POLÍTICAS INFORMATICAS

POLÍTICAS PARA LA INFRAESTRUCTURA DE TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

1. Alcance de la políticas

Las políticas estipuladas en el presente documento rigen para todos las unidades de negocio y personas que adelanten procesos relacionados con la infraestructura de tecnologías de información y comunicaciones de rtvc.

1.1. Definiciones

HELP DESK (MESA DE AYUDA): es la herramienta que permite el manejo centralizado de las incidencias y requerimientos que pueden hacer los diferentes usuarios en red de equipos de cómputo en rtvc.

Custodio: persona que se hace responsable de los recursos entregados como herramientas de apoyo para el desarrollo de sus actividades.

Outsourcing: es el proceso por el cual una firma contrata a una agente externo especializado para realizar tareas sobre las cuales no se está especializado.

Anti-virus: es una herramienta cuyo objetivo es detectar y eliminar virus informáticas.

Anti-spam: es una herramienta cuyo objetivo es prevenir el corre no deseado.

Sistema de detección de intrusos: es un programa usado para detectar accesos no autorizados a un computador o a una red.

LAN (local area network): red de área local.

WAN (wide area network): red de área extendida.

1.2. Objetivo

El objetivo principal de las políticas para infraestructura de tecnologías de información y comunicaciones es garantizar el funcionamiento de la plataforma tecnológica actual de rtvc, su crecimiento, desarrollo, incorporación de nuevos productos y servicios atendiendo a las tendencias tecnológicas y del mercado, y la compatibilidad con los estándares tecnológicos y con la infraestructura instalada.

2. Descripción de las políticas

2.1. Política para la adquisición de equipos informáticos

Toda solicitud de compra, adquisición o actualización de equipos informáticos y/o partes de estos equipos, debe contar con un concepto técnico por parte del área de informática en el que se indique que se cumplen con los estándares tecnológicos aceptables para la empresa, vigilando, particularmente, su compatibilidad con la infraestructura instalada y su posibilidad de mantenimiento y soporte técnico por parte de los fabricantes o de los representantes locales de las marcas en el país.

2.2. Política de mantenimiento preventivo

El mantenimiento técnico preventivo de todos los activos de infraestructura de tecnología de información de la entidad, deberá ser planeado y supervisado por el área de informática.

2.3. Política de mantenimiento correctivo

El mantenimiento técnico correctivo de todos los activos de infraestructura de tecnología de información de la entidad, debe ser planeado y supervisado de acuerdo a:

- Los requerimientos realizados a través del Help Desk, los cuales serán atendidos de acuerdo al ingreso a la aplicación del requerimiento, sin embargo dependiendo de la criticidad del requerimiento se maneja la prioridad del mismo.

En algunos casos dependiendo el tipo de garantía que cubra un fallo en el equipo, el soporte será brindado por compañías previamente calificadas y contratadas para tal fin.

Los activos informáticos de misión crítica (servidores, equipos de comunicación, etc.) deberán estar ubicados en áreas que cumplan con los requerimientos de seguridad física, condiciones

ambientales (aire acondicionado, control de humedad, etc.) apropiados, alimentación eléctrica controlada y regulada, servicio de energía eléctrica ininterrumpida, detección y alarmas contra incendios, etc.

2.4. Política de licenciamiento de software

Todo el software instalado en rtvc deberá estar legalmente licenciado. No se permitirá la instalación de software que no conste con la respectiva licencia de uso.

La custodia y almacenamiento de todos los medios que contengan componentes de software se hará en el área de informática. Solamente en casos debidamente justificados se podría permitir que copias de los medios se entreguen y estén en custodia de los usuarios finales.

El área de informática deberá propender a realizar contratos de licenciamiento de software a nivel corporativo, obteniendo las mejores condiciones económicas para la entidad. Salvo casos emergentes debidamente justificados lo deba realizar un área en particular, siempre y cuando las adquisiciones estén contempladas en el plan de compras.

La entidad no es responsable por el licenciamiento de los equipos personales de funcionarios o contratistas.

