso diario, hasta 30GB, pero al momento de estos hacerle mantenimiento esta información debe estar separada de usada para fines corporativos para que se le realice copia de seguridad, con esto se garantiza que solo los datos pertenecientes a la información de la corporación es guardada sin llevar datos adicionales.

1.3.1.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO

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

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

Servidores

- ✓ El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario administrador.
- ✓ Los administradores de servicios, tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.
- ✓ Todo servicio provisto o instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas, en ningún momento se obviarán situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.

1.3.1.6. CONTROL DE ACCESO A LAS APLICACIONES

- ✓ Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso específicas para cada usuario del entorno operativo de la aplicación, y los diferentes accesos a los módulos permitidos.
- ✓ Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo al 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.
- ✓ 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.

- ✓ 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.
- ✓ 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.

Uso de Aplicaciones:

- ✓ El uso de los programas que actualmente existen en la Corporación (SICOF, QFDocument, SIA, Gtasas). Son aplicativos adquiridos por la empresa y por ende tiene su garantía se soporte por las personas que suministraron dichos Software; son estas personas las encargadas de darle el soporte y los cambios necesarios para que funcionen correctamente, solo la Corporación brinda la infraestructura Hardware (Servidores, PC, Red de Datos) y el Área de sistemas es un apoyo de soporte del mismo a los usuarios que trabajan sobre las aplicaciones.
- ✓ El acceso a estas aplicaciones solo se le dará a los funcionarios y usuarios que la dirección o responsables del sistema informático así lo amerite para su funcionamiento y trabajo sobre él.
- ✓ A estos aplicativos se le hace copias de seguridad diarias y programadas para que en caso de una anomalía puede restablecerse el sistemas.

1.3.1.7. MONITOREO DEL ACCESO Y USO DEL SISTEMA

- ✓ 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.
- ✓ Los archivos de 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.
- ✓ Se efectuará una copia automática de los archivos de Log, y se conducirá o enviara hacia otra terminal o servidor, evitando se guarde la copia localmente donde se produce.

1.3.2. GESTIÓN DE OPERACIONES Y COMUNICACIONES

1.3.2.1. RESPONSABILIDADES Y PROCEDIMIENTOS OPERATIVOS

- ✓ El personal administrador de algún servicio, es el responsable absoluto por mantener en óptimo funcionamiento ese servicio, coordinar esfuerzos con el coordinador de sistemas, para fomentar una cultura de administración segura y servicios óptimos.
- ✓ Las configuraciones y puesta en marcha de servicios, son normadas por el departamento de informática.
- ✓ 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.

1.3.2.2. PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

- ✓ La unidad 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.

- ✓ La aceptación del software se hará efectiva por la Gerencia de la Corporación, previo análisis y pruebas efectuadas por el personal de informática.
- ✓ Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad.
- ✓ 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 los mismos.
- ✓ 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.
- ✓ 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.
- ✓ Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.
- ✓ Cualquier prueba sobre los sistemas, del ámbito a la que esta se refiera deberá ser documentada y cualquier documento o archivo que haya sido necesario para su ejecución deberá ser borrado de los dispositivos físicos, mediante tratamiento electrónico.

1.3.2.3. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

- ✓ Se adquirirá y utilizará software únicamente de fuentes confiables.
- ✓ En caso de ser necesaria la adquisición de software de fuentes no confiables, este se adquirirá en código fuente.
- ✓ Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

1.3.2.4. MANTENIMIENTO

- ✓ El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal que suministro o se le adjudico el contrato del mismo en caso de que sea software adquirido por esta modalidad; la unidad de informática, o del personal de soporte técnico hará el acompañamiento del mismo y apoyo al proceso de mantenimiento.
- ✓ El cambio de archivos de sistema, no es permitido, sin una justificación aceptable y verificable por el gestor de seguridad.
- ✓ Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación. Estos mantenimientos están programados 2 veces al año y se efectúan en todos los equipos informáticos de la Corporación.

1.3.2.5. MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

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

- ✓ 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.
- ✓ Todo medio de almacenamiento con información crítica será guardado bajo llave en una caja especial a la cual tendrá acceso únicamente, el gestor de seguridad o la gerencia administrativa, esta caja no debería ser removible, una segunda copia será resguardada por un tercero, entidad financiera o afín.
- ✓ Se llevará un control, en el que se especifiquen los medios de almacenamiento en los que se debe guardar información.

Nivel 3: SEGURIDAD FÍSICA

1.4.1. SEGURIDAD FÍSICA Y AMBIENTAL

1.4.1.1. SEGURIDAD DE LOS EQUIPOS

- ✓ El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.
- ✓ Los servidores, sin importar al dominio o grupo de trabajo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.
- ✓ 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 administrador y las personas responsables por esos activos, quienes deberán poseer su debida identificación.

1.4.1.2. CONTROLES GENERALES

- ✓ 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.
- ✓ El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.
- ✓ Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.
- ✓ 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.
- ✓ Deberá llevarse un control exhaustivo del mantenimiento preventivo y otro para el mantenimiento correctivo que se les haga a los equipos.
- ✓ 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.
- ✓ Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\.

- ✓ Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- ✓ Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación al Área de Sistemas a través de un plan detallado.
- ✓ Queda terminantemente prohibido que el usuario o funcionario distinto al personal al Área de Sistemas abra o destape los equipos de cómputo.
- ✓ Toda visita a las oficinas de tratamiento de datos críticos e información (unidad de informática, sala de servidores entre otros) deberá ser registrada.
- ✓ La sala o cuarto de servidores, deberá estar separada de las oficinas administrativas de la unidad de informática o cualquier otra unidad, departamento o sala de recepción del personal, mediante una división en la unidad de informática, 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.
- ✓ 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.
- ✓ 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.
- ✓ 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.

