1. OBJETIVOS

Definir las directrices para:

a) Asegurar que la seguridad y privacidad de la información se diseña e implementa dentro del ciclo de vida de desarrollo seguro del software y los sistemas de información.

b) Asegurar que todos los requisitos de seguridad y privacidad de la información se identifican y se abordan al desarrollar o adquirir aplicaciones

c) Asegurar que los sistemas de información se diseñan, como implementan y operan de forma segura dentro del ciclo de vida del desarrollo.

d) Asegurar que el software se escribe de forma segura, lo que reduce el número de posibles vulnerabilidades de seguridad y privacidad de la información en el software.

e) Validar si se cumplen los requisitos de seguridad y privacidad de la información cuando las aplicaciones o el código se despliegan en el entorno de producción.

f) Asegurar la aplicación de las medidas de seguridad y privacidad de la información requeridas por la Universidad en el desarrollo de sistemas tercerizados.

g) Proteger el entorno de producción y los datos del peligro que suponen las actividades de desarrollo y prueba.

h) Preservar la seguridad y privacidad de la información al ejecutar los cambios

i) Asegurar la pertinencia de las pruebas y la protección de la información operativa utilizada para las mismas.

2. ALCANCE

Las presentes directrices aplican a todos los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros de la Universidad Surcolombiana

3. DEFINICIONES

Ciclo de Vida de Desarrollo Seguro (SDLC Seguro): Conjunto de fases, actividades, controles y buenas prácticas aplicadas durante la planificación, diseño, desarrollo, pruebas, implementación, operación y retiro de sistemas de información, con el propósito de incorporar la seguridad desde el inicio y durante todo su ciclo de vida.

Entidad: puede representar a un usuario humano, así como a un elemento técnico o lógico (por ejemplo, una máquina, un dispositivo o un servicio).

Derechos de acceso con privilegios: son derechos de acceso proporcionados a una identidad, una función o un proceso que permite realizar actividades que los usuarios o procesos típicos no pueden realizar.

Desarrollo Seguro: Enfoque de desarrollo de software que incorpora requisitos y controles de seguridad en todas las etapas del ciclo de vida, con el fin de prevenir, detectar y corregir vulnerabilidades.

Gestión de Cambios: Proceso mediante el cual se solicitan, evalúan, aprueban, implementan, documentan y verifican los cambios realizados sobre sistemas, aplicaciones o componentes tecnológicos.

Software: Conjunto de programa, instrucciones y reglas informáticas para ejecutar ciertas tareas específicas en un dispositivo electrónico

Software de Terceros: Aplicación, componente, biblioteca, servicio o código desarrollado y administrado por un proveedor o entidad externa a la organización.

4. MARCO DE REFERENCIA

La gestión de riesgos y oportunidades en la Universidad Surcolombiana considera para su labor, los lineamientos definidos en las directrices y políticas institucionales, además de las consideraciones definidas en:

- La norma ISO 31000:2018– Gestión del riesgo. Principios y directrices.
- La norma ISO IEC 27005:2022 – Gestión de riesgos para la seguridad de la información.
- Los lineamientos definidos en los documentos del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Los requisitos aplicables a la gestión del riesgo, detallados en el estándar ISO IEC 27001:2022 y la ISO IEC 27701:2025
- Código de Práctica para Controles de Seguridad de la Información - GTC ISO IEC 27002:2022 Tecnología de la Información. Técnicas de Seguridad.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Guía de Administración de riesgos y el diseño de controles en entidades públicas
- CONPES de Seguridad Digital (CONPES 3854 de 2016 y actualizaciones)
- Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- Política de Gobierno Digital (Decreto 1078 de 2015 y actualizaciones)
- Modelo Integrado de Planeación y Gestión – MIPG (DAFP)
- FURAG (Formulario Único de Reporte de Avance de la Gestión)
- Ley 1581 de 2012 y Decreto 1377 de 2013
- Lineamientos y guías de la Superintendencia de Industria y Comercio.