El software adquirido deberá ser siempre a través del licenciamiento legal del mismo. Este tipo de software siempre deberá incluir información para su instalación, la cual deberá ser usada por el personal de soporte técnico. Además debe exigirse al proveedor o a través de terceros, el entrenamiento en el uso y aplicabilidad del software, para el personal usuario al cual está destinado el mismo.

La instalación de software en los equipos de cómputo de la entidad debe ser realizada únicamente por el personal de informática. Sin embargo para proyectos especiales como el Centro de Emisión, TDT y los que se implementen a futuro, atendiendo a la particularidad de estos equipos, estas instalaciones de software son responsabilidad del líder del proyecto.

2.5. Política de custodia y tenencia de activos informáticos

Los activos informáticos y de comunicaciones solo podrán ser utilizados por funcionarios o contratistas que los requieran para el desarrollo de sus actividades diarias.

Los activos informáticos de usuario final (PC´s, monitores, teclados, impresoras, etc.) serán custodiados por el funcionario o contratista encargado de su operación.

Los custodios deberán ser empleados regulares de la empresa, a quienes se asignan los activos informáticos y son responsables pecuniariamente de su buen uso e integridad. Los usuarios son quienes utilizan para su labor diaria o eventual el activo informático y pueden ser empleados regulares de la empresa o no (empleados de outsourcing, contratistas externos, consultores, etc.)

La asignación de equipos informáticos a Custodios/Usuarios la hace el área de informática en base a los requerimientos que reciba de las otras áreas de la empresa para incluirlas en el plan de compras anual.

Una vez que un activo informático ha sido asignado a un Custodio/Usuario no puede ser asignado a ningún otro usuario.

Los recursos informáticos se brindaran en función de los recursos disponibles y las prioridades establecidas.

2.6. Política de software

El software desarrollado en rtvc se hará dentro del ámbito de competencia del área de informática. Ningún proyecto de desarrollo local de software se podrá hacer en cualquier otra dependencia de la empresa. El desarrollo local de software deberá cumplir los estándares técnicos que determine el área de informática.

Todas las modificaciones, cambios y ampliaciones a la funcionalidad actual de las aplicaciones informáticas, se harán por solicitud exclusiva de los responsables de las áreas que tengan relación con la funcionalidad de los sistemas.

Las áreas usuarios de menor nivel podrán identificar necesidades de cambios, y deberán canalizarlos dentro de sus estructuras organizacionales, esto es, siguiendo el órgano regular hasta llegar al nivel de responsable de área. Solamente el nivel responsable de área podrá interactuar con el responsable del área de informática para exponer y solicitar los cambios.

El área de informática evaluará los requerimientos de cambios y procurará atenderlos todos, siempre y cuando sean razonables, necesarios y justificados, no causen incompatibilidades funcionales o de datos con otras aplicaciones en funcionamiento y su relación costo-beneficio sea conveniente para la entidad. El área de informática atenderá los cambios requeridos de acuerdo a la prioridad en el tema a desarrollar.

El software desarrollado por el cual rtvc contrate este servicio, será propiedad intelectual de rtvc.

Cuando se adquiere software especializado a terceros o desarrollado por terceros, deberá siempre cumplir con los estándares corporativos en cuanto a sistema de base de datos, herramienta de desarrollo de la aplicación y sistema operativo base.

La custodia y almacenamiento de todos los medios que contengan componentes de este tipo de software se hará en el área encargada de su operación. En casos de que el área de informática lo solicite se podrá entregar copias con fines de respaldo.

En los casos en que en otras áreas, como parte componente de contratos de adquisición de bienes y/o servicios, se incluya software, como parte integrante o complementaria los equipos, o como parte componente de los servicios, el área contratante deberá contar con la participación del área de informática en el proceso de adquisición.

Para los contratos de soporte y/o mantenimiento de sistemas de información se debe involucrar al área de informática para apoyar la interventoria de los mismos.