- ✓ Las salas o instalaciones físicas de procesamiento de información deberán poseer información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.
- ✓ Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Área de Sistemas, en caso de requerir este servicio deberá solicitarlo.

Mantenimiento de equipos

- Únicamente el personal autorizado por el Área de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.
- Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.
- El servicio técnico y de soporte diario solo lo deben realizar las personas pertenecientes al Área de Sistemas de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge.
- Los soportes diarios y servicio técnico se relacionan en el formato GA-FO-24 del SISTEMA INTEGRADO DE GESTIÓN CALIDAD proceso GA-PR-02 SOPORTE SISTEMAS.
- Se realizan 2 Mantenimientos anuales y Copias Backup en la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge; dicho procedimiento también se relaciona en el formato GA-FO-28 y Programación del mismo GA-FO-29.

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:

- ✓ La Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, se reserva el derecho de respaldo, a cualquier miembro usuario de la red, o miembro de las áreas administrativas, ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.
- ✓ Todo el software comercial que utilice la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, deberá estar legalmente registrado, en los contratos de arrendamiento de software con sus respectivas licencias.
- ✓ La adquisición de software por parte de personal que labore en la Corporación, no expresa el consentimiento de la Corporación, la instalación del mismo, no garantiza responsabilidad alguna para la Corporación, por ende la Corporación no se hace responsable de las actividades de sus empleados.
- ✓ Tanto el software comercial como el software libre son propiedad intelectual exclusiva de sus desarrolladores, la Corporación respeta la propiedad intelectual y se rige por el contrato de licencia de sus autores.
- ✓ El software comercial licenciado a la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, es propiedad exclusiva de la Corporación, 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.

- ✓ 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, con el apoyo de la unidad de bienes y suministros.
- ✓ 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.
- ✓ El software desarrollado internamente, por el personal que labora en la Corporación es propiedad exclusiva de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge.
- ✓ 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.
- ✓ 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.

1.5.1.2. REVISIÓN DE POLÍTICAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

- ✓ Toda violación a las políticas de licenciamiento de software, será motivo de sanciones aplicables al personal que incurra en la violación.
- ✓ El documento de seguridad será elaborado y actualizado por el Coordinador de Sistemas, su aprobación y puesta en ejecución será responsabilidad de la gerencia administrativa.
- ✓ Cualquier violación a la seguridad por parte del personal que labora, para la Corporación, así como terceros que tengan relación o alguna especie de contrato con la Corporación se harán acreedores a sanciones aplicables de ley.

1.5.1.3. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS

- ✓ Se debe efectuar una auditoria de seguridad a los sistemas de acceso a la red, semestral, 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.
- ✓ Toda auditoria a los sistemas, estará debidamente aprobada, y tendrá el sello y firma de la gerencia.
- ✓ Cualquier acción que amerite la ejecución de una auditoria a los sistemas informáticos deberá ser documentada y establecida su aplicabilidad y objetivos de la misma, así como razones para su ejecución, personal involucrada en la misma y sistemas implicados.
- ✓ La auditoria 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.
- ✓ 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 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 de los Valles del Sinú y del San Jorge.

2.2. SEGURIDAD ORGANIZACIONAL

2.2.1. EN CUANTO A POLÍTICAS GENERALES DE SEGURIDAD

Unidad de Informática:

- ✚ El usuario acatará las disposiciones expresas sobre la utilización de los servicios informáticos de la red institucional.
- ✚ El administrador hará respaldos periódicos de la información así como la depuración de los discos duros.
- ✚ El 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.
- ✚ El administrador decidirá, sobre el uso de los recursos del sistema restricción de directorios y programas ejecutables para los usuarios.
- ✚ 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.

- ✚ El administrador de sistemas, dará de alta y baja a usuarios y revisará las cuentas periódicamente para estar seguros de que no hay usuarios ficticios.
- ✚ Recomendar sobre el uso e implementación de nuevas tecnologías para administración de los sistemas y la red.
- ✚ Reportar a la alta dirección, las fallas en el desempeño de la red. Solucionar los problemas que se generen en su red local.
- ✚ La Corporación 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.
- ✚ El Administrador monitoreará las acciones y tareas de los usuarios de la red institucional.
- ✚ Se prestará el servicio de Internet, siempre que se encuentren presentes los requisitos de seguridad mínimos.
- ✚ El usuario no tiene derecho sobre el servicio de Internet sino es mediante la aceptación de la normativa de seguridad.
- ✚ Se suspenderá cualquier usuario que utilice los computadores fuera del ámbito institucional, y los objetivos para los que estos fueron creados.

2.2.2. EXCEPCIONES DE RESPONSABILIDAD

- ✚ La Corporación debe establecer con sus empleados un contrato de confidencialidad de común acuerdo.
- ✚ Toda acción debe seguir los canales de gestión necesarios para su ejecución.
- ✚ La alta gerencia, proveerá la documentación necesaria para aprobar un acuerdo de no responsabilidad por acciones que realicen dentro de la red institucional.
- ✚ Las gestiones para las excepciones de responsabilidad son acordadas bajo común acuerdo de la gerencia y el comité de seguridad.

