PLAN DE SEGURIDAD INFORMÁTICA

2017 - 2019

YESID GONZALEZ DUQUE

Director General

JORGE ELIÉCER JURADO SAPUYES

Subdirector Administrativo

GRUPO DE SISTEMAS

FUNCIONARIOS

CARLOS ALBERTO ORTÍZ AUX

DIEGO GUZMÁN IRAGORRI

EFRAIN ALFONSO HOYOS

CONTRATISTAS

YESICA PAOLA GONZALEZ

FERNANDO RIASCOS

JOSE LUIS RIVERA

CORPORACIÓN AUTÓNOMA REGIONAL DEL CAUCA

INTRODUCCIÓN

La Corporación Autónoma Regional del Cauca CRC con NIT No. 891.501.885-4 es una entidad de carácter público, del orden nacional, cuyo objetivo principal es la administración de los recursos naturales renovables, propendiendo por el desarrollo sostenible de conformidad con las disposiciones normativas y legales.

En su estructura orgánica, dentro de la Subdirección Administrativa se encuentra conformado un grupo de sistemas el cual debe encargarse de mantener la funcionalidad permanente de los diferentes sistemas de información y servicios informáticos que actualmente tiene la entidad, además de seguir con los lineamientos establecidos por las demás entidades del gobierno garantizando que las acciones tendientes al funcionamiento de la entidad cumplan la normatividad vigente.

Es importante ofrecer un proceso de mejora y estabilidad a estos servicios de los cuales dependen las aplicaciones disponibles para satisfacer las actividades de las Subdirecciones misionales y el actuar tecnológico que en general apoya todas las labores misionales y corporativas de la CRC, por lo cual desde el grupo de sistemas, se deben realizar esfuerzos para mantener en una mejora continua esta oferta para proveer a las direcciones territoriales y en general a toda la CRC de un sistema siempre disponible con las mejores condiciones técnicas posibles para el actuar institucional.

Así mismo, todas estas labores se encaminan hacia garantizar la integridad y confiabilidad absoluta de todos los activos de información disponibles, llevando la utilización e implementación del Sistema de Información Ambiental Corporativo, hacia la eficiencia y eficacia requerida para el actuar misional.

De igual manera, la integración de actividades y esfuerzos en esta materia son de suma importancia en aras de velar por el buen y ágil funcionamiento de la Corporación, buscando además que la Entidad como tal, cumpla con todos y cada uno de los requisitos establecidos por la Ley, en cuanto al alcance de las metas establecidas por las distintas autoridades estatales.

OBJETIVO GENERAL

Planificar, orientar y desarrollar los mecanismos necesarios para dotar de disponibilidad, confidencialidad e integridad al conjunto de datos y activos de información de la Entidad.

OBJETIVOS ESPECÍFICOS

- Formular el esquema de seguridad de la información de acuerdo a las necesidades del Sistema de Información Ambiental Corporativo.
- Instaurar medidas de control de acceso a los activos de información de la Corporación.
- Alinear a la normatividad vigente a nivel Nacional las políticas de gestión y administración de activos de información de la Corporación.
- Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información en la Corporación.
- Proyectar la implementación del presente plan junto con sus actividades y documentos relacionados.

JUSTIFICACIÓN

En la actualidad, la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener una compañía, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo más preciado: la información.

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Hoy en día las empresas que manejen sistemas de información han generado la necesidad del aseguramiento de la información, generando políticas y controles, buscando garantizar la estabilidad y confiabilidad de la información, proyectándose ser reconocidas a nivel nacional como internacional, teniendo buena credibilidad y ubicándose siempre en los primeros lugares.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno en Línea, y el conjunto de normativas que rigen al respecto, además de la situación actual del sistema de información y los servicios tecnológicos de la CRC, se hace necesario levantar una línea de base sobre la cual se articulen diferentes esfuerzos encaminados a ofrecer la seguridad en la información, teniendo en cuenta las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en las redes, en los servicios y demás herramientas tecnológicas dispuestas para tal fin.

Es importante aclarar que este proyecto se encamina a formar las bases para una declaratoria de lineamientos progresivamente aplicables que vayan dando forma al Plan de Seguridad Informática partiendo desde las copias de seguridad, su protección, integralidad, restricción de acceso y demás elementos a tener en cuenta.

Los principales beneficiarios son en primera medida la Alta Dirección, ya que se ofrecerá disponibilidad y veracidad en la información que se usa para la toma de decisiones. Por otra parte, los usuarios finales del sistema de información que alimentan y requieren de agilidad y seguridad al momento de ingresar información que puede o no ser pública, a través de los servicios tecnológicos de la CRC.

ALCANCE Y DELIMITACIÓN DEL PLAN

El alcance del presente Plan se suscribe al cubrimiento de la Seguridad de la Información de los componentes relevantes del Sistema de Información Ambiental Corporativo de la CRC.

El plan se desarrollará en la Corporación Autónoma Regional del Cauca, hasta el mes de diciembre de 2019, en cuya oportunidad, según el cambio de Administración y teniendo en cuenta la actualización de normativas, este documento se actualizará de manera pertinente.

La implementación de este plan se realizará con el liderazgo del grupo de Sistemas de la Subdirección Administrativa, y la adopción será responsabilidad de todos los funcionarios y contratistas según las competencias establecidas.

MARCO DE REFERENCIA

ANTECEDENTES

En los últimos años, las entidades públicas tienden a mejorar la eficiencia, efectividad y eficacia de su gestión a partir de la reducción de costos por diferentes medios y buscando siempre la mejora del aprovechamiento de sus recursos, para lo cual buscan: optimizar sus procesos misionales, revisar y actualizar políticas de adquisición en la entidad, automatizar los procesos manuales, dinamizar la integración de los procedimientos de su sistema integrado de gestión, entre otros. Esto se realiza a partir de los lineamientos de la Política Gobierno en Línea, en la cual se describen las características sobre las cuales debe enmarcarse la ejecución de todos estos objetivos.

Para la optimización de estos procesos se hace necesario utilizar las tecnologías de información de acuerdo a las necesidades de la entidad, teniendo en cuenta la visión, misión y estrategias que la alta dirección quiere implementar en la Entidad.

El Plan Estratégico de Tecnología de Información y comunicación de la Corporación Autónoma Regional del Cauca es un conjunto de políticas tecnológicas e iniciativas de la Oficina de Sistemas que deben soportar la visión, misión y estrategias que la Corporación tiene, teniendo en cuenta que la razón de ser de las tecnologías de información son las áreas misionales de la Corporación y por ende ambas perspectivas (misión y tecnología) deben estar alineadas y contar con mecanismos para facilitar éste alineamiento.