2.7. Política de software antivirus, anti-spam, detección de intrusos

Es responsabilidad del área de informática el mantener activo, vigentes sus licencias y actualizado todo el software de protección tal como antivirus, antispam, detección de intrusos, etc., que protejan las instalaciones y activos informáticos de rtvc, así como también procuren una operación expedita y sin sobrecargas de la red de datos.

2.8. Política de plan de contingencia

El área de informática deberá tener un Plan de Contingencia que permita recuperar su operación en corto tiempo, en caso de fallas o inoperabilidad de su infraestructura informática.

2.9. Política de red de datos

La instalación de puntos de red conectados a las redes LAN o WAN de la empresa la hará exclusivamente el área de informática, de manera directa, con sus propios técnicos o a través de la contratación externa del servicio de instalación.

El área de informática tendrá la responsabilidad de llevar un control de inventario de los puntos de red instalados en todos los edificios y oficinas de la entidad. Esto incluye la certificación rotulación

de los mismos de acuerdo al estándar previamente establecido, y el uso de un sistema informático de control de este inventario.

En caso de requerirse un punto de red se debe canalizar y sustentar el requerimiento ante el responsable de área. De encontrar justificada la necesidad, cada responsable deberá hacer llegar al área de informática el requerimiento para ser atendido.

Para proyectos de cableado estructurado se utilizaran los estándares definidos internacionalmente para este fin cumpliendo toda la normatividad vigente, para la planeación, implementación y seguimiento de estos proyectos se debe contar con el aval técnico del área de informática.

Para ingresar un equipo de cómputo a la red de datos de rtvc el equipo debe tener todas las actualizaciones al día en sistema operativo y debe tener instalado el antivirus con todos sus paquetes actualizados.

2.10. Política de plataforma tecnológica

Se deberá orientar la expansión de la plataforma tecnológica de la entidad hacia redes y equipamiento de últimas tecnologías; a fin de que se beneficie de sus altas prestaciones, capacidades, economías de escala y de la inter-operatividad con otras marcas y tecnologías. Cumpliendo con los estándares y normas técnicas vigentes a la fecha de la implementación.

La entidad orientará el desarrollo de su plataforma tecnológica hacia redes convergentes, que permitan la prestación de servicios de voz, video, datos y otros de manera integrada.

Para la expansión de su infraestructura actual se deberá considerar las tecnologías existentes, sus áreas de incidencia y disponibilidad, de manera de evitar costos adicionales en la entidad.

2.11. Política de operaciones

Todos los trabajos de mantenimiento preventivo y correctivo que se planifiquen realizar en los sistemas de operación deben ser ejecutados en horarios de menor impacto en el servicio a nuestros clientes.

POLÍTICAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACION

1. Alcance de la políticas

Las políticas estipuladas en el presente documento rigen para todos las unidades de negocio y personas que manejen información de la entidad.

1.1. Definiciones

Confidencialidad: es la propiedad de la información por la que se garantiza que esta sea accesible únicamente por personal autorizado.

Integridad: es la propiedad de la información por la que se garantiza que esta sea modificable únicamente por personal autorizado.

1.2. Objetivo

El objetivo principal de las políticas para seguridad de los sistemas de información es proteger la información estratégica y determinar los niveles de acceso y confidencialidad.

2. Descripción de las políticas

1.1. Política de confidencialidad en los datos

El área de informática no violara el derecho a la privacidad y la confidencialidad de los datos colocados en los sistemas de información. Solo se permitirá el acceso de manera formal cuando este sea solicitado por un funcionario que tenga la autoridad competente con la respectiva justificación.

1.2. Política de seguridad de los sistemas de información

Las personas y dependencias que tengan bajo su responsabilidad información confidencial de rtvc deben tomar las medidas necesarias para protegerla y serán responsables de las consecuencias en caso de ausencia de esa protección.

Los dueños de la información serán los responsables de verificar que existan procedimientos y procesos de seguridad para asegurar el manejo y la integridad de la información que reside en medios magnéticos o en documentos.

Las contraseñas, claves, códigos de acceso, llaves, combinaciones y cualquier elemento de seguridad de similares características que permiten acceder a servicios, sistemas, redes, y a ubicaciones físicas con control de acceso son personales e intransferibles. Su uso, administración y reserva será responsabilidad del usuario asignado.

