# POLÍTICA DE DESARROLLO SEGURO

| | |
|---|---|
| **Referencia documental** | SGSI-A.8.25-DOC-03 |
| **Versión** | 07 |
| **Publicado** | 31 de julio de 2023 |
| **Última revisión** | 05 de marzo de 2025 |
| **Clasificación** | Confidencial |

# POLÍTICA DE DESARROLLO SEGURO

## Control de cambios

| Versión | Fecha | Revisó | Cambios |
|---|---|---|---|
| 01 | 31/07/2023 | Jorge José Jiménez del Cueto | Nuevo |
| 02 | 14/09/2023 | Jorge José Jiménez del Cueto | Actualización del método de firmado |
| 02 | 11/10/2023 | Jorge José Jiménez del Cueto | Se corrige la ortografía |
| 03 | 24/10/2023 | Jorge José Jiménez del Cueto | Se actualiza del control A.8.29 en Plan de Pruebas el inciso a), En la ruta UTIC-SSI "Actualizar Documentación" de GitLab se encuentran detalladas las actividades y pruebas de desarrollo. |
| 04 | 10/06/2024 | Jorge José Jiménez del Cueto | Se agrega referencia del Manual de desarrollo de sistemas en el punto A.8.25 Ciclo de vida de desarrollo seguro.<br>Cambia la codificación del nombrado de archivos.<br>Actualización del formato.<br>Se agrega referencia del Estándar de codificación en el punto A8.25 y A.8.28.<br>Revisión del documento. |
| 05 | 16/07/2024 | Jorge José Jiménez del Cueto | Se agrega la sección alcance. |
| 06 | 21/10/2024 | Jorge José Jiménez del Cueto | Se actualiza formato con la imagen gubernamental de la nueva administración. |
| 07 | 05/03/2025 | Jorge José Jiménez del Cueto | Se actualiza el formato con la imagen institucional y el nombre de la nueva dependencia. |

# POLÍTICA DE DESARROLLO SEGURO

## Distribución

| Nombre | Área / Rol / Departamento |
|---|---|
| Todo el personal. | DGTIC de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco |

## Tabla de autorizaciones

| Elaboró | Revisó | Autorizó |
|---|---|---|
| **[Firma Digital]**<br>Maribel López Almeida<br>**Operador del SGSI** | **[Firma Digital]**<br>Jorge José<br>Jiménez del Cueto<br>**Responsable del SGSI** | **[Firma Digital]**<br>Edmundo<br>Rosique Valenzuela<br>**Representante de la alta dirección** |

# POLÍTICA DE DESARROLLO SEGURO

## Índice

# POLÍTICA DE DESARROLLO SEGURO

## Introducción

El desarrollo seguro se ha convertido en un aspecto crucial para la seguridad de la información en la actualidad. La creciente dependencia de las organizaciones en la tecnología y el manejo constante de datos confidenciales ha aumentado la exposición a amenazas y vulnerabilidades cibernéticas. Por lo tanto, garantizar que los procesos de desarrollo de sistemas y aplicaciones se realicen de manera segura y protegida es esencial para proteger la integridad, confidencialidad y disponibilidad de la información de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco.

## Objetivo

Establecer un marco integral que asegure la incorporación de prácticas seguras en todas las etapas del ciclo de vida del desarrollo de sistemas y aplicaciones. Mediante la aplicación de este enfoque, la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco logra la mitigación de riesgos en los desarrollos, proteger la información de los usuarios, asegurar la continuidad del negocio, mejorar el cumplimiento normativo y elevar el nivel de seguridad de la información.

## Alcance

Esta política aplica a todos los empleados, contratistas, consultores, y cualquier otra persona involucrada en el desarrollo de software y sistemas de información de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco. Incluye todas las fases del ciclo de vida del desarrollo de software, desde la planificación y diseño hasta la implementación, pruebas, despliegue y mantenimiento.

## A.8.25 Ciclo de vida de desarrollo seguro

Se debe garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo seguro del software y los sistemas.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo | Confidencialidad<br>Integridad<br>Disponibilidad | Proteger | Seguridad de aplicaciones<br>Seguridad de sistemas y redes | Protección |

a) La presente política deberá ser difundida a las partes interesadas de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco mediante correo electrónico, gestor documental y portal interno.
b) Esta política debe revisarse por lo menos una vez al año.
c) Debe contarse con una separación de entornos Productivos y No Productivos, (Desarrollo, Preproducción, Sandbox y Producción).
d) Debe guiarse la seguridad en el ciclo de vida del desarrollo de software acorde a:
    i. Principios de arquitectura e ingeniería en sistemas seguros,
    ii. De acuerdo al documento SGSI-A.8.28-DOC-16 Estándar de codificación.
    iii. De acuerdo al documento SGSI-A.8.25-DOC-04 Manual de desarrollo de sistemas.
e) Debe contar con requisitos de seguridad desde la fase de especificación y diseño del proyecto.
f) Debe contar con pruebas de seguridad para el desarrollo y aceptación cada tres meses.
g) Debe gestionarse la configuración y acceso al código fuente del desarrollo conforme a la política de desarrollo seguro.
h) Debe gestionarse el cambio para seguridad en el control de versiones y licencias en los ambientes mediante el controlador de versiones de GitLab.
i) Debe contar con desarrolladores consientes de la importancia de la codificación segura.