5. GENERALIDADES

Estas directrices son la declaración general que establece la Universidad para el ciclo de vida de desarrollo seguro con base en los siguientes controles de acuerdo a las normas:

ISO/IEC 27001:2022

A.8.25 Ciclo de vida de desarrollo seguro
A.8.27 Arquitectura de sistemas seguros y principios de ingeniería
A.8.28 Codificación segura
A.8.29 Pruebas de seguridad y privacidad en el desarrollo y la aceptación
A.8.30 Desarrollo tercerizado
A.8.31 Separación de los entornos de desarrollo, prueba y producción
A.8.32 Gestión de cambios

A.8.33 Información de la prueba

ISO/IEC 27701:2025

A.3.27 Ciclo de vida de desarrollo seguro
A.3.28 Requisitos de seguridad de las aplicaciones
A.3.29 Principios de arquitectura e ingeniería de sistemas seguros
A.3.30 Desarrollo externalizado
A.3.31 Información de prueba

6. DIRECTRICES

6.1 CICLO DE VIDA DE DESARROLLO SEGURO

El desarrollo seguro es un requisito para crear un servicio, una arquitectura, un software y un sistema seguro, para lograr esto, la Universidad tiene en cuenta los siguientes factores:

a) separación de entornos de desarrollo, pruebas y de producción;

b) guía sobre la seguridad y privacidad en el ciclo de vida de desarrollo de software:

1. seguridad y privacidad en la metodología de desarrollo de software
2. directrices de codificación seguras para cada lenguaje de programación utilizado, ver GUIA DE BUENAS PRÁCTICAS EN BASES DE DATOS

c) requisitos de seguridad y privacidad en la fase de especificación y diseño, ver ES-GSPI-FO-06 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS;

d) Controles de firewall a través de equipos físicos como F5 Y Checkpoint;

e) repositorios seguros para el código fuente y la configuración, seguridad en el control de versiones; ver BUENAS PRÁCTICAS PARA MANEJO DE REPOSITORIO Y VERSIONAMIENTO EN GITHUB;

f) conocimientos y formación necesarios sobre seguridad y privacidad de las aplicaciones;

g) capacidad de los desarrolladores para prevenir, encontrar y corregir vulnerabilidades;

h) requisitos de licencia y alternativas para asegurar soluciones rentables y evitar futuros problemas de licenciamiento;

Si se subcontrata el desarrollo de aplicaciones, la Universidad debe obtener la garantía de que el proveedor cumple con las reglas de desarrollo seguro establecidas.

6.2. REQUISITOS DE SEGURIDAD Y PRIVACIDAD DE LAS APLICACIONES

Se debe identificar y especificar los requisitos de seguridad y privacidad de las aplicaciones, los cuales se determinan generalmente a través de una evaluación de riesgos.
Los requisitos de seguridad y privacidad de las aplicaciones pueden abarcar una amplia gama de temas, en función del propósito de la aplicación. Ver GUÍA DE CONDICIONES MÍNIMAS TÉCNICAS Y DE SEGURIDAD DIGITAL

Los requisitos de seguridad y privacidad de las aplicaciones deben incluir, según corresponda:

a) nivel de confianza en la identidad de las entidades

b) identificar el tipo de información y el nivel de clasificación que debería procesar la solicitud;

c) necesidad de segregación de acceso y nivel de acceso a los datos y funciones de la aplicación;

d) protección frente a ataques malintencionados o interrupciones no intencionadas;

e) requisitos legales, estatutarios y reglamentarios en la jurisdicción donde se

genera, procesa o almacena la transacción;

f) necesidad de privacidad asociada a todas las partes implicadas;

g) los requisitos de protección de cualquier información confidencial;

h) protección de datos mientras se procesan, transfieren y almacenan;

i) necesidad de cifrar de forma segura las comunicaciones entre todas las partes implicadas;

j) controles de entrada, incluidas las comprobaciones de integridad y la validación de entrada;

k) controles automatizados;

l) controles de salida, considerando también quién puede acceder a los resultados y su autorización;

m) restricciones en torno al contenido de campos de texto libre ya que pueden conducir a un almacenamiento incontrolado de datos confidenciales;

n) requisitos exigidos por otros controles de seguridad y privacidad como las interfaces para el registro y el monitoreo o sistemas de detección de fugas de datos;

o) manejo de mensajes de error.