De su mano, el Plan de Seguridad Informática debe constituirse como una línea de mando sobre la cual se establezcan los parámetros a seguir para garantizar su principal objetivo. A este se relacionan a su vez varios procedimientos, enfocándonos en el procedimiento de Copias de Seguridad.

En el año 2016 se documentó un Plan de Seguridad Informática, sin embargo, posteriormente tras los requerimientos y análisis realizados por diferentes instancias internas y externas, se determinó que se requería la realización de un nuevo plan que recogiera la actualización de las necesidades y normativas que circundan la seguridad de la información en las instituciones públicas y principalmente en las Corporaciones Autónomas Regionales.

MARCO TEÓRICO

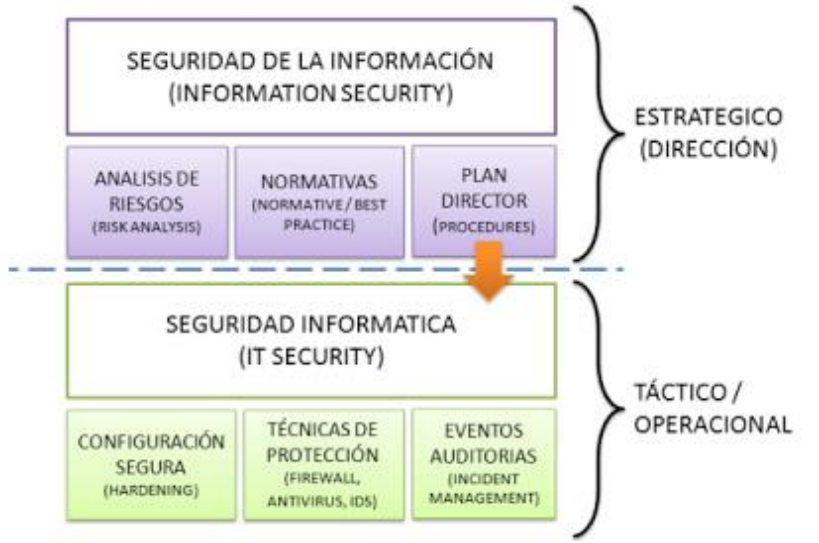
En el campo de la Seguridad Informática uno de los objetivos principales es brindar seguridad y estabilidad a la información institucional que se manipula por parte de usuarios internos y externos de la Corporación, implementando mecanismos de seguridad informática que garanticen la confidencialidad, integridad y disponibilidad de los sistemas de información corporativos y la información asociada.

Ello se aplica a ciertos procedimientos, entre ellos el de Copias de Seguridad, que busca definir los parámetros técnicos a tener en cuenta para la elaboración y custodia de las copias de seguridad de datos almacenados en los servidores de la Corporación Autónoma Regional del Cauca CRC.

Seguridad informática – Seguridad de la Información

Aparentemente son dos conceptos muy similares, sin embargo su campo de aplicación y énfasis son distintos, a pesar de que tienen que trabajar armoniosamente para el cumplimiento de su misión.

Por una parte, la seguridad informática se encarga del despliegue de aplicativos (software) y dispositivos (hardware) que evitan las fallas en los sistemas de computación, basándose en actividades principalmente técnicas para garantizar la seguridad, por ejemplo, la implementación de un firewall que proteja la red y el sistema de una entidad corporativa de ataques o accesos no deseados. Por otro lado, la seguridad de la información se centra más hacia la parte administrativa de la información que tiene que ver con la seguridad, por ejemplo, las disposiciones descritas en un procedimiento de copias de seguridad, su conservación, restauración y disposición final.



Esquema de Seguridad Informática – Seguridad de la Información

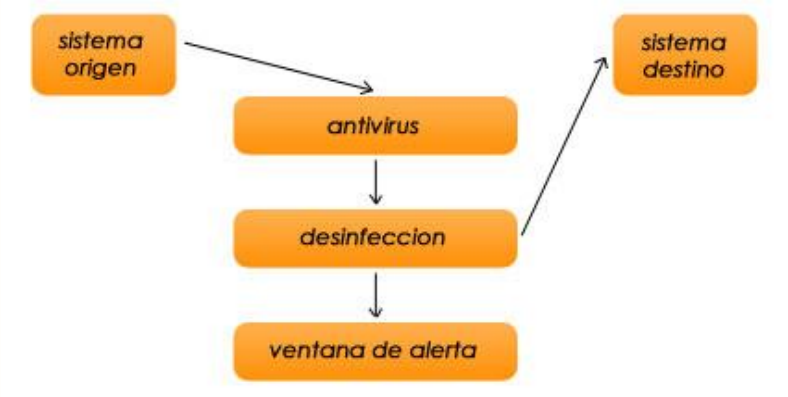
Fuente: http://www.seguridadparatodos.es

Tal como se describe en el párrafo anterior, son dos conceptos que funcionan articulada y secuencialmente para proveer de una estabilidad y una continuidad expresa en la funcionalidad permanente de un sistema que proteja los datos sensibles de una red de datos, dando al usuario la tranquilidad al disponerle de confidencialidad y herramientas en caso de sufrir una falla parcial o total en el sistema, logrando restablecer los servicios e información en un tiempo prudente.

Elementos a revisar en de Seguridad de la Información

Son diversos los elementos usados para implementar seguridad en una red de información, ofreciéndose en el mercado tanto software como hardware, siendo la elección de estos según las características específicas de la entidad o red de datos que requiere la implementación.

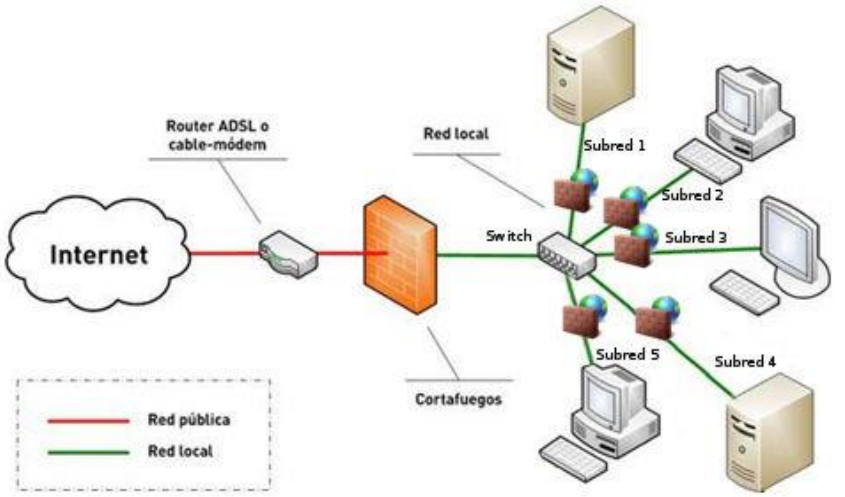
Antivirus (SW): son los elementos más básicos y más populares para el aseguramiento de la información, se ofrecen a nivel de usuario básico, así como para usuarios empresariales y hoy en día cuentan con muchas características, incluyendo funcionalidades de otros elementos como el firewall, protección de datos, escaneo de enlaces web, protección de correo electrónico, entre otros.



