Corporación Autónoma Regional de la Orinoquia, Corporinoquia

“Por una Región Viva, 2016-2019”

Política de la Gestión de la Seguridad de la información en la Corporación Autónoma regional de la Orinoquia, Corporinoquia

Trabajo presentado por: Jacksons Medina Romero

Ciudad: Yopal

Fecha: 13/06/2017

TABLA DE CONTENIDO

1 POLÌTICA DE GESTIÒN DE LA SEGURIDAD DE LA INFORMACIÒN DE CORPORINOQUIA 4
1.1 Introducción 4
1.2 Objetivo 4
1.3 Alcance 5
1.4 Términos y Definiciones 5
1.5 Política de la Seguridad de la Información 7
1.5.1 Compromiso de la Dirección 7
1.6 Política de Organización de la Seguridad de la Información 9
1.6.1 Política de Roles y Responsabilidades de Aplicación de la Política de Seguridad 9
1.6.2 Aspectos importantes en la organización Interna 10
1.6.3 Lineamientos para el uso y apropiación de dispositivos móviles 11
1.7 Políticas de Seguridad de los Recursos Humanos 13
1.7.1 Antes de Asumir el empleo 13
1.7.2 Durante la ejecución del Empleo 14
1.7.3 Terminación y cambio de empleo 14
1.8 Política de Seguridad de Gestión de los Activos 14
1.8.1 Responsabilidades por los activos 15
1.8.2 Clasificación de la Información 17
1.8.3 Manejo de Medios 19
1.9 Políticas de Seguridad de Control de Acceso 20
1.9.1 Acceso a la red de datos de Corporinoquia 20
1.9.2 Gestión de Acceso de Usuarios 21
1.9.3 Responsabilidades de los usuarios 22
1.9.4 Control de Accesos a sistemas y aplicativos 22

1.10 Políticas de Criptografía 23
1.11 Políticas de Seguridad Física y del Entorno 23
1.11.1 Normas de áreas seguras 24
1.11.2 Equipos 26
1.12 Políticas de Seguridad de las Operaciones 28
1.12.1 Procedimientos, Operaciones y Responsabilidades 28
1.12.2 Protección contra códigos maliciosos 28
1.12.3 Copias de Respaldo 29
1.12.4 Registro y seguimiento 30
1.12.5 Control de software Operacional 30
1.12.6 Gestión de la Vulnerabilidad Técnica 31
1.13 Políticas de Seguridad de las Comunicaciones 31
1.13.1 Gestión de la seguridad de las redes 31
1.13.2 Transferencia de Información 32
1.14 Políticas de Adquisición, Desarrollo y Mantenimiento de Sistemas 34
1.14.1 Requisitos de Seguridad de los sistemas de información 34
1.15 Políticas de Seguridad en las Relaciones con los Proveedores 36
1.15.1 Seguridad de la Información en relación con los proveedores 36
1.16 Políticas de Seguridad en Gestión de los Incidentes de Seguridad de la Información 37
1.16.1 Gestión de Incidentes y mejoras en la Seguridad de la Información 37
1.17 Políticas de Seguridad de La Información para la Gestión de la Continuidad del Negocio 38
1.17.1 Continuidad de la Seguridad de la información 38
1.17.2 Redundancias 38
1.18 Políticas de Seguridad para el Cumplimiento 39
1.18.1 Cumplimiento de requisitos legales y contractuales 39
2 REFERENCIAS BIBLIOGRAFICAS 41

1 POLÌTICA DE GESTIÒN DE LA SEGURIDAD DE LA INFORMACIÒN DE CORPORINOQUIA

1.1 INTRODUCCIÓN

La Corporación Autónoma Regional de la Orinoquia, Corporinoquia, identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que la misma, establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por el Corporinoquia. Para la elaboración del mismo, se toman como base el Manual de Gobierno en Línea, la Metodología de Análisis de Riesgos de Mayerit, la norma ISO 31000, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de Corporinoquia y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para Corporinoquia y por tanto es responsabilidad de todos los funcionarios y personal vinculado a la misma, velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

1.2 OBJETIVO

Brindar un instrumento guía para gestionar el uso, acceso y tratamiento de la información corporativa, como medio de gestión de la seguridad para la salvaguarda de los activos (información física, digital y herramientas tecnológicas (hardware y software)) de la Corporación Autónoma Regional de la Orinoquia, Corporinoquia.

1.3 ALCANCE

Este documento de política de gestión de la Seguridad de la Información, SGSI, aplica para la Corporación Autónoma Regional de la Orinoquia, Corporinoquia, en lo que tiene que ver con la seguridad de la información en cada uno de los procesos del Sistema de Gestión de Calidad, para las diferentes sedes de la Corporación (Sede principal Yopal, Dirección Territorial de Corporinoquia en Arauca y Primavera, y Unidad Ambiental en Cáqueza Cundinamarca), como oficinas de gran importancia en la generación de información que se genera, la necesidad de su administración y protección que se debe tener en cuanto a la exposición del riesgo a que se encuentra expuesta y que debe ser controlado.

Adicionalmente, aplica para el personal interno y externo que esté vinculado a sus procesos Corporativos, bien sea por vinculación de planta, provisional o contratista.

Para esta actividad, la Corporación, destinará un profesional Especializado para la gestión de la seguridad de la información, quien será el encargado de integrar la política de gestión de la Seguridad de la Información, con el sistema de Gestión de Calidad Corporativo de procesos.

El liderazgo del proceso de gestión de la Seguridad de la Información será ejercido por la alta dirección de la organización.

1.4 TÉRMINOS Y DEFINICIONES

Seguridad de la información: son todas las medidas necesarias utilizadas para prevenir ataques a la disponibilidad, confidencialidad e integridad de los activos de información y los sistemas de tecnología que permitir resguardarla y protegerla dentro de las organizaciones (WIKIPEDIA, 2015).

Control de acceso: Todos los procesos y procedimientos que debe cumplir un usuario o un elemento tecnológico para obtener la autorización de acceso a una aplicación, sistema de información, equipo o área restringida.

Autenticación: es el mecanismo de comprobación de la veracidad de la identidad de un usuario o activo tecnológico al intentar acceder a un recurso de procesamiento o sistema de administración de información.

Cifrado: combinación y transformación de datos mediante el uso de técnicas criptográficas para producir datos ininteligibles, asegurando su confidencialidad. A través del cifrado se previene la fuga de información, el acceso no autorizado a la misma y es utilizado como medio de protección de la misma.

Criptografía: Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.

Confidencialidad: es la garantía de que la información esté disponible y habilitada solo para el personal, entidades o procesos autorizados mediante protocolos de control de acceso.

Disponibilidad: es la garantía de que, a la información, equipos u otro tipo de activo, se tenga acceso en el momento que se requiera.
Integridad: es la protección del estado completo de los activos. Que se mantenga al 100% en todos sus componentes.

Perfiles de usuario: es la agrupación de varios usuarios con similares necesidades de información, autorizaciones y/o rango de permisos, sobre los diferentes recursos de tecnología y sistemas de información corporativos, facilitando los accesos de acuerdo con las funciones realizadas. Cuando se realizan modificaciones sobre perfiles de usuario, estas afectan a todos los usuarios pertenecientes al perfil.

Sistema de Información: conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información, orientado al tratamiento y administración de datos que interactúan con activos de información para efectuar sus tareas e informes para la toma de decisiones.

Vulnerabilidades: son todas las debilidades de protección del activo y que en un momento determinado atenta contra la seguridad del mismo. Las vulnerabilidades pueden ser explotadas por factores externos y no controlables por la Corporación. Se pueden constituir en fuentes de riesgo que pueden llegar a ser vulneradas en un momento determinado.

1.5 POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

La información de la Corporación Autónoma Regional de la Orinoquia, Corporinoquia es uno de los activos más importantes para la prestación eficaz, eficiente y efectiva de su objeto misional como es "*Corporinoquia como autoridad ambiental y administradora de los recursos naturales, gestiona el desarrollo sostenible, garantizando la oferta de bienes y servicios ambientales, mediante la implementación de acciones de prevención, protección y conservación Por una Región Viva*"[1] (CORPORINOQUIA, 2015). Dicha información ayuda en la toma de decisiones de forma eficiente, por dicho motivo existe un compromiso de protección hacia la información como una estrategia en la continuidad del negocio, administración de los riesgos de los activos, la construcción y aseguramiento de una cultura de seguridad de la información.

Esta guía define un conjunto de Políticas para la seguridad de la información, la cual, a través del compromiso decidido de la alta dirección, se aprueba, se publica y se comunica a todos los actores intervinientes dentro del proceso de gestión de la seguridad de la información.

Va dirigida a todos los funcionarios, personal externo, e interno y todo aquel que tenga responsabilidad con el uso de información física y digital de Corporinoquia, para que se adopten los lineamientos establecidos, para proteger y conservar la integridad, confidencialidad, garantizando la disponibilidad de la información física y digital, como medio de consulta y continuidad de todos los procesos misionales y de apoyo de la Corporación.

Esta política de gestión de la seguridad de la información está fundamentada en los dominios y objetivos de control del Anexo A de la norma ISO 27001:2013.

1.5.1 Compromiso de la Dirección

La Corporación está conformada por el Consejo Directivo quien es el órgano que autoriza y aprueba la Política de Seguridad de la información de Corporinoquia, como un compromiso de la alta dirección en la generación de políticas eficaces y eficientes que garanticen la seguridad de la información ambiental de la Orinoquia Colombiana.

[1] Misión Corporinoquia: Tomado del documento PGA-MAN-001 Manual de Calidad del Sistema de Gestión de Calidad de Corporinoquia.