6.2.1 Servicios transaccionales

Adicionalmente, para las aplicaciones que ofrecen servicios transaccionales entre la institución y un tercero, se debe considerar lo siguiente al identificar los requisitos de seguridad y privacidad de la información:

a) el nivel de confianza que cada parte requiere en la identidad declarada de la otra;

b) el nivel de confianza requerido en la integridad de la información intercambiada o procesada y los mecanismos para identificar la falta de

integridad;

c) los procesos de autorización asociados a quién puede aprobar el contenido de los documentos transaccionales clave, emitirlos o firmarlos;

d) la confidencialidad, la integridad, la prueba de envío y de recepción de los documentos clave y el no repudio;

e) la confidencialidad e integridad de cualquier transacción;

f) requisitos sobre la duración de la confidencialidad de una transacción;

g) seguros y otros requisitos contractuales.

6.2.2 Aplicaciones de pagos electrónicos

Para el caso de las aplicaciones que implican pagos electrónicos, se debe tener en cuenta lo siguiente:

a) los requisitos para mantener la confidencialidad e integridad de la información de los pagos electrónicos;

b) el grado de verificación apropiado para comprobar la información de pago suministrada por un tercero;

c) evitar la pérdida o duplicación de la información de las transacciones;

d) cuando se utilice una autoridad de confianza (por ejemplo, para la emisión y el mantenimiento de firmas digitales o certificados digitales), la seguridad y privacidad esté integrada e incorporada en todo el proceso de gestión de certificados o firmas de extremo a extremo.

6.3 ARQUITECTURA DE SISTEMAS SEGUROS Y PRINCIPIOS DE INGENIERÍA

6.3.1 Arquitectura de sistemas seguros

Los principios de ingeniería de seguridad y privacidad deberían establecerse, documentarse y aplicarse a las actividades de ingeniería de los sistemas de información para todas las capas de la arquitectura (negocio, datos, aplicaciones y tecnología).

Los principios de ingeniería de seguridad y privacidad proporcionan guía sobre las técnicas de autenticación de usuarios, el control de sesiones seguras y la validación y saneamiento de datos y deben incluir el análisis de:

a) la variedad de controles de seguridad y privacidad necesarios para proteger la información y los sistemas contra las amenazas identificadas;

b) las capacidades de los controles de seguridad y privacidad para prevenir, detectar o responder a eventos de seguridad y/o privacidad;

c) los controles de seguridad y privacidad específicos que requieren determinados procesos de la Institución como el cifrado de información sensible, la comprobación de la integridad y la firma digital de la información, ver AP-TIC-DR-03 DIRECTRICES PARA LA CRIPTOGRAFIA Y GESTIÓN DE CLAVES;

d) la aplicación de controles de seguridad y privacidad, mediante la integración con una arquitectura de seguridad y la infraestructura técnica;

6.3.2 Principios de ingeniería

Los principios de ingeniería de seguridad deben tener en cuenta:

a) la necesidad de integrarse con una arquitectura de seguridad;

b) infraestructura técnica de seguridad;

c) capacidad de la Institución para desarrollar y apoyar la tecnología elegida;

d) el costo, el tiempo y la complejidad de cumplir con los requisitos de seguridad y privacidad;

e) las buenas prácticas actuales.

La ingeniería de sistemas seguros debería incluir:

a) el uso de principios de arquitectura de seguridad, como:

a. Seguridad por diseño: la seguridad debe ser considerada durante todo el ciclo de vida del desarrollo del producto, desde las etapas iniciales de planificación y diseño hasta las pruebas y la implementación.

b. Seguridad por defecto: se refiere a que los productos se configuran para tener una alta seguridad cuando salen de fábrica. Para lograr la seguridad por diseño y por defecto se debe tener un equilibrio entre seguridad y funcionalidad.

c. Seguridad en el despliegue: es el concepto de implementar mecanismos en la construcción de la seguridad para ayudarla a permanecer funcional (o resistente) a los ataques.