2.2.3. CLASIFICACIÓN Y CONTROL DE ACTIVOS

2.2.3.1. RESPONSABILIDAD POR LOS ACTIVOS

- ✚ La dirección nombrará un responsable de activos en cada departamento de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge.
- ✚ Los líderes de proceso de cada departamento de la Corporación, son responsables de mantener o proteger los activos de mayor importancia.

2.2.3.2. CLASIFICACIÓN DE LA INFORMACION

- ✚ Cada líder de proceso dará importancia a la información en base al nivel de clasificación que demande el activo.
- ✚ La información pública puede ser visualizada por cualquier persona dentro o fuera de la Corporación.
- ✚ La información interna, es propiedad del contratista y de la Corporación, en ningún momento intervendrán personas ajenas a su proceso o manipulación. La información confidencial es propiedad absoluta de la Corporación, el acceso a ésta es permitido únicamente a personal administrativo.
- ✚ Los niveles de seguridad se detallan como nivel de seguridad bajo, nivel de seguridad medio y nivel de seguridad alto.

2.2.4. SEGURIDAD LIGADA AL PERSONAL

Referente a contratos.

- ✚ Todo empleado ejercerá las labores estipuladas en su contrato de trabajo.
- ✚ El empleado no tiene ningún derecho sobre la información que procese dentro de las instalaciones de la red institucional.
- ✚ La información que maneja o manipula el empleado, no puede ser divulgada a terceros o fuera del ámbito de laboral.
- ✚ El usuario se norma por las disposiciones de seguridad informática de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge.
- ✚ Los usuarios son responsables de las acciones causadas por sus operaciones con el equipo de la red institucional.

2.2.4.1. CAPACITACIÓN DE USUARIOS

- ✚ El comité de seguridad capacitará los usuarios de la red institucional, por departamentos.
- ✚ El comité de seguridad proporcionará las fechas en que se impartirán las capacitaciones.
- ✚ El material de apoyo (manuales, guías, etc.) será entregado minutos antes de iniciar la capacitación, en la sala donde será efectuada la capacitación.
- ✚ En cada capacitación se revisarán los dispositivos de conexión de servicios involucrados en la capacitación.

- ✚ Las capacitaciones deben realizarse fuera de áreas de procesamiento de información.
- ✚ 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.

2.2.4.2. RESPUESTA A INCIDENTES Y ANOMALIAS DE SEGURIDAD

- ✚ Los respaldos de información deberán ser almacenados en un sitio aislado y libre de cualquier daño o posible extracción por terceros dentro de la Corporación.
- ✚ Los respaldos se utilizarán únicamente en casos especiales ya que su contenido es de suma importancia para la Corporación.
- ✚ La Corporación debe contar con respaldos de la información ante cualquier incidente.
- ✚ Generar procedimientos manuales de respaldo de información.
- ✚ La unidad de informática tendrá la responsabilidad, de priorizar una situación de la otra en cuanto a los problemas en las estaciones de trabajo.
- ✚ En situaciones de emergencia que impliquen áreas como atención al cliente entre otros, se da prioridad en el orden siguiente:
 - a) Área Financiera
 - b) Área Planeación
 - c) Área Administrativa.
 - d) Área Jurídica., etc.
- ✚ El documento de seguridad se elaborará, tomando en cuenta aspectos basados en situaciones pasadas, y enmarcarlo en la pro actividad de situaciones futuras.
- ✚ Se prioriza la información de mayor importancia para la Corporación.
- ✚ Se evacua la información o activo de los niveles confidenciales de la Corporación.
- ✚ Respaldo los archivos de logs o registro de los sistemas en proceso, cada cierto tiempo durante el día.
- ✚ 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

- ✚ La documentación de seguridad será resguardada por el Administrador, esto incluye folletos, guías, formularios, controles entre otros.
- ✚ La elaboración de la documentación relacionada con formularios, guías, etc. Será elaborada por el sistema de gestión corporativo en colaboración con el coordinador de sistemas.
- ✚ Los canales de gestión y seguimiento para realizar acciones dentro de la red institucional, no pueden ser violentados bajo ninguna circunstancia.
- ✚ El personal encargado de dar soporte a la gestión de comunicaciones entre servicios y la prestación del mismo, no está autorizado a brindar ninguna clase de servicios, mientras no se haya seguido todos y cada uno de los canales de gestión necesarios, procedimientos enmarcados en el sistema de gestión de la calidad.

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

- ✚ Sin excepción alguna se consideran usuarios de la red institucional de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge todos y cada uno del personal que se encuentra denotado en la política de administración de acceso de usuarios.
- ✚ El acceso a los sistemas y servicios de información, es permitido únicamente a los usuarios que dispongan de los permisos necesarios para su ejecución. El usuario deberá proveer toda la información necesaria para poder brindarle los permisos necesarios para la ejecución de los servicios de la red institucional.
- ✚ Las necesidades y aprobación de acceso, de los usuarios a los servicios de la red institucional, deberá ser documentada y actualizada su información, en la política que norma su uso.

