Anexo No. 1
COPIAS DE SEGURIDAD DIGITAL IST-08

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ALCANCE DE LAS POLÍTICAS

Las políticas definidas en el presente documento aplican para todos los funcionarios públicos, contratistas y pasantes de la Corporación Autónoma Regional de la Boyacá y demás usuarios que utilicen la plataforma tecnológica y los servicios tecnológicos de CORPOBOYACÁ.

DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

CORPOBOYACA: Corporación Autónoma Regional de Boyacá.

Políticas: son instrucciones mandatarias que indican la intención de la Alta Dirección respecto a la operación de la organización.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiera la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

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

Ataque Cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

COPIA NO CONTROLADA

Brecha de seguridad: Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en si misma, sea o no protegida por reserva legal.

Criptografía de llave publica: Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Cifrar: Quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama "decodificar" o "descifrar". Los sistemas de ciframiento se llaman "sistemas criptográficos".

Certificado Digital: Un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor

No repudio: Este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

DESCRIPCIÓN DE LAS POLÍTICAS

POLÍTICA 1: ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas y pasantes que laboran para CORPOBOYACA deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a CORPOBOYACA, la Dirección General y Subdirectores, deben autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

COPIA NO CONTROLADA

Anexo No. 1
COPIAS DE SEGURIDAD DIGITAL IST-08

Para que un funcionario público, contratista o pasante tenga acceso a los servicios y recursos tecnológicos dispuestos por CORPOBOYACA, se requiere que el supervisor, jefe inmediato o coordinador solicite al proceso Gestión Soporte Tecnológico, mediante el FST-06 Administración Cuentas de Usuario la activación de dichos servicios con el perfil requerido y las restricciones necesarias.

Cada vez que se recibe un computador de escritorio o portátil para darle acceso a los servicios tecnológicos que brinda la corporación a los usuarios, es necesario, requerido y obligatorio entregar el equipo con todos los servicios instalados, configurados y en operación. Esto es, verificación y última actualización de parches de seguridad del sistema operativo, instalación del último Service-pack del sistema operativo, instalación, y configuración del antivirus utilizado por la entidad, actualización al último programa y versión de la base de datos de vacunas del antivirus, instalación y configuración del mensajero interno, configuración del servicio de red inalámbrica e inclusión en el directorio activo del Servidor, verificación e instalación de la herramienta para comprimir, verificación e instalación de la herramienta para gestionar archivos pdf, verificación e instalación de la herramienta para quemar Cd y DVD, actividades que están bajo la responsabilidad del porceso Gestión Soporte Tecnológico.

Todos los privilegios para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad.

Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

COPIA NO CONTROLADA

POLITICA 2: SEGURIDAD DE LA INFORMACION

Los funcionarios públicos, contratistas, y pasantes de CORPOBOYACA son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Corporación, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios públicos, contratistas, y pasantes no deben suministrar información de la Corporación a través de medios electrónicos a ningún ente externo sin la previa autorización del subdirector o jefe de dependencia, si algún funcionario público, contratista ó pasante lo hiciera, ésta información será suministrada como opinión a título personal y en ningún momento será la posición de la entidad.

Todo funcionario público, contratista ó pasante que utilice la plataforma tecnológica y los servicios tecnológicos disponibles, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Los funcionarios, contratistas y pasantes deben solicitar el visto bueno de un funcionario del proceso Gestión Soporte Tecnológico para liquidar el contrato de vinculación o terminar su vinculación laboral en el caso de los funcionarios de planta, este procedimiento le permite a CORPOBOYACA velar por la seguridad de la información, la confidencialidad y el buen manejo de la información.

Después de que un funcionario, contratista o pasante deja de prestar sus servicios a CORPOBOYACA, éste se compromete a entregar toda la información respectiva de su trabajo realizado al supervisor, Coordinador o jefe inmediato según sea el caso, y avala el recibido de la información el paz y salvo del funcionario retirado. Una vez retirado el funcionario, contratista y pasante debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información está en la obligación de reportar el hecho al grupo de control interno disciplinario.

COPIA NO CONTROLADA

POLITICA 3: SEGURIDAD PARA LOS SERVICIOS TECNOLÓGICOS

El sistema de correo electrónico corporativo y servicios tecnológicos prestados por CORPOBOYACA deben ser usados únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas y pasantes.

La entidad se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico corporativo para cualquier propósito. Para este efecto, el funcionario o contratista autorizará a la entidad para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

Los funcionarios públicos, contratistas y pasantes no deben utilizar versiones escaneadas de Firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico ó cualquier otro tipo de comunicación electrónica haya sido firmada por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el funcionario, contratista o pasante se encuentre en sitios de trabajo alternos, es propiedad exclusiva de CORPOBOYACA. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, investigaciones pagadas por la Corporación, estudios ambientales y de otros propósitos, programas de computación, códigos fuentes, documentación y otros materiales.