d. Mínimo privilegio: los derechos de acceso deben concederse solo a las personas que los necesiten, estén autorizadas, puedan justificar su acceso y solo durante el tiempo necesario.

e. Denegar por defecto: todo lo que no está expresamente permitido, está prohibido

f. Defensa en profundidad: es una estrategia de ciberseguridad que utiliza múltiples productos y prácticas de seguridad para proteger la red, las propiedades web y los recursos de una organización. Conocida también con el término "seguridad en capas".

g. falla segura: es asegurar que frente a cualquier fallo que aparezca, el sistema siempre pasará a un estado seguro, afectando normalmente a la disponibilidad pero nunca y, en ningún caso, afectando a la seguridad.

h. desconfianza en la entrada de aplicaciones externas

i. Mínima funcionalidad: proporcionar la mínima funcionalidad con la máxima calidad, esto no implica necesariamente una pobre funcionalidad, sino que implica lo suficiente como para conseguir que el trabajo se realice.

j. Usabilidad y manejabilidad: es la manera con que las personas interactúan de forma fácil, eficaz e intuitiva con una herramienta o sistema con el fin de alcanzar un objetivo concreto.

k. Asumir el incumplimiento: asumir responsabilidades sobre los posibles fallos que un mal funcionamiento de su producto pudiese provocar

b) una revisión del diseño centrada en la seguridad y privacidad para ayudar a identificar las vulnerabilidades de la seguridad y privacidad de la información, asegurando que se especifican los controles de seguridad y privacidad y cumplir con los requisitos de seguridad y privacidad;

c) la documentación y el reconocimiento formal de los controles de seguridad y privacidad que no cumplen plenamente los requisitos;

d) fortalecimiento de los sistemas.

La Universidad debe considerar los principios de "confianza cero", tales como:

a) asumir que los sistemas de información ya han sido vulnerados y, por tanto, no depender únicamente de la seguridad del perímetro de la red;

b) emplear un enfoque de "nunca confiar y siempre verificar" para el acceso a los sistemas de información;

c) asegurar que las solicitudes a los sistemas de información estén cifradas de principio a fin;

d) verificar cada solicitud a un sistema de información como si se originara en una red abierta y externa, incluso si estas solicitudes se originan dentro de la Institución;

e) utilizar técnicas de control de acceso dinámico y de "mínimo privilegio",

esto incluye la autenticación y autorización de las solicitudes de información a los sistemas de información;

f) autenticar siempre a los solicitantes y validar siempre las solicitudes de autorización a los sistemas de información sobre la base de información;

Se deben aplicar los principios de ingeniería de seguridad establecidos por la Universidad al desarrollo tercerizado de sistemas de información a través de los contratos y otros acuerdos entre la Universidad y el proveedor.

Los principios de ingeniería de seguridad y los procedimientos de ingeniería establecidos deben revisarse periódicamente para asegurar que contribuyen efectivamente a mejorar los estándares de seguridad y privacidad dentro del proceso de ingeniería. Ver AP-TIC-PR-12 DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS INFORMACIÓN.

6.4. CODIFICACIÓN SEGURA

La Universidad debe establecer procesos para proporcionar un buen gobierno para la codificación segura, al igual que supervisar las amenazas del mundo real y los consejos e información actualizados sobre las vulnerabilidades del software, para guiar los principios de codificación segura a través de la mejora y el aprendizaje continuos. Ver ES-GSPI-DA-03 GUIA FUENTES DE INFORMACIÓN DE AMENAZAS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, ES-GSPI-DA-01 GUIA DE INTELIGENCIA DE AMENAZAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

6.4.1 Planificación antes de la codificación

Los principios de codificación segura deben utilizarse tanto en los nuevos desarrollos como en los escenarios de reutilización, los cuales deben incluir:

a) las expectativas específicas de la Universidad y los principios aprobados para la codificación segura que se utilizarán tanto para los desarrollos de código internos como para los subcontratados;

b) prácticas de codificación comunes e históricas y defectos que conducen a vulnerabilidades de seguridad y privacidad de la información;

c) configurar las herramientas de desarrollo, como los entornos de desarrollo integrados (IDE), para ayudar a imponer la creación de código seguro;

d) seguir las directrices emitidas por los proveedores de herramientas de desarrollo y entornos de ejecución, según proceda;

e) mantenimiento y uso de herramientas de desarrollo actualizadas;

f) calificación de los desarrolladores en la escritura de código seguro;

g) diseño y arquitectura seguros, incluida la modelización de amenazas;

h) normas de codificación segura y, en su caso obligatoriedad de su uso;

i) uso de entornos controlados para el desarrollo.