El Consejo Directivo y la Alta Dirección de Corporinoquia demuestran su compromiso a través de:

- La verificación, análisis, validación y aprobación de las Políticas de Seguridad de la información de Corporinoquia, habilitadas en la Presente Política de Gestión de la Seguridad de la información.
- La sensibilización y promoción de una cultura de seguridad de la información.
- Divulgar a cada uno de los funcionarios de Corporinoquia, el documento “Política de Gestión de la Seguridad de la Información de Corporinoquia”.
- Asegurar los recursos necesarios para implementar y mantener las políticas de seguridad de la información de Corporinoquia.
- El seguimiento y control de cumplimiento de las políticas mencionadas en el presente documento.

La alta Dirección liderará el cumplimiento de la Política de Seguridad de la Información y gestionará la conformación de un Comité de Gestión de Seguridad del Información en Corporinoquia, el cual estará conformado por miembros de las siguientes áreas:

- Dirección General o su delegado
- Subdirección de Planeación Ambiental o su delegado
- Representante de la Oficina de Sistemas
- Subdirección Administrativa y Financiera o su delegado
- Subdirección de Control y Calidad Ambiental o su delegado
- Secretaria General o su delegado
- Oficina de Control Interno o su delegado
- Oficina Jurídica o su delegado
- Dirección Territorial de Arauca o su delegado
- Dirección Territorial la primavera o su delegado
- Oficina Ambiental de Cáqueza o su delegado

Dicho Comité tendrá funciones específicas de generar estrategias y mecanismos que garanticen la seguridad de la información en Corporinoquia, así como brindar apoyo en la revisión de las políticas, de acuerdo a cambios significativos, asegurando su conveniencia, adecuación, y eficacia y mejoramiento continuo.

1.6 POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La presente política de gestión de la seguridad de la información busca enmarcarse dentro del objeto misional de Corporinoquia, como una herramienta que permite la gestión de la seguridad de la información para la continuidad y gestión de los procesos. Dichas normas van dirigidas al manejo que los usuarios de la Corporación, deben tener en cuenta en cada uno de sus áreas de trabajo y su relación con el uso de la información y los demás activos de la Corporación. Adicionalmente, se abordará con respecto a los roles y funciones desempeñadas dentro de la organización con respecto a administración, operatividad y gestión de la seguridad de la información.

Define la responsabilidad en el uso de activos, permitiendo la gestión de la seguridad de los mismos, a través de la identificación de cada uno de los riesgos de los activos relacionados con el uso de la información de la Corporación.

1.6.1 Política de Roles y Responsabilidades de Aplicación de la Política de Seguridad

La responsabilidad y aplicación de la seguridad de la información es de carácter obligatorio para todo el personal vinculado a la Corporación, cualquiera que sea su tipo de vinculación, la sede o Subdirección a la cual se encuentra adscrito y el nivel de funciones o actividades que desempeñe.

El Comité de Seguridad de la Información será el encargado de gestionar todo lo relacionado con la gestión de la seguridad de la información, para lo cual, deberá realizar un plan de acción para ejecutar en cada vigencia, este debe incluir las revisiones y actualizaciones a que haya lugar, en busca del mejoramiento continuo.

Dentro del Comité de gestión de la seguridad de la información se debe nombrar un representante que será quien lidere las acciones del comité, así como de impulsar e implementar el cumplimiento de la Política de Seguridad.

La oficina de Talento Humano deberá realizar la divulgación de la aplicación de la Política de Seguridad de la información, a todo el personal que se vincule a Corporinoquia, independientemente del tipo de vinculación que tenga. Todo el personal vinculado a la entidad deberá firmar un acuerdo o compromiso donde exprese la intención de cumplimiento de la

Política de Gestión de la Seguridad de la información, el uso adecuado y cuidado de las herramientas TIC dentro y fuera de la corporación. Para el personal contratista se deberá dejar estipulado en el contrato de vinculación. Para el personal de Carrera, planta o provisional se realizará mediante carta de compromiso, según formato establecido por el área de talento humano.

Los usuarios responsables de los activos de información son responsables de su clasificación, mantenimiento y actualización, así como de documentar. Se debe definir los usuarios que tengan acceso a estos activos y a que información pueden acceder, y deben definir los tipos de permisos y roles a tener par la respectiva autenticación y autorización de acceso.

Los funcionarios de sistemas de Corporinoquia, serán los responsables de cumplir con la seguridad de los sistemas de información de la misma, lo que incluye la operación del Sistema de Gestión de la Seguridad de la Información SGSI y supervisión dentro del área de sistemas de lo definido en la política de Seguridad de la Información. Los usuarios de sistemas de información deben velar por el cuidado de sus contraseñas accesos al sistema.

Dentro de las responsabilidades que se deben cumplir en el presente ítem, hace parte el apartado “1.5.1 Compromiso de la Dirección”.

1.6.2 Aspectos importantes en la organización Interna

Las políticas de seguridad de la información generados en el presente documento, son los lineamientos que buscan defender, proteger y resguardar la información en Corporinoquia, por lo tanto, cualquier violación a lo establecido en las mismas está sujeto a la aplicación de medidas correctivas de acuerdo a los niveles de clasificación de las violaciones y mitigar posibles afectaciones contra la seguridad de la información. Estas medidas de protección se enmarcan desde: medidas administrativas hasta apertura y ejecución de procesos disciplinarios, dependiendo del nivel de afectación puede llegar a ser de tipo penal.

En los casos en que se materialice un riesgo o se presente una anomalía relacionada con el contenido de la política de seguridad de la información y dependiendo de la magnitud de la misma, se debe reportar de inmediato al jefe inmediato del área donde se presente el hallazgo, seguidamente a la oficina de Control Interno y Oficina de Control Interno Disciplinario. Si el caso da para investigación se debe hacer un llamado a las autoridades pertinentes que conozcan de la gestión de seguridad de la información, para que brinden el acompañamiento

necesario, como lo es la Policía Nacional de delitos informáticos de Colombia, más exactamente la de Yopal, Casanare, para que realice la investigación o la asesoría necesaria en caso de llegar a necesitarse. Así mismo, dependiendo si la falta lo amerita, se deberá informar a los entes de control como son Procuraduría General de la Nación, Fiscalía General de la Nación y Contraloría General de la Nación.

Adicionalmente, la Corporación deberá realizar las acciones necesarias para mantenerse en constante actualización, para lo cual debe gestionar a través del Comité de Seguridad de la Información las capacitaciones necesarias e inscripciones a grupos de interés expertos en seguridad de la información en búsqueda de retroalimentación y el mejoramiento continuo del proceso.

1.6.3 Lineamientos para el uso y apropiación de dispositivos móviles

Corporinoquia a través de la oficina de sistemas proveerá los mecanismos necesarios de seguridad y de acceso de los dispositivos móviles como teléfonos, tabletas, portátiles y demás elementos de conexión inalámbrica de uso corporativo y personal que hagan uso de los servicios y equipos proporcionados por la Corporación, y en los casos autorizados, por la alta dirección, para lo cual se debe:

Investigar las tecnologías necesarias en materia de seguridad informática enfocada a dispositivos móviles, realizar las pruebas necesarias para la protección de los dispositivos

Realizar las configuraciones necesarias aceptables para cada uno de los dispositivos móviles personales o corporativos. Para lo cual se debe establecer métodos de bloqueo y control de acceso personalizado, como contraseñas, patrones de reconocimiento, biometría, reconocimiento de voz a cada uno de los usuarios y dispositivos móviles asignados. Deben tener control de tiempos de uso para el bloqueo automático de los dispositivos y aumentar la seguridad de la información.

Todos los dispositivos móviles y equipos de cómputo que se conecten a los servicios de tecnología de la Corporación, sin excepción deben contar con un antivirus.

Todos los dispositivos móviles entregados a los usuarios para su uso, se entregan configurados. Ningún usuario está autorizado para cambiar o modificar la configuración, instalar o desinstalar software. Cualquier necesidad al respecto debe ser solicitada al área de

sistemas para su correspondiente viabilizarían. Solo se permitirán las actualizaciones que los programas instalados soliciten.

La oficina de sistemas debe llevar un registro de dispositivos móviles asignados y con acceso a la plataforma tecnológica corporativa, especificando los datos básicos del dispositivo, los permisos asignados y los datos del usuario al cual se le asigna el activo.

Los usuarios deben evitar el uso de dispositivos móviles Corporativos en redes externas a las autorizadas por la corporación, como medida de precaución y cuidado de la información que en estos equipos se maneje. Esto ayuda a evitar pérdida o robo de los activos (información y/o dispositivo). Se debe desactivar las opciones de Bluetooth e infrarrojo para evitar fuga de información.

El uso de los dispositivos móviles de la Corporación, es para uso corporativo y la información que repose en los mismos debe ser de carácter laboral y corporativo.

Los usuarios deben evitar introducir los dispositivos móviles corporativos a otros equipos de cómputo de dudosa reputación como por ejemplo computadores públicos, de hoteles, entre otros.

Para los casos de conexión remota de funcionarios a los sistemas de información y servicios de red de la corporación, a través de la Política de seguridad de la información se establece:

Identificar los riesgos que tendrá cada uno de las posibles conexiones remotas, los tipos de acceso, tiempos de conexión, permisos a otorgar, entre otros. Se deben definir los controles necesarios y su efectividad, los cuales serán verificados constantemente.

Las conexiones remotas a equipos de cómputo y servidores, se deben evitar. Solo personal autorizado por el Comité de Seguridad de la Información de la Corporación, podrá realizar actividades de acceso remoto y por un periodo de tiempo. Los permisos se otorgarán de acuerdo a las funciones desempeñadas. Los usuarios acataran las condiciones de uso establecida para las conexiones remotas. El acceso remoto se otorgará a equipos identificados por la corporación. Estas solicitudes de acceso remoto deberán estar justificada por el Jefe Inmediato del área, y será evaluada en reunión del comité mencionado.

