POLÍTICA PARA PROVEEDORES

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

COPIA CONTROLADA

Elaboró:	Revisó:	Aprobó:
_____	_____	_____
Contratista de Seguridad y Privacidad de la Información	Director Gestión de Recursos Tecnológicos	Rector(a)

1. OBJETIVO

Establecer la Política de Seguridad de la Información para proveedores de la Institución Universitaria Colegio Mayor del Cauca.

2. ALCANCE

La política que presenta este documento se aplica para todo el personal externo a la Institución Universitaria Colegio Mayor del Cauca y que presta sus servicios mediante un contrato o convenio. Cualquier empresa o tercero que para el desarrollo de las actividades contractuales deba obtener acceso a los activos de información de la Institución, debe comprometerse a conocer y acatar la presente Política.

COPIA CONTROLADA

3. DEFINICIONES

Confidencialidad: propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000: 2016].

Disponibilidad: propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000: 2016].

Integridad: propiedad de exactitud y completitud. [ISO/IEC 27000: 2016].

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

Proveedores: tercero que abastece de materiales, servicios u otros suministros a una organización, los cuales son necesarios para su desarrollo y funcionamiento.

Malware: programa o código malicioso que es dañino para los sistemas informáticos pueden ser: spyware (software espía), adware (software publicitario), phishing, virus, troyanos, gusanos, rootkits, ransomware y secuestradores del navegador.

4. POLÍTICA DE SEGURIDAD PARA PROVEEDORES

El personal externo que tenga acceso a la información de la institución deberá considerar que dicha información por defecto, tiene carácter público confidencial (véase Documento 100.05.05.D.42 la Política de Gestión de Activos). La única información

que se puede considerar como no confidencial es aquella que esté dispuesta en los canales de difusión pública.
Para acceder a los sistemas de información de la Institución, se necesita un acceso adecuado, como se indica en la política de control de acceso. Se incorporará a cada tercero una identificación segura y única para su autenticación.

En el caso que, por asuntos únicamente relacionados a lo laboral, el empleado de la empresa proveedora entre en posesión de información confidencial en algún tipo de soporte, debe entenderse que esa posesión es de forma temporal, con obligación de secreto y sin que ello le confiera algún derecho de posesión, titularidad o copia sobre dicha información. El empleado de la empresa proveedora se compromete a devolver los soportes mencionados inmediatamente después de la finalización de la tarea que dio origen al uso temporal de los mismos, y en cualquier caso, al cabo del término de la contratación que tenga con la Institución.

Los recursos que se ponen a disposición del personal externo están disponibles exclusivamente para cumplir las obligaciones y propósito de los contratos que se firmen con ellos. Por tanto, se prohíbe:

- El uso de estos recursos para actividades no relacionadas con el objeto del servicio.
- La búsqueda o explotación de vulnerabilidades en cualquier aplicación o equipos.
- Introducir en los sistemas de información o la red interna contenidos obscenos, inmorales, amenazadores u ofensivos.
- Introducir voluntariamente cualquier tipo de malware, dispositivo lógico, físico o cualquier tipo de secuencia de instrucciones que pueda causar daño o alteración en los recursos informáticos
- Intentar obtener accesos o permisos diferentes a los que les hayan sido asignados.
- Intentar acceder a áreas restringidas de los sistemas de información sin la respectiva autorización.

Cada usuario externo, por el hecho de serlo, asume ciertas responsabilidades, como son:

- Cumplir con la política de confidencialidad y demás políticas relacionadas con seguridad y privacidad de la información.

COPIA CONTROLADA

- El usuario será responsable de todas las acciones registradas en los sistemas informáticos de la institución realizadas con su identificador asignado.
- Los usuarios externos deberán acatar los controles para contraseñas que se indican en la política de control de acceso.
- Los usuarios externos no deben revelar bajo ninguna circunstancia su identificador y/o contraseña a otra persona, ni mantenerla por escrito a la vista o alcance de terceros.
- Si un usuario tiene sospechas de que su acceso está siendo utilizado por otra persona, debe cambiar inmediatamente su contraseña y reportar el incidente al proceso de Gestión de Recursos Tecnológicos o líder de Seguridad de la Información de la Institución.

5. DOCUMENTOS DE REFERENCIA

- 100.05.05.D.42 Política de Gestión de Activos
- 100.05.05.D.40 Política de Control de Acceso
- Acuerdo de Confidencialidad
- 104.01.02.D.17 Mejores Prácticas

6. DISPOSICIONES FINALES

6.1. DIFUSIÓN

El personal autorizado por el proceso Gestión de Recursos Tecnológicos realizará la socialización y/o difusión de esta política a la comunidad universitaria y grupos de interés, de acuerdo a las directrices del documento 104.01.02.D.13 Plan de sensibilización de Seguridad de la Información.

6.2. ACTUALIZACIÓN

Para garantizar la vigencia, mejora continua y actualización de esta política, deberá ser revisada por lo menos una vez al año por personal competente y autorizado del proceso Gestión de Recursos Tecnológicos y será el Comité Institucional de Gestión y Desempeño quien apruebe las mejoras a implementar.

Durante la actualización se deberá tener en cuenta la normatividad vigente, lineamientos institucionales y resultado de auditorías de seguridad y privacidad de la información.

COPIA CONTROLADA

6.3. SANCIONES

El incumplimiento de esta política se aplicará la normativa vigente en la Institución Universitaria Colegio Mayor del Cauca, además de las normas emitidas a nivel nacional y regional a través del proceso Gestión y Desarrollo del talento humano.

7. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIOS REALIZADOS
2 de diciembre de 2019	Se realizó actualización, y ajustes relacionando los documentos de referencia codificados.
21 de septiembre del 2021	Se actualizó apartado de sanciones.
7 de octubre del 2021	Se actualizó apartado de sanciones. Se actualizó códigos de documentos de referencia.
23 de junio del 2022	Se realizó revisión de la política en todos sus aspectos con el equipo de seguridad de la información donde se considera que actualmente no requiere modificación relevante a la fecha evaluada. Se realizó actualización de cargo de asesor TIC a Director de Gestión de Recursos Tecnológicos.
13 de octubre de 2022	Se actualiza la política de acuerdo a revisión realizada por el proceso de Gestión de Recursos Tecnológicos.

COPIA CONTROLADA