Fuente: http://www.veintisietemasuno.com

Establecen políticas de seguridad actualmente actualizables online y permanentemente, los proveedores de antivirus constantemente están desarrollando técnicas y protecciones para las amenazas emergentes en internet día a día. Se considera indispensable e ineludible la adquisición de antivirus al usar dispositivos computacionales, sobre todo para aquellos sistemas operativos más intuitivos y fáciles de acceder como Microsoft Windows.

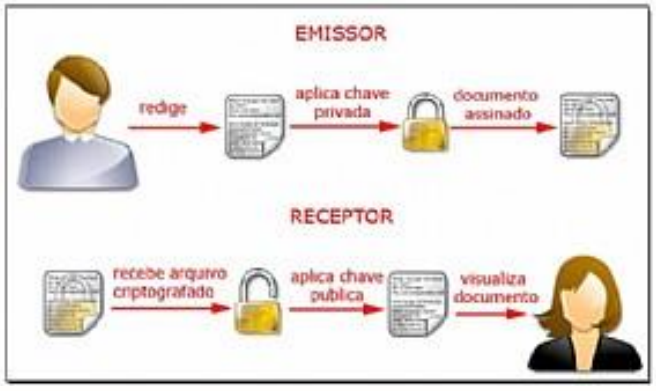
Cortafuegos (HW/SW): se pueden adquirir en dispositivos físicos como en desarrollos de software o híbridos. Son esenciales para las grandes entidades que deben proteger los datos más aún cuando cuentan con servicios alojados localmente como página web, aplicativos propios, bases de datos, servidores de correo, etc.



Fuente: http://geekland.eu

Funcionan administrando los accesos a la red y a las distintas secciones y servicios de la misma, buscando garantizar que la información sea manejada solo por quien tiene permiso para hacerlo y de la manera que se ha establecido previamente en las políticas. Actualmente son muy populares los cortafuegos que funcionan en Linux, aunque también algunas empresas usan appliance híbrido, dispositivos físicos que integran un firmware actualizable automáticamente en línea.

Certificados Digitales (HW/SW): también se encuentran tanto a nivel lógico como físico (tokens), y son usados por múltiples entidades, principalmente las entidades bancarias y aquellas que requieren de un sumo cuidado en la información.



Fuente: http://www.jornallivre.com.br

Se genera un archivo codificado que mantiene segura la identidad de los participantes en una transacción de información y requiere de un tercero de confianza para establecer la seguridad en la conexión.

Personal relevante para la Seguridad Informática

Chief Security Officer: El oficial en jefe de seguridad, es el encargado de que tanto la seguridad informática fluya a través de los servicios prestados como que la información cuente con la seguridad adecuada para garantizar la continuidad del negocio.

Debe tener los siguientes conocimientos:

Sistemas Operativos: tales como Windos, Linux, UNIX con una profundidad avanzada.

Mecanismos de Seguridad: diferentes metodologías y herramientas para la implementación de la seguridad en la información.

Protocolos de Seguridad: principales políticas aplicables a la seguridad informática y a la Seguridad de la Información.

Legislación: Normas, decretos, leyes y lineamientos dispuestos por el gobierno a las entidades públicas o privadas frente al manejo, administración y seguridad en la información.

En las entidades públicas este perfil generalmente no está establecido a menos que sea una entidad lo suficientemente grande y a menos que la alta dirección haya sido sensibilizada acerca de la importancia de garantizar la seguridad informática.

Generalmente se auditan procesos de gestión de la calidad porque es lo primero que anhela una entidad, además de que son cosas que quizás son más tangibles y visibles por parte de los usuarios finales.

Enfoques en Seguridad Informática

Según los esquemas comunes para las entidades gubernamentales de nuestro país, sobretodo en cuanto a la aplicación y desarrollo de la estrategia de Gobierno En línea, se pueden estar aplicando los siguientes:

Estándares:

ISO/IEC 20000: Norma técnica para la administración del servicio de las tecnologías de la información.

ISO/IEC 27000: Norma técnica con la descripción general y vocabulario sobre la administración de sistemas de seguridad de la información.

NTC ISO 27002: Norma técnica para la práctica de controles de seguridad de la información.

NTC ISO 27003: Guía para la implementación de sistemas de gestión de la seguridad.

NTC ISO 27005: Estándar con las guías para la gestión de riesgos de seguridad de la información.

NTC ISO 31000: Estándar con los principios y guías básicas para la gestión de riesgos.

ISO 27031: Guía de seguridad para la continuidad del negocio basada en la idoneidad de las tecnologías de la información.

NTC ISO 22301: Estándar con los requerimientos para la continuidad del negocio basada en la administración de los sistemas.

TIA 942: Estándar de infraestructura de telecomunicaciones para centros de datos.

MARCO CONCEPTUAL

Es necesario tener claras ciertas definiciones para el tema a tratar, así:

- Seguridad: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.
- Integridad: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.
- Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.
- Acceso: Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.
- Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.
- Ataque activo: Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos

o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

- Ataque pasivo: Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo ésto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.
- Amenaza: Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.
- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos

públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.
- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
- Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa

obligación de proteger dicha información en observancia del marco legal vigente.

- Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad

MARCO LEGAL

La puesta en marcha de auditorías en seguridad informática, su relacionamiento con el Plan de Seguridad Informática y el procedimiento de Copias de seguridad, están fundamentados bajo la normas:

- ISO/IEC 20000
- NTC ISO 22301
- NTC ISO 27002
- NTC lSO
- TIA 942
- ISO 27031
- NTC ISO 27003

De igual manera se unifican al manual interno de trabajo y al Sistema Integrado de Gestión de la Corporación Autónoma Regional del Cauca, además de los siguientes lineamientos o leyes:

- Ley 23 de 1982 sobre derechos de autor.
- Ley 1266 de 2008 Por medio del cual se dictan disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos.
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales". La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante Tratamiento) por parte de entidades de naturaleza pública y privada.
- Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y las tecnologías de la información y las telecomunicaciones TIC.
- Resolución CRC No 3153 del 11 de Febrero de 2013. Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETIC.