La oficina de control interno de la Corporación dentro de su proceso de auditoría interna, deberá verificar la eficacia de los controles implantados para las conexiones de acceso remoto.

1.7 POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

1.7.1 Antes de Asumir el empleo

El recurso humano para Corporinoquia es uno de los activos más importantes en la gestión de los procesos misionales y de apoyo, por lo tanto, es importante garantizar contar con el personal mejor calificado, para lo cual, se deben definir unos estándares de seguridad que aseguren un proceso formal de selección, orientado a las funciones, cargo y roles que desempeñara al interior dela corporación cada funcionario, para lo cual se debe:

En los procesos de selección de personal para suplir vacantes, se debe verificar la veracidad y autenticidad de la información suministrada por el candidato a ocupar un cargo en Corporinoquia. Esta verificación será un requisito de cumplimiento antes de vincular al nuevo personal.

La oficina de Talento Humano deberá realizar la divulgación de la aplicación de la Política de Seguridad de la información, a todo el personal que se vincule a Corporinoquia, independientemente del tipo de vinculación que tenga. Todo el personal vinculado a la entidad deberá firmar un acuerdo o compromiso donde exprese la intención de cumplimiento de la Política de Gestión de la Seguridad de la información, el uso adecuado y cuidado de las herramientas TIC, dentro y fuera de la corporación.

Cada supervisor o jefe inmediato deberá comprobar el cumplimiento de la firma de los acuerdos de confidencialidad de la información por parte de los contratistas o funcionarios asignados, antes de autorizar el acceso a la información. Esta política aplica para todo el personal inclusive al provisto por empresas contratistas que realicen labores en Corporinoquia.

1.7.2 Durante la ejecución del Empleo

Para iniciar a ejecutar labores del empleo el funcionario debe firmar el acuerdo de confidencialidad de la información. Y este debe aplicar la Política de Seguridad de la información con el fin de garantizar la integridad, confidencialidad y disponibilidad de la información en la Corporación.

El área de talento humano en conjunto con el área de sistemas de Corporinoquia, deben establecer jornadas de capacitación en temáticas relacionadas con la seguridad de la información. La asistencia de todo el personal de planta es de carácter obligatorio y la asistencia por parte de contratistas es obligatoria dependiendo del grado de relación con la información misional y de apoyo de la Corporación, según sus funciones y cargo.

La oficina de Control Interno Disciplinario debe establecer un proceso sancionatorio formal, el cual debe ser socializado y conocido por todos los funcionarios. Este procedimiento facilitará los mecanismos para emprender acciones contra empleados o contratistas que hayan cometido violaciones a la seguridad de la información.

1.7.3 Terminación y cambio de empleo

Se debe definir las responsabilidades y los deberes de la seguridad de la información que deben asumir los funcionarios o contratistas que terminen su vinculación laboral con Corporinoquia, en el acuerdo de confidencialidad de la información firmado por las partes, así como en el proceso contractual vinculante. El supervisor o jefe inmediato tendrá la responsabilidad de asegurar que toda la información suministrada al funcionario al momento de ingreso y la generada en el desarrollo de su proceso laboral en la Corporación, por el funcionario a retirar sea entregada en su totalidad y que se garantice su confidencialidad.

1.8 POLÍTICA DE SEGURIDAD DE GESTIÓN DE LOS ACTIVOS

Corporinoquia como propietaria de la información física e información digital procesada, almacenada y transmitida desde la infraestructura tecnológica y la física en cada una de las áreas, Centro de Documentación y bodega de archivo de la Corporación, otorga responsabilidad sobre los activos de información asignada a cada una de las subdirecciones, Secretaria General y Direcciones Territoriales, asegurando el desempeño de la presente política de seguridad de la información.

Los sistemas de información, la información, los equipos de cómputo de escritorio y portátil, la red de datos, scanner, impresoras, UPS, planta eléctrica y todo el conjunto de plataforma tecnológica propiedad de Corporinoquia, son activos de la misma, y son asignados a cada uno de los funcionarios, contratistas y personal autorizado como herramientas de apoyo al cumplimiento del objeto misional de la Corporación.

Los activos donde se encuentre la información almacenada deben estar asignados a un responsable y se debe brindar las garantías de seguridad necesarias para su protección. Los propietarios de los activos a quienes se encuentran asignados por inventario, deben mantener actualizado su inventario de activos de información, utilizarlos en cada uno de sus procesos y áreas y brindarles la seguridad necesaria.

1.8.1 Responsabilidades por los activos

La Dirección General, las Subdirecciones, las Direcciones Territoriales y la Secretaria General de Corporinoquia, debe actuar como propietarios de la información física y digital de la corporación, ejerciendo la autorización de accesos a la información con los permisos de acuerdo al rol que desempeñe el funcionario.

Los propietarios de los activos deben monitorear constantemente la validez de usuarios y perfiles autorizados al acceso de información. Para esto deben contar con un listado de activos del área que lideran, la clasificación de la información, los usuarios autorizados y permisos otorgados.

Todos los activos que procesan información son sujetos de auditoria por la oficina de control interno y de revisión de cumplimiento de los controles establecidos.

La oficina de Sistemas de Corporinoquia es la propietaria de los activos de información correspondiente a la plataforma e infraestructura tecnológica (Servidores), por consiguiente, debe asegurar su operación y administración de forma eficaz.

Cualquier cambio a realizar en la infraestructura de la plataforma tecnológica debe ser autorizado por la oficina de sistemas en lo referente a instalación, cambio de equipos o traslados de la misma. Todos los recursos tecnológicos deben tener una configuración adecuada, que permita la preservación de la seguridad de la información.

La oficina de sistemas es la responsable de preparar los equipos tecnológicos para el uso adecuado de los mismos en la Infraestructura tecnológica de la Corporación (equipos de cómputo de escritorio y portátiles, impresoras, escáner, plotter, entre otros). Adicionalmente, es responsable de recibir los equipos tecnológicos para su alistamiento, asignación y reasignación e informar al almacén los cambios necesarios para el control de inventario, generar las copias de seguridad (backup) de la información de los funcionarios que se retiran o cambian de actividad o área, previa solicitud por correo electrónico enviado por parte del jefe inmediato del funcionario que entrega el equipo de cómputo. Dicha solicitud se debe presentar vía correo electrónico al email: soporte@corporinoquia.gov.co.

Se debe revisar de manera periódica los riesgos de los activos, para identificar su estado y generar nuevas medidas de control en los casos que sea necesario, identificar nuevos riesgos y controlarlos. Esta actividad debe realizarse entre el responsable del bien y la oficina de sistemas.

Se debe realizar revisiones periódicas a la funcionalidad de los recursos de la plataforma tecnológica y los sistemas de información de Corporinoquia, para identificar su estado, y generar la protección de activos de información, tecnológicos y no tecnológicos, en caso de encontrarse o no vulnerable.

El uso de los servicios tecnológicos deben ser autorizados por: Director General, Subdirectores, Secretario General, Director Territorial, Coordinadores de Área, Jefes de oficina mediante solicitud a la oficina de sistemas de Corporinoquia, al email: soporte@corporinoquia.gov.co.

El Director General, Subdirectores, Secretario General, Director Territorial, o personal designado, deben recibir los equipos de tecnología asignados a sus funcionarios (Planta o contratista) cuando estos se retiran del área. El equipo debe quedar asignado en el área al que pertenece. Se deberá informar a la oficina de sistemas los cambios realizados al email: soporte@corporinoquia.gov.co.

Cuando un funcionario, contratista u otro tipo de personal vinculado con la corporación se retira de la empresa, este debe estar a paz y salvo por todo concepto de activos y servicios informáticos asignados, para lo cual, debe comparecer a la oficina de sistemas y almacén

para la firma del respectivo Paz y Salvo, el que lo acredita que ya ha cumplido con la entrega de los activos y desactivación de servicios informáticos en la corporación.

Los recursos tecnológicos deben ser utilizados por todos los usuarios, de forma ética, eficiente y de forma exclusiva para el beneficio de Corporinoquia.

Los usuarios no deben utilizar software no autorizado en los equipos corporativos, y ningún otro elemento que afecte la infraestructura tecnología de Corporinoquia. Cualquier necesidad de software se debe informar a la oficina de sistemas para su evaluación y posterior decisión de adquirirla. No se debe usar software sin licencia en la Corporación. Los equipos de cómputo corporativo deben contar con Licencia de Antivirus y mantenerla actualizada.

Los usuarios no deben conectar cargadores de celular, ventiladores, radios, u otro tipo de dispositivos diferentes a equipos de cómputo, en la red de corriente regulada de la Corporación.

Todas las estaciones de trabajo, dispositivos móviles, impresoras, scanner, plotter, UPS, Planta Eléctrica, entre otros, son asignadas a un responsable y este a su vez velará por la seguridad, cuidado y normal funcionamiento de los mismos, a través del compromiso de uso adecuado y uso eficiente de dichos activos.

1.8.2 Clasificación de la Información

La Corporación a través del comité de seguridad de la información y el Comité de Archivo, debe definir la Guía de clasificación de la información corporativa, identificando su importancia y sensibilidad. Los propietarios de la información la deben catalogar y deben determinar los controles requeridos para preservar la confidencialidad, integridad y disponibilidad de la misma. Los niveles de clasificación de la información y sus controles deben ser aprobados por el Consejo Directivo de Corporinoquia.

La guía de clasificación de la información (sensibilidad, grado de importancia, confidencialidad, etc.), de Corporinoquia debe ser socializada a todos los funcionarios de la corporación (planta y contratistas), una vez esté aprobada por el Consejo Directivo de la misma.