- ✚ La vinculación de servicios por parte de terceros con la red institucional, es característica propia del personal en outsourcing, contratistas, proveedores de software.
- ✚ La identificación del usuario se hará a través del formulario que le proporcionara el Administrador, y se autenticara, mediante la firma impresa de la persona que tendrá acceso al sistema o se acreditará con su cuenta de usuario.
- ✚ Cualquier petición de servicio, por parte de personal de la Corporación o ajeno a la misma, no se concederá sino es mediante la aprobación de la política de acceso y prestación de servicio.
- ✚ La cuenta temporal es usada únicamente con propósitos legales y de ejecución de tareas, por olvido de la información de la cuenta personal.
- ✚ La cuenta temporal es únicamente acreditable, si se proporciona la información necesaria para su uso.
- ✚ Toda cuenta nula u olvidada, se eliminara del/los sistema/s, previa verificación o asignación de una nueva cuenta, al usuario propietario de la cuenta a eliminar.
- ✚ El sistema no aceptará contraseñas con una longitud menor a la expresada en la política de creación de contraseñas.
- ✚ El usuario se responsabiliza en crear una contraseña fuerte y difícil de adivinar.

2.3.1.2. RESPONSABILIDADES DEL USUARIO

- ✚ El Administrador debe desactivar cualquier característica de los sistemas o aplicaciones que les permita a los usuarios, almacenar localmente sus contraseñas.
- ✚ El usuario deberá estar consiente de los problemas de seguridad que acarrea la irresponsabilidad en la salvaguarda y uso de su contraseña.
- ✚ 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.
- ✚ Las cuentas de usuario son personales, en ningún momento deben ser utilizadas por personal ajeno al que le fue asignada.
- ✚ La práctica de guardar las contraseñas en papel adherido al monitor o áreas cercanas al equipo de trabajo, es una falta grave y sancionable.
- ✚ Las contraseñas deben ser memorizadas desde el mismo momento en que le es asignada.
- ✚ Se desechará, toda documentación que tenga que ver con información relacionada a su cuenta de usuario, minutos después de habersele entregado y siempre que haya sido memorizada o resguarda su información.
- ✚ Es importante que el usuario establezca contraseñas fuertes y desligadas de su vida personal o de su entorno familiar o no empleando formatos comunes de fechas.
- ✚ Toda falla en el equipo debe ser documentado por el operador de la estación de trabajo.

Normativa del uso de correo electrónico.

- ✚ 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.
- ✚ El servidor de correo bloqueará archivos adjuntos o información nociva como archivos .exe o de ejecución de comandos como applets java, javascript o archivos del tipo activeX o IFrame.
- ✚ Ningún usuario externo a la Corporación, puede usar los servicios de correo electrónico proporcionado por la red institucional.
- ✚ Es responsabilidad del usuario hacer un correcto empleo del servicio de correo electrónico.
- ✚ Cualquier actividad no consecuente con los ítems siguientes se considera un mal uso:
 - a) El no mandar ni contestar cadenas de correo.
 - b) El uso de su cuenta con fines académicos y/o investigación.
 - c) La depuración de su bandeja de entrada del servidor (no dejar correos por largos periodos).
 - d) El no hacer uso de la cuenta para fines comerciales.
 - e) El respetar las cuentas de otros usuarios.
 - f) El uso de un lenguaje apropiado en sus comunicaciones.
 - g) El respetar las reglas de "Conducta Internet" para las comunicaciones.

h) Respetar los términos dados en el contrato de trabajo sobre normativas y políticas de seguridad.

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

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

✚ La información y el software tienen la característica de ser propiedad intelectual, la Corporación 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

✚ Al ser contratado como empleados de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, se les entregará la documentación necesaria para cubrir todas las necesidades inherentes a su cargo.

✚ 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. El administrador de sistemas tomará las medidas necesarias para asignar los servicios a los usuarios externos.

✚ 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

- ✚ El administrador de sistemas diseñará los mecanismos necesarios para proveer acceso a los servicios de la red institucional.
- ✚ Los mecanismos de autenticación y permisos de acceso a la red, deberán ser evaluados y aprobados por el Administrador de la red.
- ✚ El Administrador, hará evaluaciones periódicas a los sistemas de red, con el objetivo de eliminar cuentas de acceso sin protección de seguridad, componentes de red comprometidos.
- ✚ El personal que de soporte a escritorio remoto efectuará la conexión desde un maquina personal, en ningún momento lo hará desde una red o área de servicios públicos.
- ✚ El administrador de sistemas, verificará que el trafico de red sea, estrictamente normal, la variación de este sin ninguna razón obvia, pondrá en marcha técnicas de análisis concretas.
- ✚ Los dispositivos de red, estarán siempre activos, y configurados correctamente para evitar anomalías en el tráfico y seguridad de información de la red institucional.
- ✚ Se utilizarán mecanismos y protocolos de autenticación como, ssh, IPsec, Claves públicas y privadas, autenticación usuario/contraseña, cualquiera de ellos será valido para la autenticación.
- ✚ 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:

- ✚ El administrador de sistemas tendrá especial cuidado al momento de instalar aplicaciones en los servidores, configurando correctamente cada servicio con su respectivo permiso de ejecución.
- ✚ 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.
- ✚ El servidor de dominios, verificará y desactivará cualquier estación de trabajo, que este en uso después de la hora de salida o finalización de la jornada laboral.
- ✚ No le esta permitido al usuario operador, realizar actividades de configuración del sistema, bajo ninguna circunstancia.
- ✚ Los servidores estarán debidamente configurados, evitando el abuso de personal extraño a las administraciones estas.
- ✚ 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.
- ✚ La cuenta administrativa, es propiedad exclusiva del administrador de sistemas.
- ✚ Las aplicaciones prestadoras de servicios correrán con cuentas restrictivas y jamás con privilegios tan altos como los de la cuenta administrativa.