DISPOSICIONES DE SEGURIDAD

Las disposiciones relacionadas a continuación, tendrán aplicabilidad al Inventario de Activos de Información de la Corporación, el cual deberá clasificar los activos a los que se les debe brindar mayor protección, identificando claramente sus características y rol al interior de un proceso

Las actividades a realizar para obtener el inventario de activos son

- Definición
- Revisión
- Actualización
- Publicación

SEGURIDAD FÍSICA

Consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

De igual manera se pueden tener acciones hostiles que pongan en riesgo la infraestructura física que soporta los servicios tecnológicos en donde se alojan los activos de información de la CRC, tales como:

- Robo
- Fraude
- Sabotaje

En este nivel, se deben establecer controles de acceso a las áreas vulnerables y sensibles, usando guardias, detectores de metales, sistemas biométricos, verificación automática de firmas, seguridad con animales o protección electrónica.

Como se describe en el PETIC (Ver página 22), la Corporación ha realizado grandes esfuerzos en la adquisición de equipos de cómputo, servidores, acceso a internet, adecuación de la red de datos, eléctrica, área de sistemas y cuarto de redes. En servidores tenemos:

Marca	HDD Total	Servicio	Responsable
DELL Inc/COLIBRI/192.168.1.27	1136.5 Gb	Apache named iptables ssh samba	Administrador de servidores (contratista o funcionario)
VMWARE, ESXI 5.5 Inc	1847 Gb	CITA (postgres, apache, php), Pbx_Virtual (elastix, apache) y SIRH, bacula (bacula, apache, samba, php)	Administrador de servidores (contratista o funcionario)
VMWARE, ESXI 6.0 Inc	2500 Gb	Administrador de servidores (contratista o funcionario)	Administrador de servidores (contratista o funcionario)
Dell Inc/Danta/192.168.1.13	872.7 Gb	Oracle 10g	Administrador de servidores (contratista o funcionario)

La Corporación dispone a su vez de:

Dispositivo	Cantidad
Computadores	215
Portátiles	61
Tabletas	30
Impresoras	54
Proyectores	25
Escáneres	11
	396

Por lo tanto, es necesario definir unas normas o disposiciones para la buena utilización de los equipos de cómputo de propiedad de la Corporación y toda la infraestructura tecnológica que dispone. Se deberá tener en cuenta:

Seguridad de los equipos de cómputo e infraestructura tecnológica de la CRC

- La red física se instala aislada de cualquier tipo de cableado adicional que conduzca cualquier tipo flujo de carga eléctrica con el fin de evitar accidentes como interferencia en la red cableada o altas y bajas tensiones en la red eléctrica.
- La sala o cuarto de servidores, deberá estar separada del área del grupo de sistemas o cualquier otra área o en su defecto mantener una división, esta sala deberá ser utilizada únicamente por servidores que presten servicios informáticos a la CRC y/o dispositivos a fines y los equipos requeridos en la infraestructura eléctrica, de red y comunicaciones.
- Los dispositivos críticos que almacenan la información de la Corporación, deben ser ubicados en áreas acondicionas en temperatura adecuada y con un nivel de seguridad verificable y manejable por el administrador.
- En todo caso, el acceso a los servidores debe ser preferencialmente virtual, con credenciales de acceso administradas por el responsable de los servidores.
- El cuarto de servidores, cableado y el área donde labora el grupo de sistemas son zonas restringidas únicamente accesibles por personal autorizado o que labore en dichas instalaciones.
- El cuarto de servidores será única y exclusivamente para realizar procesos de soporte, adecuación o manipulación de servidores, no se permite por ningún motivo la realización de actividades ajenas a las anteriormente mencionadas.
- 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.

- El grupo de sistemas de la Corporación diseñará la red de cableado estructurado de acuerdo con las necesidades institucionales y conforme a la normativa establecida.
- La Corporación debe contar con un plan de mantenimiento preventivo y correctivo para los equipos de cómputo de su propiedad, incluyendo los servidores, dispositivos de red, eléctrico y seguridad.
- Los usuarios de equipos de cómputo que manipulen información crítica, deberán evitar la utilización de medios de almacenamiento externo y que puedan facilitar la pérdida de dicha información.
- 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.

Recomendaciones generales a usuarios finales

- Las violaciones de las Políticas para la Seguridad de la Información, serán sancionadas conforme a la Ley 734 del 5 de febrero de 2002 y en especial el artículo 34 numerales 2, 3, 4, 5 y 10, y las normas que lo modifiquen.
- El personal de la Corporación tiene totalmente prohibido la intervención física sobre los dispositivos que intervienen en la red institucional; cuando surja un inconveniente o necesidad se debe actuar conforme al procedimiento de soporte técnico y funcional y poner la respectiva solicitud en Intranet en la opción de soporte técnico.
- El usuario es responsable por la custodia y manejo de los computadores, impresoras u otros equipos que se encuentran asignados a su cargo, y su responsabilidad será determinada mediante un proceso disciplinario siendo extendida a los daños ocasionados a estos dispositivos por uso indebido, siempre que los daños se deban a negligencia o descuido en la operación.
- Solo el personal autorizado por el grupo de sistemas y/o la Subdirección Administrativa serán los encargados exclusivos de intervenir físicamente todos los elementos dentro de la infraestructura física institucional como es lo eléctrico, red, comunicaciones y seguridad.