La oficina de sistemas debe gestionar las técnicas de cifrado de la información, en los casos que se requiera, así como realizar la administración del software que cifra y descifra la información, teniendo en cuenta la guía de clasificación de la información. En caso de requerirse herramientas de cifrado se deben gestionar los recursos necesarios para la adquisición de las herramientas que faciliten el cumplimiento del presente ítem.

La Oficina de Sistemas debe generar las acciones para eliminar información de forma segura, en los equipos dados de baja o cuando cambian de usuario, evitando la recuperación y reconstrucción de la misma.

El comité de archivo debe autorizar la destrucción de información cuando se ha cumplido su ciclo de gestión y archivo, de acuerdo a las tablas de valoración documental de Corporinoquia. La Secretaria General como líder del proceso de gestión Documental de Corporinoquia, debe garantizar la destrucción correcta la documentación física, que ya perdió funcionalidad en el ciclo de vida documental, para evitar que pueda ser reconstruida. Los encargados de destruirla serán la Secretaria General.

La Secretaria General a través del responsable del Centro de Documentación y bodega de archivo serán los responsables de la custodia, cuidado y almacenamiento de la información física y Backup digital de la Corporación.

La Secretaria General como líder de la Gestión Documental en la Corporación, deberán garantizar la gestión de proceso de los funcionarios en cuanto a las tareas a realizar en los sistemas de información relacionados con la Gestión Documental a través de la sensibilización del uso del sistema, la verificación y revisión a través de auditorías del mismo, en relación al cumplimiento de cargue de información en los sistemas de información de forma completa.

La oficina de Sistemas de la Corporación garantizará la estabilidad funcional de los sistemas de información de la Corporación, la asignación de permisos y roles de acuerdo al procedimiento establecido en el sistema de gestión de calidad y realizará los Backup de información necesarios para reestablecer los servicios en caso de caídas del mismo.

La Secretaria General y el funcionario encargado del Centro de Documentación y bodega de archivo serán los responsables de la custodia, cuidado y almacenamiento de la información física y Backup digital de la Corporación (Transferencia de información).

La encargada del área del Centro de Documentación y Bodega de Archivo, deberá administrar los contratos relacionados con el resguardo de documentos físicos, de la Corporación. Debe contemplar toda la seguridad necesaria de los mismos, teniendo en cuenta las cláusulas de confidencialidad, integridad y disponibilidad.

Los usuarios responsables de activos de información deben monitorear la clasificación de sus activos de información y reclasificarlos cuando sea necesario. Toda la información física debe estar protegida, con controles de acceso físico y garantizar las condiciones adecuadas de almacenamiento y resguardo seguro.

Los usuarios deben acatar los lineamientos de la Guía de Clasificación de la información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como la información física de la Corporación.

La información de Corporinoquia deberá ser identificada en las tablas de retención documental, y allí se establecen los tiempos de almacenamiento para cada uno de los tipos documentales.

1.8.3 Manejo de Medios

La información de discos duros de copias de seguridad o información de manejo de información importante en el centro de datos de la Corporación, debe estar cifrada para evitar robos, alteración o pérdida de información. Para esto, la oficina de sistemas garantizará los medios necesarios para cifrar y descifrar los medios extraíbles correspondientes.

Todos los medios extraíbles asignados a funcionarios para manejo de información, deben ser registrados y dependiendo de la clasificación que se le dé a la información allí guardada es necesario generar técnicas de cifrado y descifrado. El funcionario a quien se le asigne un medio extraíble adquiere la responsabilidad de proteger la información y el activo entregado. En caso de querer devolverlo al área de almacén, el funcionario deberá informar por escrito y al correo corporativo soporte@corporinoquia.gov.co, de la la oficina de sistemas, sobre la sensibilidad y valor de la información allí guardada. la oficina de sistemas debe brindar un concepto de la información que se tiene allí almacenada y generar los mecanismos necesarios para eliminar, o proteger la información a través de un Backup de seguridad.

Los tokens de seguridad asignados a los funcionarios de la Subdirección Administrativa y Financiera son de carácter personal e intransferible y se debe mantener total seguridad por su alto grado de importancia en la realización de trámites de carácter presupuestal y financiero con el Gobierno Nacional. Los tokens asignados son de uso exclusivo en los equipos asignados por la corporación, para tal fin, en caso de pérdida se debe reportar de inmediato a la oficina de sistemas de Corporinoquia.

El área de Tesorería requerirá de un equipo de cómputo de uso exclusivo para realizar las transacciones bancarias on line con los bancos autorizados por la Corporación. No se deberá navegar en otras páginas diferentes a estas y no se deberán realizar acciones diferentes o uso de otros programas en dicho equipo. Todas las actividades adicionales se realizarán en el equipo de cómputo asignado para actividades de red interna y uso del sistema de información Financiero de la Corporación, así como los sistemas financiero s de orden nacional.

La oficina de sistemas debe implementar mecanismos que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de Corporinoquia, así como los medios para su disposición final segura. La asignación de periféricos se debe autorizar dependiendo del perfil del cargo del funcionario solicitante.

El personal de la corporación a quienes se les asigne equipos periféricos debe acogerse a las normas de uso de periféricos y medios de almacenamiento.

1.9 POLÍTICAS DE SEGURIDAD DE CONTROL DE ACCESO

1.9.1 Acceso a la red de datos de Corporinoquia

La oficina de sistemas como responsable de la red de datos y los recursos instalados en la misma, debe protegerlos contra el control de accesos no autorizados a través de mecanismos de control de acceso lógico y proteger los puntos de red que se encuentren visibles y vulnerables de ataques.

Dentro del proceso TIC, de la oficina de sistemas se debe realizar el procedimiento de autorización y controles para restringir el acceso los recursos de la red de datos de la Corporación.

Se debe implementar métodos de autenticación en el servicio de red inalámbrica que evite accesos no autorizados.

Se debe verificar periódicamente los controles de acceso, permisos, tiempos de acceso, para todos los usuarios, validando que los usuarios autorizados tengan únicamente los permisos de red y la plataforma tecnológica para los que fueron autorizados.

Todos los personales antes de contar con acceso deben ser autorizados por el jefe inmediato, solicitando a través de correo electrónico a la oficina de sistemas, al email: soportecorporinoquia.gov.co, en donde debe enviar información básica del nuevo funcionario (nombre, identificación, profesión, área asignada, rol a desempeñar y autorización de información que puede ser consultada y que tipo de permisos se le concederán (crear, modificar, eliminar).

1.9.2 Gestión de Acceso de Usuarios

La oficina de sistemas debe elaborar el procedimiento para la administración de usuarios de la red de datos, los servicios tecnológicos y sistemas de información de la Corporación. Este debe contemplar la creación, modificación, eliminación y bloqueo de las cuentas de usuarios.

La oficina de sistemas es la encargada de crear, modificar o eliminar usuarios, de la red de datos y sistemas de información corporativa, previa solicitud de los jefes de área. Lo anterior, debe contemplar la generación de contraseñas seguras, con lineamientos como longitud, complejidad, cambio periódico, cambio de contraseña en el primer acceso, control histórico y bloqueo por número de intentos fallidos en la autenticación. Estos usuarios se deben comunicar vía correo electrónico a cada nuevo usuario.

Los propietarios de los activos de información deben validar periódicamente todas las autorizaciones sobre sus recursos de acuerdo a los perfiles otorgados e informar a la oficina de sistemas, las diferencias encontradas, para llevar a cabo los cambios y controles necesarios.

1.9.3 Responsabilidades de los usuarios

Los usuarios de los recursos tecnológicos y los sistemas de información de la corporación deben realizar un uso adecuado y responsable de los mismos, protegiendo la confidencialidad y salvaguardando la información autorizada, bien sea para consulta y/o modificación.

Los usuarios no deben compartir la información de cuentas de usuario y contraseñas. Esta información es intransferible y de uso únicamente corporativo.

Cuando se presente alguna alteración de la información y otro funcionario lo descubra, está en la obligación de informarlo al jefe inmediato del área donde se presenta el hallazgo.

1.9.4 Control de Accesos a sistemas y aplicativos

Las Subdirecciones, Secretaria General y Direcciones Territoriales, actuaran como propietarias y gestoras de los sistemas de información y demás aplicativos que apoyan los procesos misionales y de apoyo de la Corporación, velaran por la asignación, modificación y revocación de privilegios de acceso a sus aplicativos de forma responsable y controlada.

La oficina de sistemas propenderá porque los diferentes sistemas de información estén protegidos de accesos no autorizados a través de mecanismos de acceso lógico, así como las exigencias necesarias de seguridad para el desarrollo de software seguro en todas las etapas de desarrollo de software.

Los Jefes de área encargados de gestionar los sistemas de información, información física y digital, y aplicativos de software, serán quienes autorizan el acceso a funcionarios, estableciendo los permisos autorizados para acceder al sistema, para lo cual lo debe solicitar al email: soporte@corporinoquia.gov.co. Estos accesos deben ser monitoreados contantemente, por los propietarios del sistema de información.

La oficina de sistemas debe realizar e implantar el procedimiento de asignación de accesos a los sistemas y aplicativos de Corporinoquia.

Los ambientes de desarrollo, pruebas y producción, deben ser ambientes separados a nivel físico y lógico, contando cada uno con sus servidores, equipos, plataforma, aplicaciones y dispositivos, para evitar fallos en la integridad de la información en producción.

La oficina de sistemas debe establecer un procedimiento de requisitos básicos de seguridad, el cual contemple autenticación, autorización, auditoria, registro de eventos, entre otros, al momento de realizar desarrollos de software o tercerizarlos. A la vez, se deben definir claramente los requisitos necesarios al momento de gestionar un proyecto de desarrollo de software en la Corporación, y controlar que estos se cumplan en los tiempos de respuesta propuestos. Adicionalmente, velar por que el desarrollo de software cumpla con las etapas del ciclo de Vida de desarrollo de Software Seguro.