A través de las Directivas de seguridad de dominio, se mantendrán configurados cambios periódicos que obliguen a cada usuario a restablecer la contraseña de ingreso cada (60) días cumpliendo con requisitos como:
La longitud mínima de cada contraseña debe ser de 5 caracteres
El usuario no podrá reutilizar las (2) dos últimas contraseñas almacenadas
Estas directivas aplican también para el ingreso al sistema de gestión documental Orfeo puesto que se autentica mediante el directorio activo.

En cuanto al sistema administrativo y financiero Seven se configuran cambios periódicos de la contraseña cada 6 meses, cumpliendo con los siguientes requisitos:
La longitud mínima de cada contraseña debe ser de 10 caracteres y la máxima de 15 caracteres alfa numéricos
El usuario se inactiva en el momento de ingresar en tres oportunidades contraseñas que no corresponden.

Bajo ninguna circunstancia personal contratado por rtvc puede hacer uso de los recursos informáticos para realizar actividades de vulnerabilidad de otros sistemas de información o ataques a redes y aplicaciones externas, ni para contravenir normas jurídicas nacionales o internacionales.

El uso de los recursos lógicos de la entidad deben ser destinados exclusivamente para fines institucionales.

Los permisos de acceso a todos los sistemas sean estos de las plataformas informáticas, de telecomunicaciones, financieras, y cualquier otra plataforma que existiere, tendrán un tiempo de expiración de acuerdo a la aplicación.

En el momento que una persona se desvincule de rtvc bien sea funcionario o contratista debe informarse al área de informática de manera inmediata y por escrito para proceder a la inactivación de las cuentas que esta persona tenia asociadas.

POLÍTICAS DE RESPALDO DE INFORMACIÓN - BACKUP

1. Alcance de la políticas

Las políticas estipuladas en el presente documento rigen para todos los equipos servidores de nuestra entidad:

1.1. Definiciones

Backup: También conocidas como copia de seguridad. Un backup es la copia total o parcial de la información o de segmentos de información almacenados en un medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento, con el fin de salvaguardar la información y en el caso de pérdida de la información original, poder restaurarla.

1.2. Objetivo

El objetivo principal de las políticas de backup es garantizar la disponibilidad de la información que ha sido almacenada atendiendo a la importancia de la misma.

2. Descripción de las políticas

2.1. Política de copias de respaldo localmente

Semanalmente se deben hacer copias de la información de las unidades dispuestas en los discos duros de los equipos servidores de rtvc.

Cada usuario es responsable de ubicar la información de la cual se debe hacer copia de respaldo en la unidad pública del área destinada para tal fin.

2.2. Política de copias de respaldo externo

La entidad debe contar con un servicio para custodia y resguardo de los medios donde están almacenadas las copias de respaldo de datos en forma semanal.

2.3. Política de revisión de las copias de seguridad

Semestralmente se debe hacer la restauración de una copia de seguridad seleccionada en forma aleatoria para asegurar que las copias se están realizando de manera adecuada.

POLÍTICAS DE SEGURIDAD PARA LOS SITIOS WEB DE RTVC

2. Alcance de la políticas

Las políticas estipuladas en el presente documento rigen para todos los sitios web de nuestra entidad y todas sus unidades de negocio y que en adelante nombraremos de forma genérica como sitios web corporativos, los cuales son:

Sitio Web Institucional: http://www.rtvc.gov.co

Sitio Web de la Intranet: http://sites.google.com/a/rtvc.gov.co/rtvc-intranet/

Sitio Web de Radiónica: http://www.radionica.gov.co

Sitio Web de Radio Nacional de Colombia: http://www.radionacionaldecolombia.gov.co

Sitio Web de Bicentenario: http://www.bicentenario.gov.co

Sitio Web de Señal Colombia: http://www.senalcolombia.gov.co

Sitio Web de Institucional: http://www.institucional.gov.co

2.1. Definiciones

Backup: También conocidas como copia de seguridad. Un backup es la copia total o parcial de la información o de segmentos de información almacenados en un medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento, con el fin de salvaguardar la información y en el caso de pérdida de la información original, poder restaurarla.

