POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
CONTROL DE ACCESO

Elaborado por:	Revisado por:	Aprobado por:
Asesor TIC	Asesor TIC	Rector(a)

OBJETIVO

Establecer las políticas y normas para garantizar un adecuado control de acceso a los sistemas de información de la Institución Universitaria Colegio Mayor del Cauca

1. ALCANCE

Este documento aplica para todos los funcionarios, contratistas, y terceras personas que tengan acceso a las instalaciones de la Institución.

2. DEFINICIONES

Control de acceso: garantizar que el acceso a los activos esté autorizado y restringido en función de los requisitos comerciales y de seguridad. [ISO/IEC 27000: 2016].

Autenticación: Comprobación de la identidad de una persona, entidad u ordenador.

Política: intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000: 2016].

Equipo desatendido: Terminal que no está bajo supervisión de un funcionario de la entidad temporalmente.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información de un sistema de tratamiento de la información sean asociadas de un modo inequívoco a un individuo o entidad [CESID: 1997]

3. POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN – CONTROL DE ACCESO

La institución Universitaria Colegio Mayor del Cauca establece medidas de control de acceso a nivel de red, sistema operativo, sistemas de información y servicios de TI para los controles de acceso lógico. Estas medidas son de conocimiento de todo el personal de la Institución y limitan el acceso a los activos de información de acuerdo con lo indicado por el rol o perfil del cargo establecido.

Normas y estándares:

1. La Institución establece la definición e implementación de un procedimiento para la asignación de privilegios de acceso a los usuarios, los cuales deben estar claramente documentados, comunicados y cuyo cumplimiento será controlado por el líder de seguridad o líder del proceso responsable del activo de información que se quiere acceder.
2. El proceso responsable deberá mantener los registros de las autorizaciones a personal de la institución o terceros, del acceso a los diferentes sistemas de información de la Institución.
3. Los datos de acceso a los sistemas de información están conformados por un ID único a cada funcionario, contratista o tercero, un nombre de usuario y una contraseña. En el momento de terminación o modificación del contrato con cualquier funcionario o tercero, será responsabilidad del proceso de TI remover los respectivos permisos para acceso a la información interna de la Institución, previa comunicación del proceso de Gestión de Talento Humano.
4. El líder de seguridad o proceso de auditoría de la seguridad de la información deberá realizar revisiones periódicas a los privilegios otorgados a los diferentes sistemas de información, conservando registros de las revisiones y los hallazgos.
5. Las contraseñas de usuario deberán tener un mínimo de 8 caracteres y una combinación de números, letras en minúscula y mayúscula. Es deseable que también tengan caracteres especiales.
6. Todo el personal deberá cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima de 3 meses.
7. Los sistemas de información deberán impedir la entrada permanentemente al usuario luego de 5 intentos fallidos de autenticación.
8. Todos los empleados deben cumplir las siguientes normas:
    a) Mantener sus credenciales de acceso en secreto
    b) Sus datos de acceso deben ser fáciles de recordar.
    c) No deben estar basadas en información personal, como fechas de nacimiento, números de teléfono, etc. que algún tercero pueda adivinar u obtener fácilmente.
    d) Cualquier incidente relacionado con: pérdida o robo de contraseñas o indicios de pérdida de confidencialidad debe ser notificado de acuerdo con lo establecido.
9. Los equipos desatendidos deben contar con las siguientes normas para garantizar su protección:

a) Los equipos instalados en áreas de usuarios, como estaciones de trabajo o servidores de archivo requieren protección específica contra accesos no autorizados cuando se encuentran desatendidos.
b) El personal debe bloquear de forma manual su equipo de cómputo al abandonar el lugar de trabajo.
c) El dispositivo debe bloquearse automáticamente tras 3 minutos de inactividad.
d) Todos los equipos de cómputo deben ser apagados al finalizar la jornada laboral o estar bloqueados de ser necesario que permanezca activo.

10. El proceso de TI es responsable de restringir el acceso a páginas de contenido para adultos, redes sociales, mensajería instantánea y demás páginas que no sean de uso corporativo mediante el uso de un servidor proxy, firewall o la estrategia que mejor se ajuste a los recursos y protección de los activos de información.
11. El acceso a los sitios web anteriormente mencionados será permitido únicamente con aprobación del jefe inmediato (líder de proceso), según la necesidad del cargo y posterior verificación del líder de seguridad de que el sitio no contenga código malicioso.
12. Se deben mantener instalados y habilitados únicamente los servicios y puertos que sean utilizados por los sistemas de información y software de la institución. El acceso lógico a estos servicios debe ser controlado mediante la apropiada configuración del firewall.
13. Todos los usuarios (incluido el personal de soporte técnico, como operadores, administradores de red, programadores de sistemas y administradores de bases de datos) deben tener un identificador único, de uso personal y exclusivo, con el fin de que las actividades tengan trazabilidad en los sistemas de información.
14. En caso de hacer uso de un sistema de administración de contraseñas, debe:
    a) Permitir que los usuarios puedan cambiar su contraseña, teniendo en cuenta los requisitos mencionados anteriormente, e incluir un esquema de confirmación para contemplar los errores de ingreso.
    b) Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
    c) No permitir mostrar las contraseñas en texto claro cuando son digitadas.
    d) Almacenar las contraseñas en forma cifrada.
15. Las conexiones deben ser restringidas al horario normal de oficina, a menos que exista un requerimiento operativo de horas extra. En caso de permitir

acceso por fuera de este horario, debe documentarse qué funcionarios o contratistas tienen este permiso, sus motivos y evidencia de la autorización expedida por el líder de la oficina de gestión de información y comunicaciones.

16. No está permitido:

a) El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, web transfer, descargas de música, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en la Institución.
b) El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook (NO CORPORATIVO), Kazaa, Nuke, skype, youtube, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la Institución.
c) La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

4. DOCUMENTOS DE REFERENCIA

- Política de Seguridad de la Información.

5. CONSIDERACIONES GENERALES

No aplica.

6. ANEXOS

No aplica.

7. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CONTROL DE CAMBIO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN CONTROL DE ACCESO			
Proceso: Comunicaciones y TIC Subproceso: Gestión de Recursos Tecnológicos			
Código 104.03.01.02.02.D.10	Versión 01	Emisión 25-09-2018	Página 1-1