La oficina de sistemas debe contar con un repositorio de archivos fuente de los diferentes sistemas de información y además se debe restringir su acceso para evitar riesgo de pérdida de la integridad, confidencialidad y disponibilidad de los aplicativos de instalación.

Los desarrolladores deben asegurar que los sistemas de información desarrollados requieran autenticación para todos los recursos y páginas del sistema, excepto las calificadas como informativas y de consulta a los usuarios externos. Adicionalmente deben tener en cuenta las diferentes restricciones de vulnerabilidades como SQL Injection y XSS, entre otras.

1.10 POLÍTICAS DE CRIPTOGRAFÍA

La Guía de clasificación de la información permite identificar la información confidencial y de mayor seguridad, por esta razón la corporación deberá implementar los mecanismos necesarios para cifrar la información en formato digital, catalogada como de uso restringido bajo técnicas de cifrado para de proteger su confidencialidad e integridad.

La Corporación, desde la oficina de sistemas deberá crear e implantar un procedimiento para administración de llaves de cifrado y protocolos para la aplicación de controles criptográficos.

1.11 POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

La Subdirección Administrativa y Financiera a través de la Oficina de Recursos Físicos, deberá velar por la gestión de controles efectivos de seguridad física y control de acceso que asegure el perímetro de las instalaciones en las sedes de la corporación y oficinas ambientales en toda su jurisdicción, evaluará los riesgos y amenazas físicas internas y externas y las condiciones medioambientales de las oficinas, los centros de documentos, bodega de archivo y los centros de datos de las mismas.

También deberá velar por que los equipos del centro de datos de la Corporación permanezcan con una temperatura por debajo de los 18°C, con el fin de garantizar la disponibilidad e integridad de la información digital Corporativa. Adicionalmente, el acceso al Centro de Datos debe ser restringido al personal autorizado, dentro de la oficina de sistemas.

Las oficinas del centro de documentos y los centros de datos de las sedes, donde se encuentra información sensible, equipos, infraestructura tecnológica y de soporte de sistemas de información y red de comunicaciones, su acceso será restringido. La autorización la otorga la Secretaria General, al Centro de Documentos y el Subdirector de Planeación y el líder de la Oficina de Sistemas a todo lo relacionado con tecnología.

1.11.1 Normas de áreas seguras

Los accesos al centro de datos de cómputo o a los centros de cableado deben ser autorizados por el Subdirector de Planeación Ambiental o en su defecto el líder de la oficina de Sistemas. Los ingresos a estas áreas deben estar acompañadas por personal de planta de la Oficina de Sistemas de la Corporación y deben ser registrados los ingresos en una bitácora que se debe ubicar al ingreso del centro de datos.

Funcionarios o contratistas de la oficina de sistemas o personal que cuente con permisos y autorización de acceso a centro de datos de computo o centro de cableado y que sea descontinuado o trasladado de área, se le deben quitar de forma inmediata los privilegios de acceso al centro de cómputo (servidores) y centro de cableado.

La Subdirección Administrativa y Financiera a través de la oficina de recursos físicos deberá facilitar un sistema de control ambiental (en cuanto a flujos de temperatura y humedad), con generación automático de alertas y detecciones de cambios de temperatura (condiciones ambientales) en el Centro de Datos de la Corporación, Sección de Planta eléctrica y Centro de UPS, que permitan actuar ante cualquier cambio brusco de temperatura, para mantener la protección y normal funcionamiento de los recursos en las áreas mencionadas.

Adicionalmente, se debe contar con sistemas de detección y extinción de incendios, al interior de las sedes de la Corporación, junto con sistemas de vigilancia, seguridad física y monitoreo.

La Subdirección Administrativa y Financiera a través de la oficina de recursos físicos y la Subdirección de Planeación Ambiental a través de la oficina de Sistemas, deberá velar por el normal funcionamiento y mantenimiento de la red eléctrica, red de voz (telefonía) y la red de datos (cableado estructurado), se debe realizar bajo programación y lo debe realizar personal idóneo y calificado.

Se debe asignar la responsabilidad a un funcionario de planta de la oficina de sistemas para que realice control y monitoreo de los sistemas de alarmas de los sistemas de seguridad de los equipos del centro de datos y centros de cableado de la Corporación.

La oficina de Recursos Físicos proporcionara los recursos y elementos necesarios para ayudar a proteger y velar por el normal funcionamiento y correcto estado de los controles físicos implantados en cada uno de los activos ubicados dentro de las instalaciones físicas de la Corporación. A la vez, evaluar la posibilidad de mejorar los mecanismos de control para proveer de seguridad las instalaciones de la misma.

El ingreso de personal externo a la Corporación, se realizará a través de identificación de Visitante, en donde diga el área a donde se desplaza. Se debe llevar un registro del control de accesos de todo el personal a la Corporación y la oficina de recursos físicos se encargará de la custodia de dichos registros.

El acceso a los centros de cableado de datos, voz y cableado eléctrico, se deberá realizar previa autorización y conocimiento del área de recursos físicos y la oficina de sistemas en los casos que sea necesario, con el fin de disminuir intercepciones o daños. No se debe dejar líquidos inflamables cerca de los centros de cableado.

Los funcionarios vinculados a la Corporación (planta y contratista) deben portar el carné que lo identifica como funcionario de la misma; lo deben usar durante la su permanencia en sus instalaciones. En caso de pérdida deben reportarlo de forma inmediata a la oficina de Talento Humano.

Los funcionarios de la Corporación y personal previsto por empresas o terceras partes vinculadas a la misma, no deben intentar ingresar a sectores o áreas que no están autorizados. Deben estar autorizados para ingresar a oficinas diferentes a las asignadas en su objeto laboral.

1.11.2 Equipos

La Corporación a través de la oficina de sistemas, debe garantizar la seguridad necesaria de todos los equipos de cómputo con el fin de evitar robos, fallos o daños en los mismos. Se deben generar estrategias que protejan la confidencialidad, integridad y disponibilidad de los recursos tecnológicos dentro y fuera de la corporación.

Se debe prever dentro del plan de acción anual de la oficina de sistemas, la actividad de programación de mantenimiento preventivo y correctivo de equipos de cómputo y demás equipos de la plataforma tecnológica y realizar su ejecución.

La oficina de sistemas debe emprender e implementar mecanismos de estandarización de seguridad para equipos de cómputo corporativos y configurarlos de acuerdo a los estándares y mecanismos generados.

La oficina de sistemas debe definir las condiciones básicas que deben cumplir los equipos de cómputo de personal contratista que necesiten conectarse a la red de datos, verificando su cumplimiento de dichas condiciones antes de dar acceso a los servicios de red.

Se deben brindar mecanismos de autenticación fuerte. La generación y utilización de contraseñas seguras.

Se debe definir un procedimiento de altas y de bajas para la disposición final de equipos de cómputo de la corporación. La Subdirección Administrativa y Financiera deberá gestionar los mecanismos necesarios para lograr que los equipos de cómputo e implementos de tecnología (hardware y software) que se encuentren obsoletos y en estado inservible, sean dados de baja.

La oficina de control interno debe incluir dentro del plan anual de auditorías la verificación de equipos de cómputo de forma aleatoria en las diferentes subdirecciones y centros de atención de la Corporación.

La oficina de recursos físicos debe garantizar la restricción de acceso físico a los diferentes equipos de cómputo y a las áreas donde se procesa la información sensible de trámites ambientales y proceso sancionatorio.

La oficina de Recursos Físicos debe generar mecanismos y controles de seguridad que protejan los activos al ingreso y a la salida de la Corporación. Para esto, se debe contar con documento donde se autorice la entrada o salida de activos, por el profesional Universitario de Planta de Recursos Físicos.

Los equipos como servidores, panta eléctrica, red de datos, red de corriente regulada, UPS de 20 y 30 Kw, deben tener pólizas de seguro todo riesgo. El área de Recursos físicos deberá garantizar las pólizas todo riesgo de los equipos en mención.

Los funcionarios de la oficina de sistemas, sección soporte y mantenimiento, son los únicos autorizados para realizar movimientos y asignación de recursos tecnológicos. Está prohibida la disposición de elementos tecnológicos que pueda realizar cualquier funcionario de la Corporación, diferente a los ya mencionados.

Cuando se presente algún daño relacionado con su equipo de cómputo, o cualquier recurso tecnológico a su cargo, el usuario responsable deberá informar y solicitar su verificación al email: soporte@corporinoquia.gov.co. El usuario no debe intentar solucionar el problema. La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Corporación, solo puede ser realizado por los funcionarios de la Oficina de Sistemas o personal autorizado por la misma.

Los usuarios de los equipos de cómputo deben bloquearlos al momento de abandonar su puesto de trabajo.

Los usuarios de los equipos de cómputo de la corporación (planta y contratista), deben apagarlos en horas no laborales.

En caso de pérdida o robo de un equipo de cómputo corporativo, se debe informar de inmediato al jefe o líder del proceso para que se inicie el trámite interno. Se debe instaurar denuncia ante la autoridad competente más cercana.

Al terminar la jornada laboral, los funcionarios (planta y contratista) deben asegurarse de dejar sus sitios de trabajo en perfecto orden. No deben dejar documentación física expuesta. Toda la documentación corporativa se le debe garantizar su confidencialidad.

Se debe colocar el protector de pantalla autorizado en todos los equipos de cómputo, relacionados con el Sistema de Gestión de Calidad y el escritorio del computador debe permanecer limpio de archivos u otros iconos.