2.3.1.6. CONTROL DE ACCESO A LAS APLICACIONES

- ✚ El usuario tendrá los permisos de aplicaciones necesarios para ejercer su trabajo.
- ✚ Tienen acceso total a las aplicaciones y sus archivos, los usuarios que lo ameriten por su cargo dentro de la Corporación, siempre que sea aprobado por el comité de seguridad.
- ✚ Los niveles de privilegio son definidos por el comité de seguridad, en base a lo importante o crítico de la información que procesará el usuario.
- ✚ Antes de ser puestas en ejecución, las aplicaciones recibirán una auditoria sobre fallos o información errónea que puedan procesar.
- ✚ Se hace énfasis en la importancia que tienen las salidas de información provistas por una aplicación, sin importar el medio de salida.
- ✚ La información será visualizada únicamente en terminales previamente definidas, ya sea mediante direccionamiento de hardware o direccionamiento IP.
- ✚ En el registro de sucesos del sistema se registran todas las actividades realizadas por un determinado usuario, sobre las aplicaciones.
- ✚ 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

- ✚ 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.
- ✚ De ser necesarios, se crearan 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.
- ✚ Es necesario efectuar un respaldo de los archivos de registro o logs, fuera de los dispositivos que les creen.
- ✚ 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.

- ✚ Es la unidad de sistemas es quien crea las reglas para la ejecución de algún servicio.
- ✚ 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

- ✚ Ninguna persona que labore para la Corporación, está facultada para instalar software en las estaciones de trabajo, sin antes haberse aprobado su utilización.
- ✚ Sin importar el origen del software y la utilización del mismo dentro de la Corporación, éste será evaluado, haya sido o no aprobada su utilización. Ninguna clase de código ejecutable será puesto en marcha sin antes haber pasado el control de análisis sobre seguridad del mismo.

- ✚ Antes de efectuar cualquier análisis o prueba sobre los sistemas de producción, se realizarán backups generales, de la información que en ellos se procesa y del sistema en sí.
- ✚ Los sistemas o dispositivos que aun están conectados a la red, pero que no tienen utilización productiva alguna para la Corporación, se les deberá eliminar cualquier rastro de información que hayan contenido.

2.3.2.3. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

- ✚ El software que venga de empresas no reconocidas o acreditadas como no confiables, no tendrá valor alguno para la Corporación siempre que esta sea en formato ejecutable.
- ✚ El administrador supervisará la instalación y correcta configuración de software antivirus en todas y cada una de las estaciones de trabajo de la Corporación.

2.3.2.4. MANTENIMIENTO DE SISTEMAS Y EQUIPO DE CÓMPUTO

- ✚ El usuario no está facultado a intervenir física o lógicamente ninguna estación de trabajo, que amerite reparación.
- ✚ 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.
- ✚ En caso de ser afirmativo el cambio de archivos se hará un backup general de la aplicación o sistema al cual se le realiza el cambio.
- ✚ Cualquier falla efectuada en las aplicaciones o sistemas, por la manipulación errónea de archivos, posterior mantenimiento deberá ser notificada y reparada por el personal técnico encargado en dicha función.

- ✚ deberá haber una bitácora completa, en cuando a las versiones de actualización del software y de las revisiones instaladas en los sistemas.

2.3.2.5. SEGURIDAD EN EL MANEJO DE LOS MEDIOS DE ALMACENAMIENTO

- ✚ Bajo ninguna circunstancia se dejarán desatendidos los medios de almacenamiento, o copias de seguridad de los sistemas.
- ✚ Todo medio de almacenamiento deberá ser documentado e inventariado en un registro específico y único sobre medios de almacenamiento.
- ✚ La ubicación de los medios de almacenamiento deberá estar alejada del polvo, humedad, o cualquier contacto con material o químicos corrosibles. La llave de seguridad que da acceso a los medios de almacenamiento resguardados bajo supervisión de la gerencia, será mantenida bajo estricta seguridad por cualquiera de las dos entidades encargadas de mantener la seguridad de los medios.
- ✚ 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:

- ✚ La unidad de sistemas diseñará, toda la red de la Corporación siguiendo la normativa de cableado estructurado.

- ✚ Es totalmente prohibido, salvo autorización o supervisión expresa de la unidad de sistemas, la intervención física de los usuarios sobre los recursos de la red institucional (cables, enlaces, estaciones de trabajo, dispositivos de red).
- ✚ Solo el personal autorizado es el encargado exclusivo de intervenir físicamente los recursos de la red institucional.

Personal de Informática:

- ✚ El soporte técnico a las estaciones de trabajo y servidores, es responsabilidad de la unidad de informática, por tanto deben tomarse todas las medidas de seguridad necesarias para evitar cualquier anomalía por manipulación errónea efectuada por terceros.
- ✚ Las estaciones de trabajo y servidores, deben operar en óptimas condiciones, efectuando un mantenimiento constante y acorde a las especificaciones de los fabricantes del equipo.
- ✚ Se deberá proteger las salas que contengan los servidores, o equipos de información críticos, con paredes recubiertas de material aislante o anti incendios.
- ✚ Las líneas de alimentación de energía externa deberán estar protegidas con filtros de protección para rayos.
- ✚ 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.
- ✚ Al permanecer en las instalaciones de procesamiento de información, se dedicara 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 diseñad

- ✚ El personal debe contar con su respectiva identificación, donde se identifique su nombre, área de trabajo, cargo que desempeña dentro de dicha área y su fotografía.
- ✚ 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.