6.4.2 Durante la codificación

Las consideraciones durante la codificación deben incluir:

a) prácticas de codificación segura específicas de los lenguajes y técnicas de programación que se utilicen, ver GUÍA DE BUENAS PRÁCTICAS EN BASE DE DATOS;

b) utilizar técnicas de programación estructurada;

c) documentar el código y eliminar los defectos de programación, que pueden permitir la explotación de las vulnerabilidades de la seguridad y privacidad de la información;

d) para el código seguro, los desarrolladores no deben compartir información institucional en herramientas de desarrollo que utilicen inteligencia artificial (IA) dado que la información puede quedar pública en la web.

e) prohibir el uso de técnicas de diseño inseguras como el uso de contraseñas codificadas, muestras de código no aprobadas y servicios web no autenticados.

Las pruebas deben realizarse durante y después del desarrollo. Los procesos de pruebas estáticas de seguridad de las aplicaciones pueden identificar vulnerabilidades de seguridad y privacidad en el software.

6.4.3. Revisión y Mantenimiento

Una vez que el código se ha hecho operativo:

a) las actualizaciones deben ser empaquetadas y desplegadas de forma segura;

b) se deben tratar los errores, las sospechas de ataques y las vulnerabilidades de seguridad y privacidad de la información notificadas;

c) el código fuente debe estar protegido contra el acceso no autorizado y la manipulación

Si se utilizan herramientas y bibliotecas externas, la Universidad debe considerar:

a) asegurarse de que las bibliotecas externas se gestionan mediante el mantenimiento de un inventario de las bibliotecas utilizadas y sus versiones y que se actualicen regularmente con los ciclos de lanzamiento;

b) la selección, la autorización y la reutilización de componentes bien examinados, en particular los componentes de autenticación y cifrado;

c) la licencia, la seguridad y el historial de los componentes externos;

d) la garantía de que el software es mantenible, tiene un seguimiento y procede de fuentes acreditadas y de confianza;

e) la disponibilidad a largo plazo de los recursos y artefactos de desarrollo.

Cuando sea necesario modificar un paquete de software, debe tenerse en cuenta los siguientes puntos:

a) el riesgo de que los controles incorporados y los procesos de integridad se vean comprometidos;

b) la posibilidad de obtener el consentimiento del proveedor;

c) la posibilidad de obtener los cambios necesarios del proveedor como actualizaciones estándar del programa;

d) el impacto si la Universidad se hace responsable del futuro mantenimiento del software como resultado de los cambios;

e) la compatibilidad con otros programas informáticos en uso.

6.5. PRUEBAS DE SEGURIDAD Y PRIVACIDAD EN EL DESARROLLO Y LA ACEPTACIÓN

Los nuevos sistemas de información, las actualizaciones y las nuevas versiones deben probarse y verificarse durante los procesos de desarrollo. Las pruebas de seguridad y privacidad deben ser una parte integral de las pruebas de los sistemas o componentes y deben incluir pruebas de:

a) funciones de seguridad y privacidad como autenticación de usuarios, restricción de acceso y uso de cifrado;

b) codificación segura;

c) configuraciones seguras, incluidas las de los sistemas operativos, los cortafuegos y otros componentes de seguridad y privacidad.

Los planes de pruebas deben determinarse mediante un conjunto de criterios. El alcance de las pruebas debe ser proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio introducido. Ver AP-TIC-FO-15 REPORTE DE PRUEBA

La Universidad puede aprovechar las herramientas automatizadas, por ejemplo, las herramientas de análisis de código y/o los escáneres de vulnerabilidad y debe verificar la corrección de los defectos relacionados con la seguridad y privacidad.