Los funcionarios públicos, contratistas y pasantes que hayan recibido aprobación para tener acceso a Internet a través de las estaciones de trabajo corporativas o computadoras portátiles personales, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet implantadas por la Corporación las cuales prohíben entre otras:

"Toda actividad que sea de carácter lucrativo o comercial en nombre individual, privado o negocio particular. La exhibición de material pornográfico en cualquier lugar de la entidad utilizando el equipo de cómputo y/o los servicios de comunicación de la entidad, asimismo el uso de equipo para observar o reproducir pornografía.

COPIA NO CONTROLADA

La transmisión de materiales que violen cualquier regulación Colombiana como por ejemplo materiales con derechos de propiedad intelectual, materiales que legalmente se consideren amenazantes u obscenos.

Utilizar el correo Electrónico para enviar y/o continuar cadenas de mensajes relacionados con cualquier tema, estas cartas en cadena son totalmente prohibidas.

No se deberá bajar de ningún sitio WEB software no licenciado en la Entidad.

Uso del servicio de manera tal que constituya una molestia, abuso, amenaza o que de cualquier forma atente contra la integridad de los usuarios del servicio de Internet.

Violar la seguridad de los sistemas, sites o host sin previa autorización del dueño.

Cambiar la información de identidad con el objetivo de hacerse pasar por otra persona o entidad. Sin embargo, no está prohibido el uso de alias o remailers anónimos para cualquier propósito legítimo.

Escuchar emisoras ON LINE, (ya que esto aumenta el tráfico, congestiona el ancho de banda y por ende causa lentitud de navegación para los demás usuarios de la red)

No se permitirá el uso del denominado "CHAT" en ningún horario (Página Web, ICQ, Messenger, etc.)

Configurar una página web para actuar de manera maliciosa contra los usuarios que la visiten."

CORPOBOYACA prohíbe el servicio de Internet en la plataforma tecnológica de su propiedad a través de otras empresas Prestadoras de Servicio de Internet haciendo uso de dispositivos inalámbricos diferentes al servicio disponible propio. Con el fin de minimizar el riesgo a la integridad de la información y la seguridad de los sistemas de información Corporativos.

En cualquier momento que un funcionario, contratista o pasante publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la entidad.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente comunicarse con el personal del proceso Gestión Soporte Tecnológico, no utilizar la computadora y desconectarla de la red.

El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de "no repudio".

El proceso Gestión Soporte Tecnológico en conjunto con el proceso Gestión Comunicaciones debe proveer material y charlas para recordar regularmente a los funcionarios, contratistas y pasantes acerca de sus obligaciones con respecto a la seguridad de la plataforma tecnológica y los servicios tecnológicos.

POLITICA 4: SEGURIDAD EN LOS SERVICIOS TECNOLÓGICOS

Todos los Servicios Tecnológicos deben cumplir como mínimo con lo siguiente: Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los servicios tecnológicos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

COPIA NO CONTROLADA

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el de la Administración de usuarios.

Logs de Operaciones: Hace referencia a las pistas o registros de los sucesos relativos a la operación.
El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicas para cada usuario, bien sea controlado y administrado por un Directorio Activo o una herramienta similar que cumpla con esta tarea.

Las palabras claves o contraseñas de acceso a los servicios tecnológicos, que designen los funcionarios públicos, contratistas y pasantes son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su cuenta de de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricas basadas en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de respaldo para garantizar que no sea inapropiadamente modificada, borrada o no recuperable.

COPIA NO CONTROLADA

POLITICA 5: SEGURIDAD PARA USUARIOS TERCEROS

Los dueños de los Recursos Tecnológicos e Informáticos que no sean propiedad de CORPOBOYACA y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente deben recibir y aceptar el documento de políticas de seguridad.

Los usuarios terceros tendrán acceso a los Servicios y Recursos Tecnológicos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el Jefe inmediato, supervisor o coordinador. En todo caso deberán firmar una solicitud de activación y acceso a servicios tecnológicos y aceptaran a dar un buen uso a los recursos y servicios.

Si se requiere un equipo con módem, este equipo no podrá en ningún momento estar conectado a la Red al mismo tiempo.

La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por el Proceso Gestión Soporte Tecnológico con el fin de no comprometer la seguridad de la información interna de la entidad.

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

Como requisito para interconectar la red de CORPOBOYACA con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por CORPOBOYACA. La entidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La entidad se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por CORPOBOYACA.

COPIA NO CONTROLADA

POLÍTICA 6: SOFTWARE UTILIZADO

Todo software que utilice CORPOBOYACA será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad.

Debe existir una cultura tecnológica al interior de CORPOBOYACA que garantice el conocimiento por parte de los funcionarios públicos, contratistas y pasantes de las implicaciones que tiene el instalar software ilegal en las computadoras de CORPOBOYACA.