CMS (Content Management System): Sistema gestor de contenidos es un programa que permite crear una estructura de soporte para la creación y administración de contenidos de un sitio web. El CMS es una interfaz que controla una o varias bases de

datos donde se aloja el contenido del sitio. El sistema permite manejar de manera independiente el contenido y el diseño. Así, es posible manejar el contenido y darle en cualquier momento un diseño distinto al sitio sin tener que darle formato al contenido de nuevo.

CVS (Concurrent Versions System): El CVS es una aplicación informática que implementa un sistema de control de versiones: mantiene el registro de todo el trabajo y los cambios en los ficheros (código fuente principalmente) que forman un proyecto (de programa) y permite que distintos desarrolladores (potencialmente situados a gran distancia) colaboren.

Cifrado: Se define como cifrado al proceso de convertir una información generada por una aplicación de red en una información ilegible para un intruso que trate de interceptarla en la red por donde viaja. La aplicación destino podrá recuperar la información original realizando un proceso de descifrado y con una o más claves de cifrado.

Intruso: Se conoce con este nombre cualquier usuario que trate de acceder información a la cual no tiene permiso, haciendo uso de vulnerabilidades de seguridad, de protocolos o por ingeniería social.

Log: Es un archivo que almacena un registro oficial de eventos durante un periodo de tiempo en particular. Este archivo es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para una aplicación, un servicio o un dispositivo.

Vulnerabilidad: Se conoce con este nombre cualquier debilidad que puede tener un sistema que permita a un intruso violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia de un sistema o de sus datos y/o de sus aplicaciones.

2.2. Objetivo

El objetivo principal de las políticas de seguridad de los sitios web es garantizar la confidencialidad, integridad y disponibilidad de la información que se socializa en los sitios web y de los servicios que se prestan a los usuarios que las visitan. También debe garantizar la implementación de herramientas que permitan controlar el acceso a recursos y servicios y dispositivos de nuestra infraestructura web.

3. Descripción de las políticas

3.1. Política de uso de registro de usuarios

Los sitios web corporativos deben manejar un componente de registro de usuarios, el cual debe permitir la administración de las cuentas para prestar servicios de acuerdo al perfil de cada una. Este registro de usuario debe validar a los mismos mediante una contraseña, la cual tiene que viajar cifrada por la red. El usuario debe tener la posibilidad de recuperar la contraseña a través del correo electrónico.

Sólo se permite el acceso al sitio web de la Intranet a usuarios registrados y con alguna vinculación demostrable con nuestra entidad. El usuario de acceso a la Intranet será creado por el administrador de la red, en el momento que se cree su cuenta de correo electrónico y dicho usuario debe ser eliminado en el momento en que el vínculo de la persona con la entidad termine.

3.2. Política de gestión de sesiones seguras

Los usuarios del servidor dedicado que aloja nuestros sitios web sólo pueden acceder al mismo haciendo uso de sesiones seguras a través de ssh, garantizando que tanto las contraseñas como la información viaje cifrada por la red. Está prohibido el acceso desde equipos públicos como café internet, equipos de universidades y desde cualquier equipo donde puedan estar instalados programas por los cuales pueda capturarse la contraseña antes del cifrado de la misma.

Para los usuarios de los sitios web corporativos no se aplica esta política, ya que por las características de la información y los servicios que tienen acceso, no se hace necesario que las sesiones viajen cifradas por la red.

3.3. Política de backups

El administrador del servidor web debe preparar, actualizar de manera periódica y revisar el funcionamiento de unos actividades para realizar los backups de los sitios web, los cuales deben garantizar la disponibilidad de los sitios en caso de alguna eventualidad como un desastre, o de ataques contra la integridad de la información realizados por algún intruso.

El administrador del servidor web debe entregar un documento donde se resuma la actividad de copias de seguridad realizadas durante el mes.