En el caso de los desarrollos internos, estas pruebas deben ser realizadas inicialmente por el equipo de desarrollo. A continuación, deben realizarse pruebas

de aceptación independientes para asegurar que el sistema funciona como se espera y debe tenerse en cuenta:

a) la realización de actividades de revisión del código como elemento relevante para la comprobación de las fallas de seguridad y privacidad, incluidas las entradas y condiciones no previstas;

b) la realización de escaneos de vulnerabilidad para identificar configuraciones inseguras y vulnerabilidades del sistema;

c) la realización de pruebas de penetración para identificar el código y el diseño inseguro.

En el caso de los desarrollos tercerizados, se deben tener en cuenta los requisitos de seguridad, privacidad, los productos y servicios deben ser evaluados antes de su adquisición.

Las pruebas deben realizarse en un entorno de pruebas que se ajuste lo más posible al entorno de producción objetivo para asegurar que el sistema no introduce vulnerabilidades en el entorno de la Universidad y que las pruebas son fiables.

6.6. DESARROLLO TERCERIZADO

En los casos en que el desarrollo del sistema se subcontrata, la Universidad debe comunicar y acordar los requisitos y expectativas, monitorear y revisar continuamente si la entrega del trabajo subcontratado cumple con el procedimiento. Ver AP-TIC-PR-12 DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS INFORMACIÓN

Los siguientes puntos deben considerarse en toda la cadena de suministro externa de la Institución:

a) acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado

b) requisitos contractuales para las prácticas de diseño, codificación y pruebas seguras

c) suministro del modelo de amenaza a considerar por desarrolladores externos;

d) pruebas de aceptación de la calidad y exactitud de los resultados

e) suministro de pruebas de que se han establecido niveles mínimos aceptables de seguridad y privacidad;

f) evidencia de que se han realizado pruebas suficientes para evitar la presencia de contenidos maliciosos (tanto intencionados como no intencionados) en el momento de la entrega;

g) acuerdos de custodia del código fuente del software;

h) derecho contractual a auditar los procesos y controles de desarrollo;

i) requisitos de seguridad y privacidad para el entorno de desarrollo;

j) tomar en consideración la legislación aplicable (como es el caso de la protección de datos personales).

6.7. SEPARACIÓN DE LOS ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN

Debe identificarse y aplicarse el nivel de separación entre los entornos de producción, prueba y desarrollo que es necesario para evitar problemas de producción teniendo en cuenta los siguientes factores:

a) separar adecuadamente los sistemas de desarrollo y producción y hacerlos funcionar en dominios diferentes (por ejemplo, en entornos virtuales o físicos separados);

b) definir, documentar y aplicar normas y autorizaciones para el despliegue de software desde el estado de desarrollo al de producción;

c) probar los cambios en los sistemas y aplicaciones de producción en un entorno de prueba antes de aplicarlos a los sistemas de producción;

d) que no se realicen pruebas en entornos de producción, salvo en circunstancias definidas y aprobadas;

e) que los compiladores, editores y otras herramientas de desarrollo o programas de utilidad no sean accesibles desde los sistemas de producción cuando no sean necesarios;

f) mostrar etiquetas de identificación del entorno adecuadas en los menús para reducir el riesgo de error;

g) no copiar información sensible en los entornos de los sistemas de desarrollo y de prueba, a menos que se proporcionen controles equivalentes para los sistemas..

En todos los casos, los entornos de desarrollo y prueba deben estar protegidos tomando en consideración:

a) la aplicación de parches y la actualización de todas las herramientas de desarrollo, integración y prueba (incluidos constructores, integradores, compiladores, sistemas de configuración y bibliotecas);

b) configuración segura de los sistemas y programas informáticos;

c) control de acceso a los entornos;

d) monitoreo de los cambios en el ambiente y en el código almacenado en el mismo;

e) supervisión segura de los entornos;

f) realización de copias de seguridad de los entornos.