- La instalación, mantenimiento, adecuación y modificación del hardware y software instalado en los puestos de trabajo de la Corporación, será permitida solo a los funcionarios o contratistas del grupo de sistemas autorizados para tal fin, previa asignación o traslado por parte del almacén de la Corporación.
- La utilización del servicio de Internet está permitido para asuntos institucionales. Se restringirá el acceso a aquellos sitios de streaming y demás que demanden un alto consumo de ancho de banda, además de aquellos que se consideren peligrosos por contenidos relacionados con virus y demás. Se excluyen las solicitudes de visualización de contenidos para la labor institucional, las cuales deben registrarse mediante la herramienta dispuesta en intranet.
- La Corporación Autónoma Regional del Cauca se reserva el derecho de vigilar o monitorear el uso de las herramientas tecnológicas de acuerdo con las leyes y reglamentaciones aplicables y, si se comprueba que existe un uso indebido de estas, se puede estar sujeto a sanciones.
- Los contratistas que por su objeto contractual deban ingresar sus equipos de cómputo u otros equipos tecnológicos a las dependencias de la Corporación, deben acogerse a las políticas de seguridad dispuestas por la Subdirección Administrativa.
- Es responsabilidad de cada empleado apagar los equipos de oficina que estén a su cargo, al finalizar la jornada diaria de trabajo.
- Todos los funcionarios y contratistas de la Corporación debe contar y portar con su respectiva identificación o carné corporativo en donde se detalla su nombre, cédula, tipo de vinculación y su fotografía.

Personal De Sistemas

- El soporte técnico a los equipos de cómputo de propiedad de la Corporación y servidores, es responsabilidad del grupo de sistemas, por tanto deben tomarse todas las medidas de seguridad necesarias para evitar cualquier anomalía por manipulación errónea efectuada por terceros.
- Los equipos de cómputo y servidores de propiedad de la Corporación, deben operar en óptimas condiciones, efectuando un mantenimiento constante y acorde con las especificaciones de los fabricantes del equipo, cumpliendo

con lo establecido en el procedimiento soporte técnico y funcional y el procedimiento de administración de servidores.

- Se debe mejorar el centro de datos de tal forma que soporte los nuevos servicios, soluciones informáticas y sistemas de información implementados.
- Se deben optimizar los sistemas ininterrumpidos de potencia (UPS) y demás elementos de la red eléctrica de la Corporación, realizándoles el mantenimiento preventivo continuo.

SEGURIDAD LÓGICA

Consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Para lograr lo anterior, se requieren controles como restringir el acceso a los programas y archivos, asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan, asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto, que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro, que la información recibida sea la misma que ha sido transmitida, que existan sistemas alternativos secundarios de transmisión entre diferentes puntos y que se disponga de pasos alternativos de emergencia para la transmisión de información.

De manera similar a la seguridad física se deben implementar mecanismos de control de acceso como Identificación y Autentificación, Roles, transacciones, Limitaciones a los Servicios, modalidad de acceso, ubicación y horario, controles de acceso interno y externo y administración.

Como una mezcla de los anteriores dos temas, se deben establecer controles de acceso a copias de seguridad de equipos y acceso a copias de seguridad de servidores.

Control de Acceso

- Área de Sistemas: Con el fin de disminuir el riesgo de pérdida de elementos y filtrado de información de accesos, el ingreso al área de sistemas se restringe para personal no autorizado, exceptuando casos en los cuales por naturaleza del ejercicio se requiera personal externo al grupo de sistemas.
    - Se cuenta con una alarma con sensores de movimiento y de apertura de puerta principal. Los códigos de activación y desactivación de la alarma deben ser cambiados al menos una vez por vigencia y siempre que existan novedades del personal que las maneja.
    - El cuarto de herramientas es de acceso exclusivo del grupo de sistemas, este y el cuarto de almacenamiento permanecerán asegurados con llave siempre que no exista una manipulación en su interior.
    - La puerta de acceso al área de sistemas contará siempre con un sistema magnético con panel digital, en cuyo caso, las credenciales serán renovadas en cada novedad de personal según corresponda.
- Cuarto de Redes y servidores: Se restringe el acceso a toda persona externa no autorizada al área de redes y servidores. Este cuarto se mantendrá asegurado siempre que no haya personal trabajando en su interior. Las llaves de acceso al cuarto de redes y servidores se custodiarán en un lugar seguro y solo tendrán conocimiento de su ubicación los responsables asignados.
- Acceso a las Bases de Datos: Estas credenciales serán de uso exclusivo del administrador de bases de datos y de servidores. Se podrán brindar accesos con ciertas limitaciones al grupo de soporte de software o desarrollo si existe.
- Acceso a los servidores:
    - El acceso a los servidores preferencial se realizará mediante ssh solo y exclusivamente de manera local (Red Lan), y las credenciales serán de uso exclusivo del administrador de bases de datos y de servidores. Se podrán brindar accesos con ciertas limitaciones al grupo de soporte de software o desarrollo si existe.
    - Se adicionarán restricciones por medio de credenciales, dirección IP y dirección MAC además de la necesidad del acceso exterior por medio de VPN creadas en el firewall, con el fin de evitar ataque o golpes a la seguridad e integridad de la información.

- De manera periódica se realizarán pruebas de intrusión que se pueda generar localmente o externamente que atenten contra la seguridad de la información. Estas se programarán por parte del Administrador de Servidores con una frecuencia no menor a 12 meses a partir de la fecha de adopción del presente plan.

- Administración acceso de usuarios: Son usuarios de la Corporación los empleados de planta, administrativos, contratistas y todo aquel que utilice los recursos, aplicaciones y servicios que brinda la Corporación Autónoma Regional de Cauca.

  - El grupo de sistemas manipulará las cuentas de administración de todos los equipos con una única clave que será renovada cuando se considere necesario y, mínimo dos veces por cada vigencia.

  - El grupo de Sistemas de la C.R.C. será el encargado de crear los usuarios de dominio, cuentas de correo y usuarios a las diferentes aplicaciones con las que cuenta la Corporación, solo a las personas que demuestren mediante un documento, ser empleados o contratistas de la Corporación.

  - El nombre de usuario se creará con la inicial del primer nombre y primer apellido, si se repitiere se optará por complementarlo con los otros nombres y apellidos. Ejemplo: Pedro Juan Pérez Pérez, usuario pperez. Los usuarios se deberán generar en minúsculas.

  - El usuario deberá poner una contraseña al momento de la creación de su cuenta que deberá contar mínimo con ocho caracteres alfanuméricos y deberá evitar 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. Debe contener al menos un carácter en minúscula, uno en mayúscula y un número.

  - Los usuarios asignados a una persona deberán ser únicos e intransferibles, indicando con esto que es la persona titular de dicho usuario quien tiene la responsabilidad de salvaguardar las respectivas contraseñas.

  - Los usuarios de las aplicaciones deberán tener su usuario y contraseña personal e intransferible y se asignarán previa solicitud por intranet/soporte de aplicaciones y autorización del jefe inmediato

indicando perfil específico para cada aplicación. Para acceder al sistema financiero y al de expedientes o contratación se deberá contar con la solicitud del Subdirector(a) o Jefe Oficina.