1.12 POLÍTICAS DE SEGURIDAD DE LAS OPERACIONES

1.12.1 Procedimientos, Operaciones y Responsabilidades

La oficina de sistemas como responsable del proceso TIC, en la Corporación, deberá asignar a cada uno de sus funcionarios (planta y contratista) funciones y responsabilidades definidas. Estos deben generar estrategias para el soporte, operación y administración de los recursos tecnológicos, garantizando la mejora continua de los procesos operativos para el desarrollo de las actividades.

La oficina de sistemas deberá apoyar la formulación del Plan de Acción de la Corporación en lo relacionado con las proyecciones de crecimiento en la plataforma tecnológica y gestión de la misma.

La oficina de sistemas debe elaborar los manuales de configuración y operación de los diferentes servicios tecnológicos como es: servicios de red, sistemas de información, base de datos, sistemas operativos, como medio de continuidad y estandarización en el desarrollo de las actividades en la oficina.

La oficina de sistemas debe proveer a los funcionarios de la misma los espacios necesarios para la ejecución de actividades y sus respectivos controles de prestación de servicios de calidad, hacer seguimiento y gestión para el cumplimiento de los mismos.

1.12.2 Protección contra códigos maliciosos

Se debe asegurar que los equipos de cómputo instalados en la Corporación, cuenten con software antivirus, antimalware, y anti spam licenciados y actualizados, que reduzcan el riesgo de software malicioso y respalden la seguridad de la información resguardada en la plataforma tecnológica. El personal contratista debe garantizar que sus equipos de cómputo cuenten con licencia de antivirus y licencia de sistema operativo.

Se debe configurar el software antivirus de tal forma que no pueda ser modificada por los usuarios. Adicionalmente, la configuración debe permitir las actualizaciones automáticas y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Los usuarios deben asegurarse que los archivos recibidos por correo electrónico proceden de fuentes seguras y conocidas para evitar ataque de virus o instalación de software malicioso en los equipos. En caso de sospecha de archivos desconocidos se debe llamar a la oficina de sistemas para brindar la asesoría y acompañamiento.

Los archivos que son recibidos de dudosa procedencia y/o que son abiertos o ejecutados por primera vez, deben ser analizados con el antivirus. Los medios extraíbles deben ser evaluados por el antivirus antes de abrir, al igual que los archivos que provienen de correo electrónico.

1.12.3 Copias de Respaldo

El comité de seguridad de la información debe definir un procedimiento para la realización de copias de seguridad de la información sensible e importante relacionada con los procesos misionales y de apoyo, y debe hacer seguimiento y control a las copias de seguridad de la información, verificando su realización y funcionalidad y debe gestionar la infraestructura tecnológica necesaria para que se lleven a cabo dentro y fuera de la Corporación.

La Oficina de sistemas deberá generar y adoptar el procedimiento para la generación, restauración, almacenamiento y tratamiento de copias de respaldo de la información, promoviendo su integridad y disponibilidad.

La oficina de sistema debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, comprobando su integridad y funcionalidad, para uso en caso de ser necesario.

Los propietarios de los recursos tecnológicos y sistemas de información en conjunto con la oficina de sistemas, deben definir las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Es responsabilidad de todos los usuarios de la plataforma tecnológica, ayudar a identificar la información sensible e importante que deba ser respaldada mediante copias de seguridad.

La Secretaria General a través de la responsable del Centro de Documentos y Bodega de Archivo, deberán realizar el levantamiento de requerimientos de información a transferir por cada una de las áreas al Centro de Documentos y deben especificar de qué manera y en qué tipo de medio se debe transferir (física o digital), que documentos se deben transferir y en qué tiempos. Para lo cual se debe realizar un procedimiento que describa tales actividades de forma puntual.

1.12.4 Registro y seguimiento

Corporinoquia realizará monitoreo constante al uso que dan los funcionarios y el personal contratado a los activos tecnológicos de la plataforma y sistemas de información. Así como la custodia de registros de acceso y auditoria del sistema a través de los registros de eventos.

El Comité de Seguridad de la información deberá determinar elementos y recursos tecnológicos importantes a los cuales se les debe generar log de auditoria, como medio de registro y verificación al suceso de eventos.

Se debe definir un procedimiento de revisión de logs, donde se indique la forma como se deben abordar dichas revisiones y, además, los registros de eventos a revisar y a que activo o proceso corresponden, y quienes serán los encargados de realizarlos.

Para el desarrollo de software, el equipo desarrollador debe tener en cuenta los logs de auditoria de los sistemas de información, teniendo en cuenta intentos de autenticación fallidos y exitosos, intento de evasión de controles, fallas en los controles de acceso, fallas de validación, excepciones en los sistemas, funciones administrativas y cambios de configuración de seguridad, de acuerdo a los requerimientos de funcionalidad y seguridad, presentados en los estudios previos de los procesos de contratación de desarrollo de software. Este documento debe estar aprobado por el Comité de Seguridad de la información de la Corporación.

1.12.5 Control de software Operacional

La oficina de sistemas deberá establecer procedimientos y asignar responsabilidades para brindar soporte en la instalación de software operativo (misional y de apoyo), en los equipos de cómputo. Todo software instalado en los equipos corporativos debe ser licenciado y debe

contar con soporte de proveedores. Así mismo se deben establecer de usuario, para la instalación de software operativo en los equipos de cómputo de la Corporación.

El Comité de Seguridad de la Información, en conjunto con la oficina de sistemas debe tener en cuenta los riesgos a asumir ante la migración a nuevas versiones de software. Debe verificar el normal funcionamiento de sistemas de información sobre la plataforma tecnológica cuando este es actualizado.

1.12.6 Gestión de la Vulnerabilidad Técnica

La oficina de sistemas de Corporinoquia realizara revisiones periódicas de la aparición de vulnerabilidades técnicas sobre los sistemas de información y los demás recursos de la plataforma tecnológica, con el objeto de realizar correcciones sobre a hallazgos encontrados en las pruebas. Esta revisión se realizará por el personal encargado de la oficina de sistemas y será presentado al Comité de la Seguridad de la información quienes revisaran, valoraran y gestionaran las vulnerabilidades técnicas encontradas.

Se debe gestionar los trámites correspondientes y los recursos necesarios ante la Subdirección Administrativa y Financiera, para la realización de pruebas de vulnerabilidades y hacking ético por un ente externo contratado con el fin de encontrar las posibles vulnerabilidades a ataques y definir un plan de seguridad para las vulnerabilidades encontradas.

La oficina de sistemas de la corporación, debe generar y ejecutar planes de acción que mitiguen las vulnerabilidades detectadas en la plataforma tecnológica.

1.13 POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

1.13.1 Gestión de la seguridad de las redes

La oficina de sistemas establecerá el procedimiento de autorización y controles para proteger el acceso a la red de datos y los demás activos tecnológicos de la red de la Corporación.

La red inalámbrica de la Corporación, deben contar con métodos de autenticación que eviten accesos no autorizados.

La oficina de sistemas de la Corporación debe estructurar la información a almacenar en el servidor donde se identifique claramente las áreas y temáticas a las que pertenece, y estructurar los roles y permisos que van a tener cada uno de los usuarios a la misma.

La oficina de sistemas debe instalar protección entre la red interna de Corporinoquia y la red externa (internet). Debe velar por mantener la confidencialidad de la información en el direccionamiento y enrutamiento de las redes de datos de la Corporación. Deberá gestionar ante la Subdirección Administrativa y Financiera los recursos necesarios para implementar y gestionar firewall de seguridad actualizados y robustos.

Los Subdirectores, Directora General y Jefes de área deben autorizar los privilegios de acceso a los recursos de la red de datos de la Corporación, para lo cual, deben informar los datos básicos del usuario, tipo de vinculación, función a realizar, información autorizada y tipo de rol a desempeñar con la información (creación, modificación o consulta) y área a la que pertenece, así como los diferentes accesos a sistemas de información y elementos tecnológicos de la red de datos. Dicha solicitud la debe presentar al email: soporte@corporinoquia.gov.co.

Los usuarios que deseen el servicio de conexión de equipos de cómputo a la red de datos, deberán cumplir todos los requisitos para autenticarse y únicamente deberán realizar tareas para las que fueron autorizados. Es responsabilidad del usuario y jefe de área informar al área de sistemas cualquier anomalía o cambio en su equipo de trabajo de accesos no autorizados.

1.13.2 Transferencia de Información

La Corporación asegurará los controles y procedimientos para el intercambio de información y brindará la protección de la información al momento de ser transferida a otras organizaciones.

Desde la oficina jurídica al momento de realizar el proceso de contratación con terceros se debe dejar en el contenido de los contratos las cláusulas necesarias para pactar la confidencialidad y protección de la información Corporativa.

La Corporación deberá asegurar que los propietarios o administradores de activos de información brinden protección a la información, evitando su divulgación a terceros y

brindando total confidencialidad a la misma, sobre todo en los casos de expedientes ambientales, preliminares y proceso sancionatorio, así como diferentes tipos documentales, como conceptos técnicos, resoluciones, Autos e informes Ambientales.

Se debe dejar registro de todas las transacciones de información en cada una de las dependencias de la Corporación, y estas deben estar autorizadas por el Subdirector de cada Área o Jefes Inmediatos, teniendo en cuenta la política de seguridad de la información Corporativa.

Los funcionarios responsables de activos de información realizaran intercambio de información digital, siempre y cuando esté autorizado por el jefe de área, acatando la Política de seguridad de administración de red, acceso lógico y protección de datos de tipo personal de la Corporación, teniendo en cuenta el procedimiento de intercambio de información entre la Corporación y terceros.

El área de Secretaria General, como responsable de la implementación de directrices de Gestión Documental en la Corporación deberá elaborar e implementar el procedimiento de intercambio de información (documentos y medios de almacenamiento) con terceros y la adopción de controles para la protección de la información de acuerdo a su importancia y grado de confidencialidad a tener en cuenta.