Existirá un inventario de las licencias de software de CORPOBOYACA que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado. Los funcionarios públicos, que instalen software no licenciado en los equipos de cómputo de la Corporación, se les abrirá un proceso en Control interno Disciplinario. Los contratistas que instalen software no licenciado en los equipos de cómputo de la Corporación, se le puede dar por terminado el contrato y los pasantes que instalen software no licenciado en los equipos de cómputo de la Corporación, se les dará por terminada la pasantía y se oficiará a la institución educativa correspondiente informando la falta.
El software gratuito, puede ser instalado en los equipos de cómputo, informando sobre esto al proceso Gestión Soporte Tecnológico.

POLITICA 7: ACTUALIZACION DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de CORPOBOYACA (cambios de procesador, adición de memoria o tarjetas) debe realizarlo exclusivamente un funcionario del Proceso Gestión Soporte Tecnológico.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por personal autorizado del proceso Gestión Soporte Tecnológico.

Los equipos instalados en la Plataforma Tecnológica (PC, servidores, LAN, Router, Antenas, etc.) no deben moverse o reubicarse sin la aprobación previa del Proceso Gestión Soporte Tecnológico.

POLÍTICA 8: ALMACENAMIENTO Y RESPALDO

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

El almacenamiento de la información deberá realizarse externamente a CORPOBOYACA, esto de acuerdo con la importancia de la información para la operación de CORPOBOYACA.

Los funcionarios, contratistas y pasantes de un área dueña de la información, serán los responsables de respaldar la información producida por el área, siguiendo el procedimiento definido Por el proceso Gestión soporte Tecnológico para salvaguardar la información de usuarios.

Los funcionarios públicos son responsables de los respaldos de su información en las computadoras, siguiendo las indicaciones técnicas dictadas por el proceso Gestión soporte Tecnológico. Este proceso será el autorizado para realizar el seguimiento y control de esta política.

POLÍTICA 9: CONTINGENCIA

El proceso Gestión Soporte Tecnológico, debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

POLÍTICA 10: SEGURIDAD FÍSICA

El Centro de cómputo, el área de sistemas, el Sistema de Información Geográfico Ambiental Territorial y las áreas que la entidad considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

COPIA NO CONTROLADA

Toda persona que se encuentre dentro de la entidad deberá portar su identificación en lugar visible.

En el Centro de cómputo, el área de sistemas, el Sistema de Información Geográfico Ambiental Territorial y las áreas que la entidad considere criticas deberán existir elementos de control de incendio, inundación y alarmas.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todas las computadoras portátiles, módems y equipos de comunicación deben registrar su ingreso y salida y no deben abandonar la entidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión del proceso Gestión de Recursos Financieros y Físicos de CORPOBOYACA.

Los equipos tecnológicos (PCs, servidores equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.

Los funcionarios públicos se comprometen a NO utilizar a la red regulada de energía (tomas naranjas de canaleta) para conectar equipos eléctricos diferentes a su equipo de cómputo (CPU, monitor o Equipo Portátil), como impresoras, plotters, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras, parlantes, secadores de cabello, aires acondicionados, ventiladores, taladros, cámaras fotográficas, de video y en general cualquier equipo que genere caídas de energía.

Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no están autorizados para utilizar los servicios y recursos tecnológicos de CORPOBOYACA.

POLITICA 11: ESCRITORIOS LIMPIOS

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, usb memory key, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el

COPIA NO CONTROLADA

horario normal de trabajo y fuera del mismo, con el fin de evitar la sustracción de accesorios de cómputo, como tarjetas inalámbricas, routers, mouses y otros.

POLITICA 12: ADMINISTRACION DE LA SEGURIDAD

Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los servicios y recursos tecnológicos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al Proceso Gestión Soporte Tecnológico.

Los funcionarios públicos, contratistas y pasantes que realicen las labores de administración de los servicios tecnológicos son responsables Por la implementación, permanencia y administración de los controles sobre los Recursos Computacionales. La implementación debe ser consistente con las prácticas establecidas por la Proceso Gestión Soporte Tecnológico.

El Proceso Gestión Soporte Tecnológico divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportara a la Dirección General de CORPOBOYACÁ, los casos de incumplimiento con copia a las oficinas de control interno y Sistemas. Documentará la instrumentación para llevar a cabo la ejecución de las políticas.

COPIA NO CONTROLADA

CONTROL DE CAMBIOS

Versión	Descripción del Cambio	Fecha
1	Políticas según versión 3 del PES	17/02/2014
2	Políticas según Versión 6 del IST-08 Copias de Seguridad Digital	27/06/2016

	ELABORÓ	REVISÓ	APROBÓ
CARGO:	Profesional Esp. Soporte Tecnológico.	Prof. Especia. Planeacion Organizacional.	Responsable proceso Soporte Tecnológico
NOMBRE:	Lilian M. García Gallo.	Germán G. Rodríguez C.	Luz Deyanira González C.
FIRMA:	ORIGINAL FIRMADO	ORIGINAL FIRMADO	ORIGINAL FIRMADO