INSTITUTO DEPARTAMENTAL DE TRANSITO DEL QUINDÍO

GESTIÓN ADMINISTRATIVA Y FINANCIERA

TABLAS DE CONTROL DE ACCESO - TCA

2018

VERSION 1

Tabla de contenido

POLITICAS PARA LA GESTION DE SEGURIDAD DE LA INFORMACION – CONTROL DE ACCESO

1. INTRODUCCIÓN

El presente documento establece las políticas y normas para garantizar un adecuado control de acceso a los sistemas de información del Instituto Departamental de Transito del Quindío para la Participación y el Fortalecimiento de la Democracia.

2. OBJETIVOS

- Impedir el acceso no autorizado a los sistemas de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

3. ALCANCE

Las políticas y normas definidas en este documento aplican para todos los funcionarios, contratistas y terceros que tengan acceso a los sistemas de información del Instituto Departamental de Transito del Quindío, para la Participación y el Fortalecimiento de la Democracia.

4. RESPONSABILIDADES

Oficial de Seguridad de la Información

- Sugerir procedimientos para la asignación de acceso a los sistemas, bases de datos y servicios de información multiusuario; la solicitud y aprobación de acceso a Internet o redes externas; el uso de computación móvil, trabajo remoto.
- Analizar y sugerir medidas a ser implementadas para hacer efectivo el control de acceso de los usuarios a diferentes servicios como VPN, Internet o digitalización entre otros.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de acceso, creación de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios, uso controlado de utilitarios del sistema.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.

Los Propietarios de los activos de Información

Evaluar los riesgos a los cuales se expone la información con el objeto de:

- Clasificar la información
- Determinar los controles de acceso, autenticación y utilización a ser implementados en cada caso.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los Privilegios de acceso a la información.

Los Líderes de los Procesos

Autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, acatando las normas vigentes. Asimismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

Jefe Oficina de Información Pública

Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.

Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.

Evaluar el costo y el impacto de la implementación de “enrutadores” o “Gateway” adecuados para subdividir la red y recomendar el esquema apropiado.

Implementar el control de puertos, de conexión a la red y de ruteo de red.

Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.

5. POLITICAS GENERALES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Políticas

Deben establecerse medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y servicios de TI. Los controles de acceso deben ser conocidos por todos los servidores públicos de la entidad y limitar el acceso hacia los activos de información de acuerdo a lo establecido por el perfil de cargo.

Se deben implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, bases de datos y servicios, estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

5.1 CONTROL DE ACCESO

NORMAS

Requerimientos para el Control de Acceso

Control de Acceso

Los controles de acceso deberán contemplar:

a) Requerimientos de seguridad de cada una de las aplicaciones.

b) Definir los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo a su perfil de cargo en la entidad.

Administración de Accesos de Usuarios

La Oficina de Información Pública establece procedimientos para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Creación de Usuarios

La Oficina de Información Pública, deberá mantener los registros donde cada uno de los líderes responsables de los procesos haya autorizado a los servidores públicos o terceros el acceso a los diferentes sistemas de información de la entidad.

Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que debe ser único por cada servidor público o tercero.
Cuando se retire o cambie de contrato cualquier servidor público o tercero, se deberá aplicar la eliminación o cambios de privilegios en los sistemas de

información a los que el usuario estaba autorizado.

El proceso de gestión de información y comunicaciones deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información por parte de los servidores públicos y terceros, manteniendo los registros de las revisiones y hallazgos.

Administración de Contraseñas de Usuario

Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales.

Todos los servidores públicos deberán cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima de 3 meses, a excepción de aquellos que contengan información confidencial o secreta en cuyo caso el cambio se debe realizar cada mes.

Los sistemas de información deberán bloquear permanentemente al usuario luego de 5 intentos fallidos de autenticación a excepción de aquellos que contengan información confidencial o secreta en cuyo caso después de 3 intentos fallidos de autenticación se realizará el bloqueo.

Uso de Contraseñas

Los usuarios deben cumplir las siguientes normas:

a) Mantener los datos de acceso en secreto.
b) Contraseñas fáciles de recordar y difíciles de adivinar.
c) Que las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
d) Notificar de acuerdo a lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

a) Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.
b) Bloquear el equipo de cómputo tras abandonar el puesto de trabajo.
c) Bloqueo automático de la sesión en el equipo de cómputo tras inactividad superior a 5 minutos.
d) Apagar los equipos de cómputo al finalizar la jornada laboral.

Control de Acceso a la Red

El proceso de Gestión de Tecnologías de Comunicación e Información debe asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por el jefe inmediato, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del oficial de seguridad de la información.

Autenticación de Usuarios para Conexiones Externas

La autenticación de usuarios remotos deberá ser aprobada por el líder del proceso de Gestión de Tecnologías de Comunicación e Información.

Control de Conexión a Redes

La infraestructura del Ministerio del Interior y el Fondo para la Participación y el Fortalecimiento de la Democracia deberá estar separada por Vlans para garantizar la confidencialidad de los datos que se transmitan.

Seguridad en los Servicios de Red

Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la entidad.

Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la entidad.

Control de Identificación y Autenticación de Usuarios.

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

Sistema de Administración de Contraseñas

El sistema de administración de contraseñas debe:

a) Obligar el uso de User ID´s y contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de las mismas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
d) No permitir mostrar las contraseñas en texto claro cuando son ingresadas.
e) Almacenar las contraseñas en forma cifrada.

Sesiones Inactivas

Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que Terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

Si los sistemas de información detectan inactividad por un periodo igual o superior a diez minutos, deben automáticamente aplicar, “timeout” es decir, finalizar la sesión de usuario

Limitación del Tiempo de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a

las aplicaciones de alto riesgo:

a) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
b) Documentar los funcionarios o contratistas que no tienen restricciones horarias y los motivos y evidencia de la autorización expedida por el líder del proceso de Gestión de Tecnologías de Comunicación e Información.