La información a entregar a terceros debe quedar registrada a través de documento donde se autoriza y se envía (Comunicación Oficial), y debe ser entregada únicamente por los mecanismos de envío autorizado por la Secretaria General de Corporinoquia.

La oficina de Sistemas debe ofrecer herramientas tecnológicas de intercambio seguro de información digital o en medio magnética, que permitan el cumplimiento de las Políticas de Seguridad de la información de la Corporación,

La Corporación y las áreas responsables que den contestación a solicitudes de información, deberán evaluar la pertinencia y los cuidados en la entrega de información confidencial a terceros, estos deberán velar por proteger dicha información y evitar divulgaciones no autorizadas.

Se debe habilitar un correo electrónico corporativo de uso exclusivo para envíos externos y recibidos externos de la Corporación (**atencionusuarios@corporinoquia.gov.co**). El Correo

electrónico asignado a cada uno de los funcionarios será para realizar envíos internos de comunicación y trabajo interno colaborativo. Ningún funcionario está autorizado para realizar envíos o contestaciones a título de la Corporación, a través de sus correos corporativos internos.

No está permitido brindar información Corporativa sensible vía telefónica o conferencias remotas.

La Dirección General de la Corporación a través de la oficina de Prensa será la única autorizada para realizar comunicados de prensa y de información importante de la gestión ambiental, bien sea por los medios de comunicación como radio, televisión, pagina web, redes sociales entre otros.

1.14 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

1.14.1 Requisitos de Seguridad de los sistemas de información

La Corporación debe asegurar que el software adquirido o desarrollado (internamente y por terceros), debe cumplir con el 100% de requisitos de seguridad y calidad establecidos en los términos de referencia y documento técnico de requisitos elaborado por la Corporación. Las áreas relacionadas con el software a adquirir o desarrollar deberán aportar los requisitos correspondientes y deberán ayudar a verificar su cumplimiento, durante las pruebas de funcionamiento.

Cada software a desarrollar deberá tener un área específica asignada de quienes serán los encargados de gestionarla dentro de la organización. La administración de los sistemas de información, la realizaran los funcionarios de la oficina de sistemas.

Para la definición de requisitos de seguridad de los sistemas de información a desarrollar, cada una de las áreas involucradas en el proceso deberán brindar la información necesaria hasta lograr definir claramente los requerimientos a desarrollar.

Todas las aplicaciones de software adquiridas o desarrolladas deben estar documentadas para su mejor adaptabilidad y entendimiento (manual de usuario-administración). Se debe exigir a los desarrolladores este requisito.

Los desarrolladores de software de la Corporación, deben implementar controles para la duración de sesiones activas del aplicativo software, con el fin de evitar suplantaciones de sesión, por usuarios descuidados con las sesiones al dejar equipos sin seguridad.

Para autorizar la creación de usuarios y contraseñas es necesario tener en cuenta la política de seguridad de control de accesos.

La Corporación asegurará a través de las áreas involucradas en cada desarrollo de software, bien sea interno o a través de un tercero, que se cumpla con los requerimientos de seguridad del ciclo de vida de desarrollo de software seguro, de acuerdo a la metodología de desarrollo de software seleccionada. La Corporación debe asegurar que el software a adquirir debe contar con soporte técnico durante el funcionamiento del mismo.

Antes de poner en funcionamiento el software desarrollado o adquirido en la Corporación, los responsables del área de uso del mismo, deben verificar su funcionamiento y certificar el cumplimiento de los requerimientos de calidad y seguridad, para esto, el área correspondiente debe documentar la revisión. Se debe hacer cada vez que se haga entrega de funcionalidades del sistema. La oficina de sistemas de la Corporación, debe brindar el acompañamiento necesario en estas pruebas.

En caso de requerir migraciones de información de un sistema a otro, esta debe ser autorizada por el área propietaria de la misma. La oficina de sistemas y el personal en cargado de realizar las migraciones debe garantizar los controles necesarios para asegurar que la migración de información entre ambientes de desarrollo, pruebas y producción este autorizado por el área pertinente, así como gestionar la seguridad de la información a migrar.

Durante las etapas de desarrollo, la oficina de sistemas se encargará de contar con un repositorio de control de versiones del software que está en proceso de desarrollo o desarrollado. Para esto, el desarrollador o tercero deberá hacer entrega de la versión presentada del software, a la oficina de sistemas de la Corporación.

Los contratos con objeto de desarrollo o adquisición de software deben evidenciar el tipo de licenciamiento, los derechos de autor y el tipo de uso del software que va a tener la corporación. Esto se debe plasmar en los estudios previos del proceso contractual, que lo elaborara la oficina de sistemas de Corporinoquia.

Se debe definir un procedimiento donde se indique la realización de pruebas al software desarrollado, los requisitos mínimos que debe cumplir. Se debe tener en cuenta el documento técnico de requisitos elaborado para cada caso de desarrollo de software.

La oficina de sistemas deberá encargarse de la validación de funcionalidad del sistema en cuanto a: validación de entrada de datos y generación de los datos de forma confiable. Los campos de los formularios del sistema de información desarrollado deberán facilitar la validación de la información, teniendo en cuenta: tipo de dato del campo, longitud, rangos válidos, lista de caracteres aceptados, caracteres peligrosos, entre otros.

Los sistemas de información desarrollados deben cumplir con los requerimientos del manual 3.1 de Gobierno en Línea de Colombia, en cuanto a seguridad, accesibilidad y navegabilidad. Los formularios deben brindar una guía de ruta de navegación, así como la opción de cierre de sesión de los aplicativos en cada uno de sus secciones.

1.15 POLÍTICAS DE SEGURIDAD EN LAS RELACIONES CON LOS PROVEEDORES

1.15.1 Seguridad de la Información en relación con los proveedores

La Corporación debe velar por que las empresas contratistas o terceros que tengan relación con la misma, cumplan a cabalidad los requerimientos, normatividad, procesos y procedimientos de seguridad de la información. El área jurídica encargada de la responsabilidad de firma y suscripción de contratos y convenios con terceros, apoyara la socialización del compromiso de cumplimiento de la normatividad, políticas y procedimientos de seguridad de la información al interior de la corporación.

Se debe generar compromisos de responsabilidad, de confidencialidad y seguridad de la información con terceros en cada uno de los contratos o convenios a suscribir con proveedores y prestadores de servicios.

La oficina de sistemas debe establecer las condiciones necesarias de seguridad para las conexiones de equipos de cómputo y dispositivos móviles de personal contratista a la red de datos Corporativa.

Los supervisores e interventores de contratos o convenios, deberán socializar las políticas y procedimientos de seguridad de la información de la Corporación, a cada uno de los intervinientes en los mismos, deben promover el acceso seguro a la información y a los recursos de almacenamiento, aplicando la política de seguridad de la información en la Corporación.

1.16 POLÍTICAS DE SEGURIDAD EN GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1.16.1 Gestión de Incidentes y mejoras en la Seguridad de la Información

Se debe definir el procedimiento de reportes de incidentes relacionado con la seguridad de los activos de información, sus medios de procesamiento, y toda la plataforma tecnológica, incluyendo sistemas de información y las personas. En este procedimiento se deben definir los responsables que intervendrán en el tratamiento de los incidentes.

Los propietarios de los activos de información deben informar a la oficina de control Interno y jefe inmediato del área correspondiente donde se haya identificado o presentado el incidente de seguridad identificado o que se reconozcan la probabilidad de materialización.

La oficina de sistemas deberá reportar al comité de Seguridad de la Información todos los incidentes relacionados con la seguridad de la información para su evaluación y tratamiento, con el fin de mitigar los daños a la información y generar los controles necesarios para su salvaguarda.

Se debe documentar los sucesos relacionados con daños y posibles ataques contra la seguridad de la información y los mecanismos utilizados como medio de protección para cada uno de los eventos registrados.

Los funcionarios de la Corporación, personal contratista y personal previsto por terceras partes (empresas), deberán reportar eventos o incidentes relacionados con los recursos tecnológicos y la seguridad de la información, en la Corporación. La oficina de control interno o la Subdirección Correspondiente son las encargadas de recibir los reportes de eventos mencionados en el presente ítem.

1.17 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

1.17.1 Continuidad de la Seguridad de la información

La Corporación garantizará todos los recursos suficientes para proporcionar una respuesta efectiva y dar continuidad a procesos y servicios, en caso de contingencia o catástrofes que se presenten en las instalaciones de Corporinoquia y que afecten la continuidad del negocio. Se debe garantizar la seguridad de la información y el restablecimiento de la misma como apoyo a los procesos misionales de la Corporación.

El Comité de Riesgos y el Comité de Atención y Prevención de emergencias de la Corporación, deben estar alineados para apoyar y salvaguardar la información en caso de contingencias o eventos catastróficos. El Comité de Riesgos y atención de Emergencias en conjunto con la oficina de Sistemas y la Secretaria General de la Corporación, deberán valorar y analizar los impactos causados para el inicio de la recuperación ante desastres y continuidad de las labores misionales y de apoyo de la Corporación.

La oficina de sistemas debe realizar un plan de contingencia y de recuperación ante desastres, para volverá la normalidad la infraestructura tecnológica (red de datos, sistemas de información, centro de cómputo) y cada uno de los sistemas mencionados. Cualquier anormalidad detectada en la recuperación del sistema debe ser informada al comité de Seguridad de la Información y a la Dirección General de la Corporación.

1.17.2 Redundancias

La oficina de sistemas en conjunto con el Comité de Seguridad de la Información deberá analizar y establecer requerimientos de redundancia de los diferentes sistemas tecnológicos críticos para la Corporación, especialmente para los sistemas de información de Gestión Documental y Sistema de Información Financiera. Además, será la encargada de implementar y administrar las soluciones de redundancia tecnológica, garantizando su funcionalidad a través de pruebas periódicas, para asegurar el cumplimiento de requisitos y requerimientos de disponibilidad del servicio en la Corporación.