6.8. GESTIÓN DEL CAMBIO

La introducción de nuevos sistemas y de cambios importantes en los sistemas existentes debe seguir unas normas acordadas y un proceso formal de documentación, especificación, pruebas, control de calidad y aplicación gestionada. Debe establecerse responsabilidades y procedimientos de gestión para asegurar un control satisfactorio de todos los cambios. AP-TIC-PR-03 DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS INFORMACIÓN.

Los procedimientos de control de cambios deben documentarse y aplicarse para asegurar la confidencialidad, la integridad y la disponibilidad de la información en las instalaciones de procesamiento de la información y en los sistemas de información, para todo el ciclo de vida de desarrollo del sistema, desde las primeras etapas de diseño hasta todos los mantenimientos posteriores.

Siempre que sea posible, los procedimientos de control de cambios para la infraestructura y el software de las TIC deben estar integrados e incluir:

a) planificar y evaluar el impacto potencial de los cambios tomando en consideración todas las dependencias;

b) autorización de cambios;

c) comunicar los cambios a las partes interesadas pertinentes;

d) pruebas y aceptación de pruebas para los cambios;

e) aplicación de los cambios, incluidos los planes de despliegue;

f) consideraciones de emergencia y contingencia, incluidos los procedimientos de repliegue;

g) mantenimiento de registros de los cambios que incluyan todo lo anterior;

h) asegurar que la documentación de funcionamiento y los procedimientos de los usuarios se modifiquen según sea necesario para que sigan siendo adecuados;

i) asegurar que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación se modifiquen según sea necesario para seguir siendo adecuados.

6.9. INFORMACIÓN DE LA PRUEBA

La información de las pruebas permite asegurar la fiabilidad de los resultados de las mismas y la confidencialidad de la información operativa pertinente. La información sensible (incluida la información de identificación personal) no debe copiarse en los entornos de desarrollo y pruebas.

Las siguientes directrices deben aplicarse para proteger las copias de la información operativa, cuando se utilicen con fines de prueba, tanto si el entorno de prueba se construye internamente como en un servicio en la nube:

a) aplicar a los entornos de prueba los mismos procedimientos de control de acceso que se aplican a los entornos operativos;

b) tener una autorización independiente cada vez que se copie información operativa en un entorno de pruebas;

c) proteger la información sensible mediante su eliminación o enmascaramiento;

La información de las pruebas debe almacenarse de forma segura (para evitar su manipulación, que puede dar lugar a resultados no válidos) y utilizarse únicamente con fines de prueba.

7. RESPONSABILIDADES Y AUTORIDADES

Los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros deben cumplir con la política y directrices de seguridad y privacidad de la información definidas por la Universidad Surcolombiana; así mismo, deben reportar a los propietarios de la información y otros activos asociados las violaciones a la política, directrices y/o cualquier inconsistencia o irregularidad que pueda ser generada por los usuarios.

Los líderes de procesos y propietarios de la información y otros activos de la información deben revisar periódicamente los riesgos que se identifiquen sobre el uso inadecuado de los activos.

8. DOCUMENTOS RELACIONADOS Y REGISTROS

- Estatuto de contratación
- AP-TIC-FO-15 REPORTE DE PRUEBA
- AP-TIC-PR-12 DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS INFORMACIÓN
- ES-GSPI-FO-06 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS
- GUIA DE CONDICIONES MÍNIMAS TÉCNICAS Y DE SEGURIDAD DIGITAL
- GUIA EN BUENAS PRÁCTICAS EN BASE DE DATOS
- ES-GSPI-DA-03 GUIA FUENTES DE INFORMACIÓN DE AMENAZAS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- ES-GSPI-DA-04 GUIA DE INTELIGENCIA DE AMENAZAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIO		
VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCION DE CAMBIO
01	EV-CAL-FO-17 11 de septiembre del 2026	Creación documento

ELABORÓ	REVISÓ	APROBÓ
MARTHA LILIANA HERMOSA TRUJILLO Gestión Seguridad y Privacidad de la Información **Elaboró** DIEGO ANDRES CARVAJAL RUIZ Director Centro de Tecnología Información y Control Documental **Aprobó**	ALVARO TORRENTE LÓPEZ Profesional de apoyo SGC	MAYRA ALEJANDRA BERMEO Coordinador SGC