2.4.1.2. CONTROLES FÍSICOS GENERALES

- ✚ Los respaldos de información de las estaciones de procesos críticos, solo lo realizara el personal responsable de dicho proceso.
- ✚ Las disqueteras, unidades USB y lectoras de CD deberán deshabilitarse en aquellas máquinas en que no se necesiten.
- ✚ Cada empleado de la Corporación, velará por la correcta salvaguarda de la información, el dejar información desatendida sin ningún medio de seguridad verificable es una práctica prohibida y sancionable.
- ✚ El Administrador deberá llevar el registro del mantenimiento que se realizan a los equipos de cómputo.
- ✚ Dentro de las instalaciones de la unidad de sistemas, 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. Cualquier actividad anómala, efectuada dentro de las instalaciones físicas de procesamiento de información será cancelada en el momento en que se constatare la actividad.
- ✚ El personal de procesamiento de información será relevado de su cargo, si este no está cumpliendo con las actividades asignadas a su cargo y por lo contrario dedicase su tiempo a realizar actividades extrañas a los objetivos del centro de procesamiento.

- ✚ 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. Los equipos de oficina, como cafeteras, aires acondicionados, entre otros no deben estar conectados al mismo circuito que los sistemas informáticos.
- ✚ 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.
- ✚ Los UPS son de uso exclusivo de cada estación de trabajo.
- ✚ Es responsabilidad de los usuarios la correcta utilización de los UPS.
- ✚ 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.
- ✚ Se debe efectuar una revisión periódica de los circuitos.
- ✚ Es responsabilidad del Administrador proveer los materiales informativos (carteles) necesarios en las diferentes salas o instalaciones físicas de procesamiento de información.
- ✚ El material debe ser claramente entendible y visible por todos los usuarios.

2.4.2. ACTIVIDADES PROHIBITIVAS

- ✚ Está prohibido el ingreso de bebida(s) o alimento(s) de cualquier tipo a las áreas de procesamiento de datos, sin el consentimiento expreso del administrador del área o persona encargada.
- ✚ Se prohíbe a los usuarios utilizar equipos informáticos, herramientas o servicios provistos por la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, para un objetivo distinto del que están destinadas o para beneficiar a personas ajenas a la Corporación.
- ✚ Se prohíbe el ingreso de personas en estado de embriagues sin importar el cargo que estas desempeñen, a las instalaciones físicas de procesamiento de datos críticos o no, para la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge.

2.5. SEGURIDAD LEGAL

2.5.1. CONFORMIDAD CON LA LEGISLACIÓN

2.5.1.1. CUMPLIMIENTO DE REQUISITOS LEGALES

- ✚ Las acciones de los empleados de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, referente a la utilización de software pirata dentro de las instalaciones de la Corporación, no son propias de la Corporación.
- ✚ La Corporación 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 sus instalaciones.

- ✚ La unidad 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.
- ✚ El original de los contratos de arrendamiento de software, será resguardado por la Unidad de sistemas de la Corporación.
- ✚ La Corporación no participa con sus empleados en la adquisición de software de forma no legal.
- ✚ La Corporación no respalda que sus empleados puedan instalar software no licenciado en los equipos de trabajo, los cuales son propiedad exclusiva de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge.
- ✚ La Corporación 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.
- ✚ 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 Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, sus empleados no pueden utilizar software de este tipo sin su respectiva licencia.
- ✚ La Corporación 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.
- ✚ Las copias que se hagan del software original serán que se utilicen para las instalaciones en toda la red institucional.
- ✚ La transferencia de software comercial a terceros, es una actividad únicamente permisible, por un derecho concedido a la Corporación por el propietario intelectual del software o licencia en cuestión.

- ✚ La Corporación 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.
- ✚ Al laborar para la Corporación, cualquier información, código u otros, producida, mediante tratamiento electrónico dentro de sus instalaciones, es propiedad irrevocable de la Corporación.
- ✚ Ningún empleado de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, está facultado a obtener software para la Corporación, sino es mediante los canales de gestión necesarios.

Área de Informática:

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

- ✚ La documentación de seguridad acá provista, podrá ser actualizada respetando todas y cada una de las políticas que demandan su correcto diseño y aplicabilidad.
- ✚ 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.
- ✚ 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.
- ✚ El medio exclusivo de soporte para la seguridad en el tratamiento de la información de la Corporación, lo constituyen las políticas de seguridad informática y toda su reglamentación técnica, esto incluye un sistema de gestión de seguridad de la información.

- ✚ Se suspenderá por plazo de hasta un año, por incumplimiento de la normativa de seguridad informática o de protección de datos en los casos en los que él(los) problema(s) ocasionado(s), sea(n) crítico(s) y vital(es), para el correcto funcionamiento de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge.
- ✚ El único caso en el que personal ajeno o propio de la Corporación no será sancionado por violación a la seguridad informática de la Corporación, serán, los motivos previstos en la política de excepciones de responsabilidad.

2.5.1.3. NORMATIVA SOBRE AUDITORIAS A LOS SISTEMAS DE INFORMACIÓN

- ✚ La ejecución de una auditoría a los sistemas informáticos, ameritará la planificación de la misma, herramientas a utilizar en la auditoría, objetivos de la auditoría, implicaciones legales, contractuales, requisitos y conformidad con la gerencia.
- ✚ 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.
- ✚ Salvo casos especiales toda auditoría, deberá estar respaldada por la gerencia.
- ✚ La implicación de casos especiales, en los cuales sea necesario de inmediato, amerita realizar auditorías sin una fecha planificada.
- ✚ Sin importar la razón de la auditoría, se llevara 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.
- ✚ 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.