- Las cuentas corporativas deben ser usadas únicamente para fines institucionales.
- Es responsabilidad del usuario el buen uso del correo corporativo, evitando publicar o entregar sus credenciales (usuario y contraseña) ya que estas nunca les serán requeridas, además de evitar caer en las múltiples acciones de ingeniería social para la distribución de virus y correos no deseados. En cualquier caso de sospecha al momento de recibir correos con situaciones extrañas, el usuario debe informar al grupo de sistemas para evaluar la situación y tomar las medidas pertinentes.
- El acceso a los Access Point es exclusivo del área de sistemas, y se podrán usar filtros MAC para su utilización.

CONTROL DE ACCESO A LA INFORMACIÓN

Algunos usuarios o extraños (personal no autorizado) pueden encontrar alguna forma mediante la cual, logren el acceso al sistema o la base de datos y descubrir información clasificada o datos no autorizados.

Se deberá considerar la existencia de:

- Programas de Control. Deben existir programas protegidos que mantengan y controlen a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente. El uso de tal programa puede conferir al usuario algunos de los privilegios que corresponden al controlador de dichos programas. La transferencia de privilegios es adecuada si el programa actúa como filtro de la información. Inicialmente el primer programa de control será el Antivirus instalado en la infraestructura tecnológica de la CRC.
- Palabra de Acceso (Password). Es una palabra especial o código que debe teclearse al sistema de computadora antes que se realice un proceso. Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados. A fin de proteger el proceso de obtención de una llave del sistema, cuando el usuario realiza la entrada (en inglés

LOGIN), solicita una clave de acceso con el nombre del usuario, la cual consiste de unas cuantas letras elegidas por el usuario.

- Niveles de Acceso. Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

- Nivel de consulta de la información no restringida o reservada.
- Nivel de mantenimiento de la información no restringida o reservada.
- Nivel de consulta de la información incluyendo la restringida o reservada.
- Nivel de mantenimiento de la información incluyendo la restringida.
- Nivel de consulta de la información

El privilegio de lectura está disponible para cualquier usuario y sólo se requiere un conocimiento de la estructura de los datos o del Sistema de otro usuario para lograr el acceso. La autorización de lectura permite leer pero no modificar la base de datos.

- Nivel de mantenimiento de la información

  El concepto de mantenimiento de la información consiste en:

  1. Ingreso. Permite insertar datos nuevos pero no se modifica los ya existentes.
  2. Actualización. Permite modificar la información pero no la eliminación de datos.
  3. Borrado. Permite la eliminación de datos.

Un usuario puede tener asignados todos, ninguno o una combinación de los tipos de autorización anteriores. Además de las formas de autorización de acceso de datos antes mencionados, es posible autorizar al usuario para que modifique el esquema de la base de datos, pero esta función es de responsabilidad del administrador de servidores y bases de datos

FIREWALL

La Corporación Autónoma Regional del Cauca cuenta con un firewall físico FORTINET 200D, el cual contendrá al menos las siguientes características:

- Creación de normativas basadas en identidad.
- Criterios de control de acceso (ACC): identidad de usuario, zona de origen y destino, direcciones MAC e IP, servicio.
- Integración con VPN IPsec, VPN ssl, IPS, antivirus y antispyware, antispam, filtrado web, administración de ancho de banda, gestión de vínculos múltiples.
- Múltiples zonas de seguridad.
- Enrutamiento estático y dinámico.
- Aceptación de VLAN.
- Puede instalarse y configurarse o no desde la primera instalación y tener un piloto automático
- Supervisa todas las conexiones entrantes y salientes y protege frente a ataques DoS, escaneo de puertos, etcétera.
- Control de Aplicativos.
- Control de Dispositivos.
- Las políticas de control de dispositivos se aplican tanto a usuarios comunes, usuarios específicos, por grupos o como a administradores de red.
- Todos los dispositivos pueden ser bloqueados como dispositivo y no bloquear el o los PUERTOS.
- Puede bloquear UNIDADES DE CD/DVD desde la consola.
- Puede bloquear cámaras web desde la consola.
- Puede bloquear MEMORIAS O DISCOS USB.
- En todos los casos el bloqueo se puede definir para lectura, escritura o total.
- Puede agregar dispositivos permitidos por lista blanca o MAC.

- Control de contenido web.
- Las políticas de control de contenido web se definen para usuarios comunes o administradores de red.
- Dentro del control de contenido se bloquean sitios por listas blancas y negras.
- Se exige un mínimo de 30 categorías a controlar (pornografía, deportes, sitios de radio, redes sociales etcétera)
- Permite personalizar tanto las listas blancas como las negras.
- Control de navegación en internet.
- Las políticas de control de dispositivos se definen para usuarios comunes, usuarios específicos, por grupos o como administradores de red.
- Supervisa los horarios de uso de internet.
- Puede definir las horas de navegación.
- Puede definir los días de navegación.
- Bloquea el tiempo de navegación específico.

Adicionalmente, el software antivirus deberá contener también políticas firewall para protección Individual.

ANTIVIRUS

La Corporación Autónoma Regional del Cauca realizará anualmente la renovación de la licencia dl antivirus para mejorar la seguridad de los archivos y de protección contra accesos no deseados. El antivirus podrá tener especificaciones similares a:

CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
REQUISITOS DEL SISTEMA PARA LA CONSOLA	SI

CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
El proveedor de antivirus debe ofrecer la posibilidad de instalar la consola de administración en sistemas operativos Windows y linux cliente Y/O server.	SI
El servidor de administración remota deberá ser compatible al menos con los siguientes sistemas operativos	Windows Server 2003 SP2, Windows Server 2003 R2 SP2, Windows Server 2008 x64 R2 SP1, Windows Server 2008 x64 R2 Core, Windows Server 2012 x64, Windows Server x63 Core, Microsoft SBS 2003 x86 SP2, Microsoft SBS 2011 x64 Standard, Microsoft SBS 2011 x64 Esencial
El servidor deberá soportar al menos las siguientes bases de datos	Microsoft SQL Server 2008 R2 y posteriores, MySQL 5.5 y posteriores
El proveedor deberá proteger el acceso a la consola de administración mediante la autenticación de doble factor que deberá activarse desde la consola web.	SI
El proveedor deberá ofrecer el servidor de administración al menos en 3 formatos diferentes para su instalación	All-in-one, Instalación por componentes, Appliance Virtual
La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores	Mozilla Firefox,Internet Explore, Chrome, Safari y Opera.
El servidor se deberá comunicar con los endpoints a través de un agente que sea capaz de almacenar las políticas y ejecutar tareas de manera offline	SI

CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
Los paneles informativos de la interfaz gráfica podrán ser modificados por el administrador en tiempo real.	SI
La consola deberá ser compatible con los siguientes motores de bases de datos.	Oracle, MySQL Y MSSQL
REQUISITOS PARA ESTACIONES DE TRABAJO	
La solución deberá contar con un sistema de prevención de intrusos basado en el host (HIPS)	SI
El sistema de HIPS deberá contar con los siguientes modos	Modo automático, modo Inteligente, , modo Interactivo, modo, basado en políticas, modo aprendizaje
Sistemas Operativos Windows ME, Linux Y MAC-OS	SI
La solución deberá contar con un firewall personal que permita o deniegue las conexiones en base a alguno de los siguientes modos	Modo automático, modo Interactivo, modo aprendizaje, modo basado en políticas.
La solución deberá contar con un módulo de boqueo de exploits que evite la explotación de vulnerabilidades en las aplicaciones más comunes.	Navegadores web , lectores de PDF, clientes de correo electrónico y componentes de MS Office
Memoria RAM mínima necesaria	1.024 Mb
CIFRADO	

CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
La solución tendrá que contar con un complemento de cifrado que tenga como mínimo las siguientes características.	Cifrado de archivos y carpetas, Complemento para correo electrónico y archivos adjuntos de Outlook
La solución de cifrado tendrá que contar con certificación FIPS 140-2 level 1.	SI
La solución de cifrado deberá contar con los siguientes algoritmos y estándares	AES 256 bit, AES 128 bit, SHA 256 bit, SHA1 160 bit, RSA 1024 bit, Triple DES 112 bit y Blowfish 128 bit.
La solución debe permitir la administración de políticas de cifrado tanto en redes LAN como en redes WAN.	SI
La solución tendrá que contar con un destructor seguro de documentos tipo papelera.	
La solución debe contar con un lector de elementos cifrados gratuito para los usuarios que no utilicen el cifrado.	SI
La solución debe permitir el cifrado de texto y portapapeles	SI
El esquema de cifrado debe estar bajo el modelo de llave privada.	SI
GENERALES	SI
Totalidad de la interfaz en idioma español tanto en consola como en cliente.	SI
Permite instalar una consola de administración remota a la principal para administrar	

CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
Instalador de la solución BOOTEABLE para analizar maquinas sin instalar	SI
Incluye la opción monousuaria sin consola	SI
Protección máxima mediante reconocimiento proactivo y basado en firmas	SI
CONSOLA DE ADMINISTRACION	
Instalación	SI
Instalación de Consolas secundarias para garantizar la ALTA DISPONIBILIDAD	SI
Permite integración con la autenticación de Windows	SI
Permite configurar los intervalos de actualizaciones de firmas y de producto	SI
Permite configurar notificaciones de correo electrónico para eventos de la red	SI
Al abrir la consola se debe ver monitor de estado del producto tanto local como en la red	SI
INSTALACION	SI
Puede crear un instalador del producto desde la consola que incluya las actualizaciones más recientes a fin de agilizar el proceso en caso de tener problemas con la instalación remota.	SI
Puede enviar mensajes desde la consola a los equipos cliente para informar actividades a realizar con el equipo.	SI
Permite crear restricciones de análisis para unidades directorios archivos o procesos que se	SI

CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
ejecuten en las maquinas con el fin de evitar conflictos con aplicativos internos.	
Puede proteger opciones de configuración mediante una contraseña	SI
Permite integrar los dispositivos Móviles, Smartphone - Android a la consola y administrarlos desde la misma consola.	SI
Permite visualizar y administrar la consola desde cualquier Smartphone con tecnología Androide	SI
BACKUPS	SI
El proponente debe garantizar la disponibilidad del servidor de antivirus atraves de la copia y restauración del sistema en caso de fallo.	SI
Debe permitir la exploración de copias de seguridad por medio de unidades virtuales.	SI
Permite la restauración de copias de seguridad independiente del hardware del sistema anfitrión, ya sea físico o virtual.	SI
La solución debe permitir el almacenamiento de las copias de seguridad en ubicaciones de red locales, remotas y medios extraíbles.	SI
La solución debe ser compatibles con sistemas operativos Windows y Linux en sus versiones servidor.	Windows Server / 2000, 2003,2008 y 2012 / 2012 R2 / 2008 R2 x64 Con y sin Hyper-V - CentOS ,Ubuntu, Red hat.
Debe garantizar la confidencialidad de la información contenida en las copias atraves de un mecanismo de cifrado.	SI

CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
Se debe permitir la exclusión de archivos que no se deseen incluir en la copia por medio de extensiones de archivo.	SI
Creación y generación de Informes detallados de las características implementadas.	SI
CERTIFICACIONES	SI
Certificación expedida por el Mayorista o representante de la marca en Colombia, donde conste que está Autorizado a: Comercializar, soportar, y capacitar en el producto mínimo desde hace 1 año.	SI
SERVICIOS INCLUIDOS	SI
Desinstalación completa del producto antivirus anterior	SI
Instalación y configuración de la red	SI
Soporte Remoto	SI
Capacitación Remota.	SI
Soporte técnico en sitio ilimitado sin costo durante el licenciamiento	SI
Soporte técnico 24/7 vía: telefónica, chat o mensajería instantánea	SI

DISPOSICIÓN DE RESCATE Y CONTINGENCIA

Se debe garantizar que ante contingencias, catástrofes o accidentes, la Corporación podrá continuar con su operación en el menor plazo posible y con los menores traumatismos posibles. Para esto se deben:

- Determinar los mínimos necesarios para que la Corporación pueda continuar la operación en casos de contingencia.
- Diseñar y establecer planes de contingencia soportadas en concordancia con el Procedimiento de Administración de Servidores y copias de seguridad.
- Crear, adquirir o implementar herramientas para la continuidad del negocio.
- Realizar pruebas al plan de continuidad del negocio una vez implementado.
- Se debe asegurar un control y seguimiento al plan de Seguridad informática en concordancia con el Procedimiento de Administración de Servidores y copias de seguridad enmarcadas dentro del PETIC.
- Cumplir con lo dispuesto en los Procedimientos de Administración y Restauración de Copias de Seguridad y Administración de servidores.
- Realizar instructivos para pruebas de restauración de información para las diferentes aplicaciones y las diferentes plataformas. (Copias de seguridad)
- Crear imágenes completas del sistema operativo de los servidores. (Administración de servidores).
- Ante cualquier problema de hardware en los servidores sin importar su funcionalidad o al grupo de trabajo que sirvan deberán ser separados de manera local y de no ser así, deberán ser retirados los discos de almacenamiento y resguardarlos en sitio seguro.
- Verificar periódicamente que los relojes de los sistemas de procesamiento de información estén sicronizados. (Administración de servidores).
- Identificar activos críticos y sus responsables.
- Socializar adecuadamente los procedimientos, planes, manuales e instructivos del grupo de sistemas a todos los usuarios e inculcarlos en buenas prácticas de utilización de sus elementos de cómputo asignados y todos los servicios tecnológicos dispuestos en la Corporación.