El administrador del servidor web debe permitir el acceso a la última copia de seguridad de los sitios y las bases de datos correspondientes al personal encargado de administrar cada unos de los sitios.

Es labor del administrador del servidor web y de los ingenieros desarrolladores web de cada uno de los sitios revisar de manera periódica las copias de seguridad generadas.

El administrador del servidor debe garantizar que el servidor de respaldo del servidor dedicado se mantenga actualizado con las últimas copias de seguridad, ya sean totales o incrementales.

3.4. Política de generación de logs de auditoría

Todas las aplicaciones de servidor implementadas deben tener la posibilidad de hacer seguimiento de las actividades de los usuarios a través de logs de auditoría. El administrador de cada aplicación debe realizar una revisión periódica de dichos logs para verificar tanto el buen funcionamiento de dichas aplicaciones como para estudiar los problemas de vulnerabilidad que pueden tener nuestros servicios.

Así mismo se deben generar logs para hacer seguimiento estadístico de los usuarios, de acuerdo a los requerimientos de nuestra organización o de entidades externas.

3.5. Política de acceso al servidor dedicado

Los usuarios del servidor dedicado sólo pueden acceder al mismo mediante el uso de sesiones seguras, desde computadores confiables y es responsabilidad de dichos usuarios las consecuencias de los eventos que se puedan realizar con el uso de la cuenta que le ha sido asignada.

En este servidor solamente pueden tener cuenta de acceso por sesión segura las siguientes personas:

- El Jefe de la Oficina de Informática
- El administrador del servidor dedicado
- Los ingenieros Web de cada uno de los sitios

El control de acceso a recursos y servicios a través de las cuentas creadas es responsabilidad del administrador del servidor dedicado.

3.6. Política de privacidad de los usuarios registrados en los sitios corporativos

Es responsabilidad del grupo Web de las áreas misionales velar por la confidencialidad y privacidad de la información de los usuarios que se registren en los sitios Web. Está

completamente prohibido entregar esta información a terceros que quieran obtener algún lucro de las mismas

En los términos y condiciones de cada sitio Web debe ir publicado un ítem de privacidad con el objetivo que los usuarios que se registren tengan la garantía que la información que han entregado no va a ser usada sin su consentimiento.

Como excepción a esta política se pueden entregar datos estadísticos de campañas conjuntas o de concursos que así lo requieran. Los datos entregados no deben violar los términos y condiciones, ni las políticas de seguridad publicados en cada uno de los sitios web y aceptados por los usuarios en el momento del registro.

RTVC puede hacer uso de la información para verificación de datos, campañas, para estudios de mercado y manejo de estadísticas, pero sin violar los acuerdos estipulados en los términos del servicio que el usuario obtiene cuando se registra.

3.7. Política de instalación y actualización de software en el servidor Web dedicado

El administrador del servidor Web es el responsable de la instalación, actualización y revisión de las vulnerabilidades del software instalado inherente a su labor: sistema operativo, servidor web Apache, servidor de base de datos, herramientas estadísticas y de medición de desempeño y gestión.

Los ingenieros Web de los sitios de la entidad son los responsables de la instalación, actualización y revisión de las vulnerabilidades del software instalado inherente a su labor: sistema gestor de contenidos de los sitios a su cargo.

El administrador del servidor web debe entregar un informe periódico de actualización de software, a través de una plantilla que será el documento de soporte, evidencia y trazabilidad de esta tarea.

Los ingenieros Web deben generar un informe periódico referente a las actividades realizadas bajo su cargo, con el fin de generar la documentación respectiva.

El administrador del servidor web debe encargarse de la administración del CVS ó sistema de gestión de versiones. Este sistema debe ser accedido por los miembros del grupo web que necesiten revisar las actualizaciones de cada sitio web.

No DEL CAMBIO	FECHA	E	M	C	DESCRIPCIÓN DEL CAMBIO	*RESPONSABLE*
1	22/08/2012		x		Se cambió el logo del cabezote y se actualizo su contenido	Oficina de planeación.