- ✚ Salvo caso especial, cualquier cambio efectuado al sistema de archivos, será motivo de sanción.
- ✚ 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.
- ✚ Toda aplicación para la auditoría será instalado correctamente y supervisado su uso, desde las terminales remotas en el mismo segmento de red.

3. RECOMENDACIONES

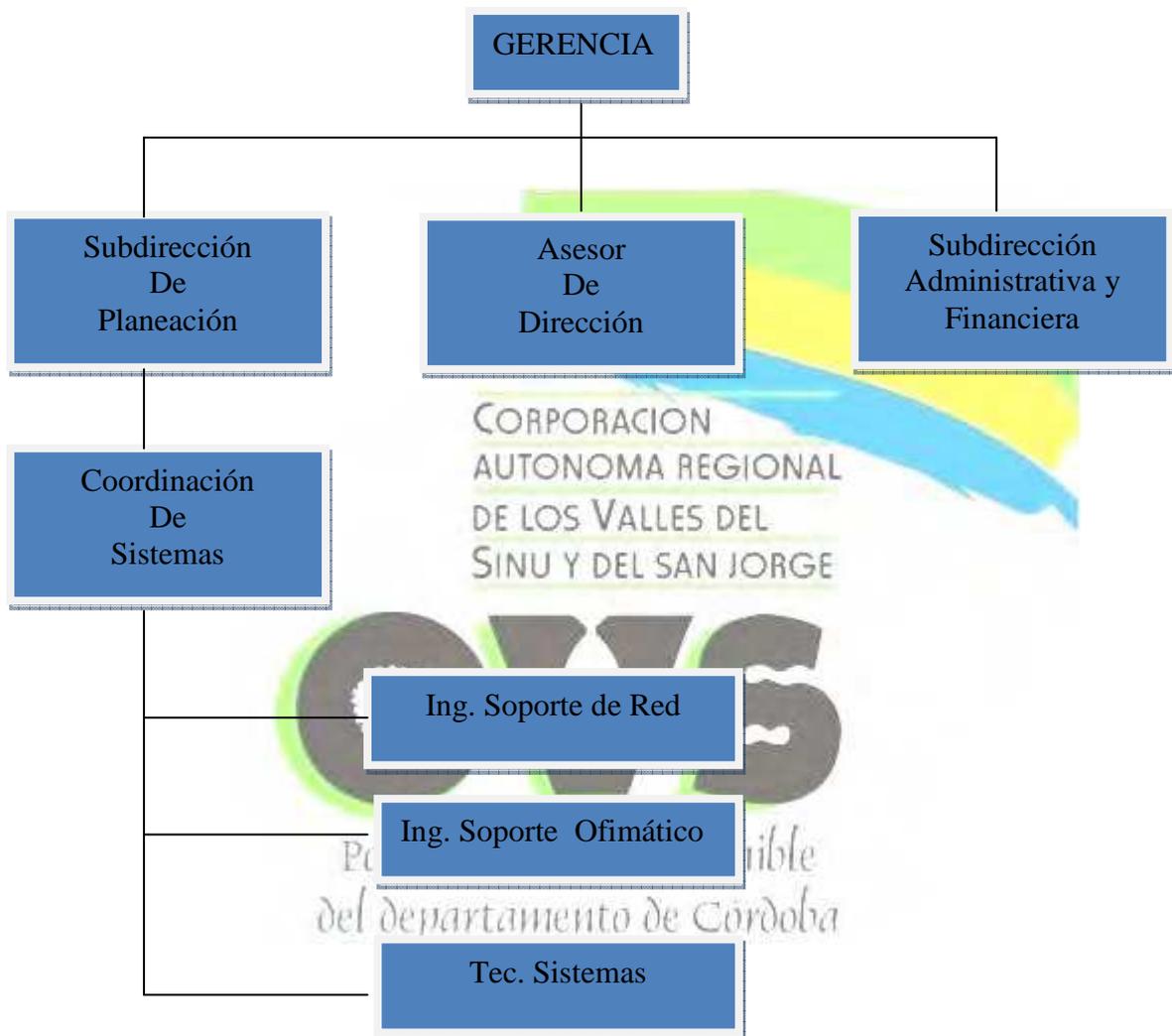
- ✚ Crear un Sistema de Gestión de Seguridad de la Información, que supervise y normalice, toda actividad relacionada con la seguridad informática.
- ✚ Aprobar y poner en marcha el manual de políticas y normas de seguridad informática.
- ✚ Actualizar de forma constante, transparente y de acuerdo a las necesidades existentes al momento, el manual de normas y políticas de seguridad informática.
- ✚ Asignar presupuesto para la gestión de seguridad de la información, independiente de la unidad de informática.
- ✚ Asignar personal al área de seguridad de la información.
- ✚ Crear un comité de seguridad de la información.
- ✚ Involucrar tanto personal técnico, como directivos de la Corporación, o a la alta gerencia 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 Corporación.
- ✚ Dar seguimiento a estándares internacionales sobre temas de seguridad de la información.
- ✚ Realizar pruebas de intrusión, locales y externas por personal de la Corporación, 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 Corporación, en temas de seguridad, adoptando un estricto control de las técnicas más comunes de persuasión de personal (Ingeniería Social).