POLÍTICAS DE SEGURIDAD

Es un conjunto de requisitos definidos por los responsables de la seguridad informática dentro de la CRC, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema."

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la CRC con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Con el fin de asegurar la dirección estratégica de la Entidad, la CRC establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la CRC.
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la CRC y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

- La CRC ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- La CRC protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- La CRC protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La CRC protegerá su información de las amenazas originadas por parte del personal.
- La CRC protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La CRC controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La CRC implementará control de acceso a la información, sistemas y recursos de red.
- La CRC garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La CRC garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La CRC garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- La CRC garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

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

ESTRATEGIAS

(PETIC 2015, 6.1.3.)

1. Articulación de las actividades del Plan de Seguridad Informática dentro del Plan de Acción de la Corporación.
2. Apoyo especializado en temáticas de seguridad informática.
3. Apoyo directivo a la temática de seguridad informática.
4. Amplia difusión de las políticas y normas de seguridad para garantizar su cumplimiento.
5. Cronogramas para la implementación de la seguridad informática soportadas en concordancia con el Procedimiento de Administración de Servidores y copias de seguridad.
6. Control y seguimiento al plan de Seguridad informática en concordancia con el Procedimiento de Administración de Servidores y copias de seguridad. (PETIC 2015, 6.1.4.)

RECURSOS

1. Activos.
2. Servidores.
3. Firewall.
4. Documentación y consultoría.
5. Nuevos desarrollos o adaptación de los actuales a la web.
6. Ingenieros en configuración de firewall, TCP/IP, ingenieros en soporte.
7. Conectividad permanente a Internet.
8. Dispositivos de almacenamiento.
9. Infraestructura corporativa.
10. Recurso humano: Directivos, Funcionarios y/o contratistas grupo sistemas.

ETAPAS DEL PLAN

PREVIAS A LA IMPLEMENTACIÓN

Diagnóstico específico a Servicios de TI, incluyendo:

- Verificar e identificar los controles y mecanismos necesarios para el cumplimiento del lineamiento de Control de consumo de los recursos compartidos por Servicios tecnológicos.
- Verificar e identificar los controles y mecanismos necesarios para el cumplimiento del lineamiento de Gestión preventiva de los Servicios tecnológicos.
- Verificar e identificar los controles y mecanismos necesarios para el cumplimiento del lineamiento de Respaldo y recuperación de los Servicios tecnológicos.
- Verificar e identificar los controles y mecanismos necesarios para el cumplimiento lineamiento del Análisis de vulnerabilidades.
- Realizar el Diagnóstico del estado actual de los procedimientos “Copias de Seguridad” y “Soporte técnico y Funcional”
- Verificar e identificar los controles y mecanismos necesarios para el cumplimiento del lineamiento de Monitoreo de seguridad de infraestructura tecnológica.
- Verificar e identificar los controles y mecanismos necesarios para el cumplimiento del elemento Seguridad, privacidad y trazabilidad de Servicios Tecnológicos.
- Verificar e identificar los controles y mecanismos necesarios para el cumplimiento del elemento Aseguramiento, control de calidad y transparencia de Servicios Tecnológicos.
- Inventario detallado y clasificado de activos de información según metodología Magerit v3.
- Compilación total de diagnóstico de seguridad de la Información de la CRC.

Plazo: Diciembre de 2017

Responsables: Grupo de Sistemas

PROPIAS DE LA IMPLEMENTACIÓN

Control y planeación operacional

- Inventario de Activos de Información
- Plan de Tratamiento de Riesgos
- Declaración de Aplicabilidad
- Indicadores de Gestión de Seguridad de la Información
- Plan de transición de IPv4 a IPv6
- Aseguramiento del Protocolo IPv6

Plazo: Diciembre de 2018

Responsables: Grupo de Sistemas, Grupo SIAC

EVALUACIÓN DE DESEMPEÑO

Monitoreo, medición, análisis y evaluación

- Plan de seguimiento y revisión del plan revisado y aprobado por la alta Dirección.
    - Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
    - Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
    - Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del plan.
    - Seguimiento al alcance y a la implementación del plan.
    - Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
    - Medición de los indicadores de gestión del plan.
    - Revisiones de acciones o planes de mejora (desde la segunda revisión en adelante).

- Plan de ejecución de auditorías y revisiones independientes al plan revisado y aprobado por la Alta Dirección.
- **Plazo:** Marzo de 2019
- **Responsables:** Grupo de Sistemas, Grupo SIAC, Control Interno

MEJORA CONTINUA

Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del Plan de Seguridad Informática.

Resultados del plan de ejecución de auditorías y revisiones independientes al Plan de Seguridad Informática.

- **Plazo:** Marzo 2019 en adelante
- **Responsables:** Grupo de Sistemas, Grupo SIAC

REFERENCIAS BIBLIOGRÁFICAS

- Magerit v3 Libro 1, Páginas 8, 22, 99, 114.
- ISO/IEC 27000:2009
- UNE-ISO Guía 73:2010
- Plan Estratégico de las Tecnologías de la Información y las Comunicaciones (PETIC). 2015-2019- Resolución 8213 de 07 de Diciembre de 2015.
- Plan de Seguridad Informática 2016 – Corporación Autónoma Regional del Cauca
- Modelo de Seguridad y Privacidad de la Información – Ministerio de las Tecnologías de la Información y las Comunicaciones (2016)
- VELÁSQUEZ Quintana, Gustavo. La Investigación Ciencias En La Escuela De Básicas, Tecnología E Ingeniería, UNAD - 2011.
- GALEANO VILLA, Jorge Luis - ALZATE CASTAÑEDA, Cristian Camilo, "Protocolo de Políticas de Seguridad Informática para las Universidades de Risaralda", disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1