1.18 POLÍTICAS DE SEGURIDAD PARA EL CUMPLIMIENTO

1.18.1 Cumplimiento de requisitos legales y contractuales

Corporinoquia como entidad Gubernamental, velará por el cumplimiento de la normatividad relacionada con la seguridad de la información, entre ellas, Manual 3.1 de Gobierno en Línea, derechos de autor (Software), por lo cual, forjará sus esfuerzos a cumplir que el software instalado en la plataforma y recursos tecnológicos cumpla con los requerimientos legales y de licenciamiento. A la vez, gestionar el cumplimiento de las normas establecidas por el Ministerio de las Tic, en cuanto a seguridad y protección de la información de las entidades gubernamentales de Colombia.

La oficina de sistemas debe presentar informes periódicos acerca de la legalidad del software instalado en los equipos de cómputo y centros de datos de la corporación. Dichos informes se deben presentar a la oficina de Control Interno de la Corporación.

La oficina de sistemas debe llevar un registro de inventario de software instalado en los equipos de cómputo y los centros de datos en donde especifique la licencia de funcionamiento a nombre de la Corporación. Se debe verificar periódicamente el software instalado en los diferentes equipos, que corresponda al permitido en cada estación y centro de datos autorizado.

Los usuarios de los equipos de cómputo corporativo, deben abstenerse de instalar software o aplicativos en sus equipos de cómputo asignados para el desarrollo de sus actividades. La oficina de sistemas es la encargada de este proceso.

El comité de seguridad de la información de la corporación, propenderá por el cumplimiento de la Ley 1582 de 2012, por medio de la cual se regula la protección de datos personales en Colombia.

Las áreas que procesan datos personales de usuarios internos y externos de la Corporación u otros, deberán cumplir con la política de seguridad de la información, cumplir la normatividad colombiana de seguridad de información e implementar controles necesarios para asegurar el tratamiento de la información sensible de los mismos, garantizando la confidencialidad, integridad y disponibilidad de la información.

La oficina de sistemas de la corporación debe implantar los controles necesarios para proteger la información personal interno y externo e información sensible almacenada en base de datos o cualquier otro repositorio, evitando su divulgación (confidencialidad), alteración (integridad) o eliminación (disponibilidad) sin la autorización respectiva.

Los usuarios de la información corporativa, deberán guardar total discreción y reserva con el uso de la misma; esta debe ser usada para el apoyo a la gestión y desarrollo de procesos misionales corporativos. Es necesario identificar la identidad de las personas o terceros a quienes se les entrega información. Esta entrega debe estar autorizada por un integrante de la alta dirección en cada una de las dependencias de la Corporación.

Los usuarios de los sistemas de información de la Corporación, deberán empoderase de la responsabilidad propia sobre las claves de acceso y autorización asignadas, para lo cual, deben cambiarla periódicamente para evitar ataques de ingeniería Social. Sus equipos de cómputo deben estar bloqueados en los momentos de inactividad o pausas activas, como mecanismo de seguridad y control.

2 REFERENCIAS BIBLIOGRAFICAS

ALCALDIA DE BOGOTA. (16 de 06 de 2015). *ALCALDIA DE BOGOTA*. Obtenido de ALCALDIA DE BOGOTA: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=38498

ARCHIVO GENERAL DE LA NACION. (10 de 06 de 2015). *ARCHIVO GENERAL DE LA NACION*. Obtenido de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_594_DE_2000.pdf

ARCHIVO GENERAL DE LA NACION_AGN. (10 de 06 de 2015). *ARCHIVO GENERAL DE LA NACION*. Obtenido de http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/ACUERDO_05_DE_2013.pdf

ARCHIVO GENERAL DE LA NACIÒN-L527. (14 de 06 de 2015). *ARCHIVO GENERAL DE LA NACIÒN-L527*. Obtenido de ARCHIVO GENERAL DE LA NACIÒN-L527: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

AUDITORIADESISTEMASADRIMELI. (15 de 06 de 2015). *AUDITORIADESISTEMASADRIMELI*. Obtenido de AUDITORIADESISTEMASADRIMELI: http://auditoriadesistemasadrimeli.blogspot.mx/

BIBLIOTECA DIGITAL ICESI. (10 de 06 de 2015). *BIBLIOTECA DIGITAL ICESI*. Obtenido de BIBLIOTECA DIGITAL ICESI: http://bibliotecadigital.icesi.edu.co/biblioteca_digital/

CMMIINSTITUTE. (13 de 06 de 2015). *CMMIINSTITUTE*. Obtenido de CMMIINSTITUTE: http://cmmiinstitute.com/get-started

CONTRATOS.GOV.CO. (16 de 06 de 2015). *CONTRATOS.GOV.CO*. Obtenido de CONTRATOS.GOV.CO: https://www.contratos.gov.co/consultas/detalleProceso.do?numConstancia=14-9-391615

CORPORINOQUIA. (25 de 05 de 2015). *CORPORINOQUIA*. Obtenido de http://l.corporinoquia.gov.co/index.php/inicio/corporinoquia

DAMETAREAS. (10 de 06 de 2015). *DAMETAREAS*. Obtenido de DAMETAREAS: www.dametareas.com

DNP. (20 de 06 de 2015). *DNP*. Obtenido de www.dnp.gov.co

ELKIN COELLO_ BLOG. (05 de 06 de 2015). *ELKIN COELLO_ BLOG*. Obtenido de helkyncoello.wordpress.com

GOBIERNO EN LINEA. (16 de 06 de 2015). *GOBIERNO EN LINEA*. Obtenido de GOBIERNO EN LINEA: http://programa.gobiernoenlinea.gov.co/apc-aa-files/eb0df10529195223c011ca6762bfe39e/manual-3.1.pdf

ISO 27000.es. (25 de 05 de 2015). *ISO 27000*. Obtenido de http://www.iso27000.es/iso27000.html

ISO27002. (14 de 06 de 2015). *ISO27002*. Obtenido de ISO27002: http://www.iso27002.es/

ISO9000CONSULTORES. (15 de 06 de 2015). *ISO9000CONSULTORES*. Obtenido de iso9000consultores.blogspot.com

MINTIC. (15 de 06 de 2015). *MINTIC*. Obtenido de MINTIC: http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html

MINTIC_CONPES. (14 de 06 de 2015). *MINTIC_CONPES*. Obtenido de MINTIC_CONPES: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

MINTIC-L1273. (15 de 06 de 2015). *MINTIC-L1273*. Obtenido de MINTIC-L1273: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MINTIC-L1341. (15 de 06 de 2015). *MINTIC-L1341*. Obtenido de MINTIC-L1341: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf

MONOGRAFIAS_COBIT. (13 de 06 de 2015). *MONOGRAFIAS*. Obtenido de MONOGRAFIAS: http://www.monografias.com/trabajos93/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas.shtml#ixzz3lNXG5xTZ

PMG-SSI_27003. (14 de 06 de 2015). *PMG-SSI_27003*. Obtenido de PMG-SSI_27003: http://www.pmg-ssi.com/2014/01/isoiec-27003-guia-para-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion

PMG-SSI-ISO_27004. (14 de 06 de 2015). *PMG-SSI-ISO_27004*. Obtenido de PMG-SSI-ISO_27004: http://www.pmg-ssi.com/2014/01/isoiec-27004-medicion-de-la-seguridad-de-la-informacion/

PMG-SSI-ISO_27005. (14 de 06 de 2015). *PMG-SSI-ISO_27005*. Obtenido de PMG-SSI-ISO_27005: http://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/

SECRETARIA SENADO. (15 de 06 de 2015). *SECRETARIA SENADO*. Obtenido de SECRETARIA SENADO: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

SECRETARIA SENADO-L1150. (15 de 06 de 2015). *SECRETARIA SENADO-L1150*. Obtenido de SECRETARIA SENADO-L1150: http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html

SECRETARIA SENADO-L594. (15 de 06 de 2015). *SECRETARIA SENADO-L594*. Obtenido de SECRETARIA SENADO-L594: http://www.secretariasenado.gov.co/senado/basedoc/ley_1150_2007.html

SECRETARIA SENADO-L962. (15 de 06 de 2015). *SECRETARIA SENADO-L962*. Obtenido de SECRETARIA SENADO-L962: http://www.secretariasenado.gov.co/senado/basedoc/ley_0962_2005.html

SEGURIDADINFORMACIONCOLOMBIA. (13 de 06 de 2015). *SEGURIDADINFORMACIONCOLOMBIA*. Obtenido de http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html

SLIDESHARE. (12 de 06 de 2015). *SLIDESHARE*. Obtenido de http://es.slideshare.net/vaceituno/analisis-de-riesgos-con-oism3-ra

TARINGA. (16 de 06 de 2015). *TARINGA*. Obtenido de TARINGA: www.taringa.net

TECNOVA-CMMI. (13 de 06 de 2015). *TECNOVA*. Obtenido de TECNOVA: http://www2.tecnova.cl/servicios/descripcion_cmmi.html

WIKIPEDIA. (25 de 05 de 2015). *WIKIPEDIA*. Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27000-series

WIKIPEDIA. (10 de 06 de 2015). *WIKIPEDIA_27001*. Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27001

WIKIPEDIA. (25 de 06 de 2015). *WIKIPEDIA_SEG INF*. Obtenido de https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

WIKIPEDIA_COBIT. (13 de 06 de 2015). *WIKIPEDIA_COBIT*. Obtenido de WIKIPEDIA_COBIT: https://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas

WIKIPEDIA_ISC2. (11 de 06 de 2015). Obtenido de https://es.wikipedia.org/wiki/ISC2