5.1. ORGANIGRAMA

ORGANIGRAMA SEGURIDAD INFORMÁTICA



5.2. REFERENCIAS

Referencias Complementarias.

- ✚ ISO/IEC 17799 Code of Best Practice for Information Security Management
- ✚ Certified Information Systems Security Professional (CISSP)
- ✚ RFC 1244, Site Security Handbook

5.3. DESCRIPCIÓN DE PUESTOS Y PERFILES

- ✚ Corresponde a la unidad de Sistemas de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, la supervisión y verificación de las redes y los dispositivos de comunicación de la Corporación, con especial atención a la compatibilidad de equipos y condiciones de seguridad de las instalaciones, así como el cumplimiento de la normativa técnica sobre verificaciones de los equipos que en cada caso sea aplicable.
- ✚ Es responsabilidad del Departamento de Informática, la organización y puesta en marcha de las comunicaciones informáticas necesarias dentro de las instalaciones de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, así como de las comunicaciones que ésta realice con terceros.
- ✚ Corresponde a éste departamento mantener informadas a las Autoridades de la Corporación y al resto de los usuarios de los avances tecnológicos que se vayan produciendo en el área de informática (hardware, software, material de informática, etc.). Haciendo efecto de las responsabilidades antes descritas, se establecerá una normativa reguladora de los servicios de comunicación informática dentro de las instalaciones físicas de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, y de las que ésta realice con terceros.

✚ Dicha normativa deberá referirse en todo caso a:

- a) La definición del servicio o servicios prestados.
- b) El nivel de prestación.
- c) Los derechos y deberes de los usuarios.
- d) Las garantías técnicas y jurídicas del servicio.

✚ Las normas generales de Seguridad Informática, de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, podrán condicionar el acceso a prestaciones de la red en función de los niveles de compatibilidad y seguridad que se establezcan.

PERFIL COORDINADOR DE SISTEMAS

✚ Corresponde al administrador, gestionar ante la gerencia una correcta aplicabilidad de las normas y políticas establecidas para salvaguardar los activos de información de la Corporación, así como de establecer los parámetros necesarios para el mantenimiento adecuado del Sistema de Gestión de Seguridad de la Información, desarrollando una serie de medidas estratégicas que propicien un alto nivel de seguridad en la infraestructura tecnológica de la Corporación Autónoma Regional de los Valles del Sinú y del San Jorge, aceptable para los fines y objetivos institucionales.

✚ El Coordinador de sistemas, podrá constituir en el momento que crea conveniente, comisiones técnicas de apoyo y asesoramiento, formadas por expertos en el área de seguridad informática; dichas comisiones serán siempre temporales.

OBJETIVOS QUE DEBE CUMPLIR

✚ Definir la misión de seguridad informática de la Corporación en conjunto con la gerencia.

✚ Aplicar una metodología de análisis de riesgo para evaluar la seguridad informática en la Corporación.

- ✚ Definir la política de seguridad informática de la Corporación.
- ✚ Definir los procedimientos para aplicar la Política de seguridad informática.
- ✚ Seleccionar los mecanismos y herramientas adecuados que permitan aplicar las políticas dentro de la misión establecida.
- ✚ Crear un grupo de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad informática dentro de la Corporación.
- ✚ Promover la aplicación de auditorías enfocadas a la seguridad, para evaluar las prácticas de seguridad informática dentro de la Corporación.
- ✚ Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad en la Corporación.
- ✚ El coordinador de sistemas tiene como principal responsabilidad la administración y coordinación diaria del proceso de Seguridad Informática de la Corporación.
- ✚ Tiene como responsabilidad asegurar el buen funcionamiento del proceso de seguridad Informática de la Corporación.
- ✚ Es deber del coordinador de sistemas, el desarrollo de procedimientos de seguridad detallados que fortalezcan la política de seguridad informática institucional.
- ✚ El coordinador de sistemas, debe ser miembro activo del comité de seguridad, y mantener contacto con los demás ingenieros de otras organizaciones, estar suscrito a listas de discusión y de avisos de seguridad.

- ✚ Es responsabilidad del coordinador de sistemas, y con colaboración de todos los funcionarios de la Corporación promover la creación y actualización de las políticas de seguridad informática, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.
- ✚ El Coordinador de sistemas debe atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales.
- ✚ Es responsabilidad del Coordinador de sistemas, coordinar la realización periódica de auditorías a las prácticas de seguridad informática.
- ✚ El Coordinador de sistemas debe establecer la misión y metas internas en cuanto a la seguridad de la información, de acuerdo a la misión y metas organizacionales.
- ✚ Es responsable de mantenerse al día de las actualizaciones y nuevas vulnerabilidades encontradas en el software de la Corporación
- ✚ Éste a su vez, coordinará con los responsables de los activos de los diferentes departamentos de la Corporación, brindando los medios necesarios para asegurar la disponibilidad, integridad y confidencialidad de la información, previamente clasificada por los responsables de los activos.
- ✚ Corresponde a los responsables de los activos, mantener un adecuado control sobre los recursos asignados a su departamento u oficina, clasificar cada activo según la importancia que éste tenga para los procesos desarrollados dentro del departamento o área que tenga bajo su administración o cargo.
- ✚ Coordinar sus esfuerzos brindando la información necesaria y relevante, con el objetivo de lograr mantener una mejor y más adecuada administración de los recursos y la Red Institucional.

