POLÍTICA DE DESARROLLO SEGURO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Contratista Seguridad y Privacidad de la Información	Director Gestión de Recursos Tecnológicos	Rector(a)

1. OBJETIVO

Establecer las políticas para la seguridad de la información en los procesos de adquisición, desarrollo y soporte de software.

2. ALCANCE

El presente documento se aplica para la adquisición de software, desarrollos internos o tercerizados, así como para el personal encargado del mantenimiento de los productos software utilizados por la Institución.

3. DEFINICIONES

Desarrollo: Creación o mejora de un producto *software* a partir de especificaciones ceñidas a los requerimientos de la Institución.

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].

4. POLÍTICA DE DESARROLLO SEGURO

La presente política establece controles para garantizar que la seguridad y privacidad de la información sea un requisito para el desarrollo de nuevos sistemas o la mejora de existentes.

En caso de que el desarrollo sea llevado a cabo por el personal de la Institución, debe incluirse los requisitos de seguridad de la información en los nuevos sistemas de

información o la mejora de los actuales. Estos requisitos deben ser identificados mediante herramientas como: obtención de requisitos de cumplimiento a partir de políticas y reglamentación, modelado de amenazas, revisiones de incidentes o umbrales de vulnerabilidades. Esta identificación debe ser documentada y revisada por las partes interesadas. En caso de que estos desarrollos sean producidos por terceros, debe seguirse un proceso formal de adquisición, que incluya los requisitos de seguridad de la información de la Institución.

Se deben realizar pruebas periódicas a los sistemas de información de la entidad, para lo cual se debe tener bien definidos ambientes de pruebas seguros; en caso de que el desarrollo sea hecho externamente a la Institución, debe exigirse este ambiente de pruebas al proveedor en los contratos, estos ambientes deberán permitir ser auditados por personal autorizado de la Institución. De igual manera, el nivel de protección de la información que se encuentra en un ambiente de prueba no puede ser menor que el utilizado en procesos de desarrollo. Debe evitarse que los datos de producción sean utilizados para el desarrollo, en caso de ser necesarios, estos datos deben permanecer en estos ambientes deberán estar bajo monitoreo permanente.

El proceso Gestión de Recursos Tecnológicos debe implementar los controles necesarios para asegurar que las migraciones entre ambientes de desarrollo, pruebas y producción sean aprobadas de acuerdo al procedimiento de control de cambios.

El Profesional Universitario de Desarrollo de Sistemas de Información, debe certificar que cualquier tipo de desarrollo que vaya a ser pasado a producción cumple con los requerimientos de seguridad establecidos antes de realizar este proceso. Esta validación se realiza con metodologías o Instructivos establecidos o creados por el equipo de desarrollo de sistemas de Información para tal fin, documentando todas las pruebas realizadas.

Es responsabilidad del Profesional Universitario de Desarrollo de Sistemas de Información que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén adecuadamente actualizados y parchados.

Todo desarrollo, que haya sido creado interna o adquirido por terceros, debe contar con un proceso de soporte. En caso de ser creado de manera interna, el (los) desarrollador(es) deben proporcionar un nivel adecuado de soporte, capacitación y documentación, en caso de ser adquirido por terceros o de manera externa, debe exigirse durante la contratación

que se cuente con un proceso de soporte, capacitación y documentación para los incidentes que puedan presentar las aplicaciones.

Todas las aplicaciones (sistemas), desarrollos internos o externos, deben asegurar que:

- Tengan una opción de cerrar sesión o desconexión, que permite terminar completamente con la sesión, disponible en todas las páginas protegidas por autenticación o control de acceso lógico.
- Los formularios de ingreso de datos deben validar aspectos como tipos de datos, longitud, rangos válidos, listas de caracteres aceptados, caracteres considerados peligrosos, etc.
- No se debe divulgar información sensible de la aplicación mediante los mensajes de error mostrados al usuario.
- Validar los datos de autenticación y cumplir con las mejores prácticas relacionadas con control de acceso lógico, adquisición, desarrollo y mantenimiento de sistemas.
- Antes de la puesta en producción, todas las características que no sean estrictamente esenciales deben ser removidas de la aplicación.
- Las conexiones a la base de datos son cerradas desde las aplicaciones tan pronto no sean requeridas.
- No se debe poder ejecutar comandos en el sistema operativo del servidor que las aloja.
- Debe prevenirse revelar la estructura de directorios de los sistemas de información de la Institución.
- Los valores para conexión a base de datos no deben estar insertados en el código sino en archivos independientes que permanecen por fuera del control de cambios, y que, de ser posible, se encuentren cifrados.
- Generar copias de respaldo, realizar pruebas y tener actualizados los procedimientos para cargue en caso de ser necesario.
- Cumplir con el Instructivo desarrollo de sistemas de información.

5. DOCUMENTOS DE REFERENCIA

100.05.05.D.40 Política de control de acceso.
104.01.02.02.I.02 Instructivo Desarrollo Sistemas de Información.

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.

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. ANEXOS

No aplica.

8. CONTROL DE CAMBIOS

FECHA DE CAMBIO	CAMBIOS REALIZADOS
2 de diciembre de 2019	Actualización del objetivo y alcance, articulación de la política de desarrollo con la política control de acceso y mejores prácticas de seguridad y privacidad de la información. Adición de numeral 6 Disposiciones Finales.
21 de septiembre del 2021	Se actualizó apartado sanciones.

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. Se actualiza código de la política según nueva TRD.
13 de octubre de 2022	Se actualiza la política según revisión realizada por el proceso de Gestión de Recursos Tecnológicos.