## A.8.26 Requisitos de seguridad de las aplicaciones

Garantizar que todos los requisitos de seguridad de la información se identifiquen y aborden al desarrollar o adquirir aplicaciones.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo | Confidencialidad<br>Integridad<br>Disponibilidad | Proteger | Seguridad de aplicaciones<br>Seguridad de sistemas y redes | Protección<br>Defensa |

## General

Los requisitos de seguridad de las aplicaciones deben incluir (según aplique):
a) Debe asegurar el nivel de confianza en la identidad de las entidades mediante autenticación conforme a la política de control de accesos establecida.
b) Debe identificarse el tipo de información y el nivel de clasificación que procesan las solicitudes generadas por sistemas, bases de datos o servicios web.
c) Debe segregarse el acceso y nivel de acceso a los datos y funciones de las aplicaciones.

d) Debe contar con protección frente a ataques malintencionados o interrupciones involuntarias (por ejemplo: desbordamiento de búfer o inyecciones código/SQL, XSS, etc.).
e) Debe cumplir con los requisitos legales y regulatorios en la jurisdicción donde se genera, procesa, completa o almacena la transacción conforme al control ***5.31 requisitos legales***.
f) Debe considerar la necesidad de privacidad de datos personales asociada con todas las partes implicadas.
g) Debe proteger cualquier información confidencial o reservada.
h) Debe proteger los datos durante el tratamiento, en tránsito y en reposo.
i) Debe cifrar de forma segura las comunicaciones confidenciales o reservadas entre todas las partes implicadas.
j) Debe considerar validación de entradas y comprobaciones de integridad mediante pruebas de seguridad.
k) Debe considerar controles automatizados (por ejemplo: límites de aprobación o aprobaciones dobles).
l) Debe controlar quién puede acceder a las salidas y su autorización.
m) Debe restringir el contenido de los campos de "texto libre" para evitar el almacenamiento incontrolado de datos, por ejemplo, en cuadros de texto de “comentarios”.
n) Debe considerar los requisitos derivados del proceso organizacional, como el registro y la supervisión de transacciones y los requisitos de no repudio.
o) Debe considerar los requisitos exigidos por otros controles de seguridad (por ejemplo, interfaces para sistemas de registro y supervisión o detección de fugas de datos).
p) Debe considerar el manejo de mensajes de error y excepciones.

## Servicios transaccionales

Para las aplicaciones que ofrecen servicios transaccionales entre la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco y un socio, los requisitos de seguridad de la información deben incluir (según aplique):

a) Debe considerar el nivel de confianza que cada parte requiere en la identidad reclamada del otro.
b) Debe considerar el nivel de confianza requerido en la integridad de la información intercambiada o tratada y los mecanismos para identificar la falta de integridad (por ejemplo: la comprobación de redundancia, hashing, firmas digitales).
c) Debe considerar los procesos de autorización asociados con quién puede aprobar el contenido, emitir o firmar documentos transaccionales clave.
d) Debe considerar la confidencialidad, integridad, prueba de envío y recepción de documentos clave y el no repudio (por ejemplo: contratos asociados con licitación y procesos de contrato).

e) Debe considerar la confidencialidad e integridad de cualquier transacción (por ejemplo: órdenes o pedidos, detalles de la dirección de entrega y recibos de confirmación).
f) Debe considerar los requisitos sobre cuánto tiempo se mantendrá la confidencialidad de una transacción.
g) Debe considerar seguros y otros requisitos contractuales.

### Solicitudes electrónicas de pedidos y pagos

Para las solicitudes que involucran pedidos y pagos electrónicos, se debe considerar lo siguiente:
a) Debe mantener la confidencialidad e integridad de la información de las órdenes.
b) Debe considerar el grado de verificación adecuado para verificar la información de pago facilitada por un cliente.
c) Debe evitar la pérdida o duplicación de la información de las transacciones.
d) Debe almacenar los detalles de la transacción fuera de cualquier entorno de acceso público (por ejemplo: en una plataforma de almacenamiento existente en la intranet de la Secretaría y no conservada ni expuesta en medios de almacenamiento electrónico directamente accesibles desde Internet).
e) Debe considerarse donde sea usada una autoridad de confianza (por ejemplo: con el fin de emitir y mantener firmas o certificados digitales) que la seguridad es integrada e incorporada a lo largo de todo el certificado de extremo a extremo o del proceso de gestión de firmas.

## A.8.27 Arquitectura de sistemas seguros y principios de ingeniería

Garantizar que los sistemas de información se diseñen, implementen y operen de forma segura dentro del ciclo de vida del desarrollo.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo | Confidencialidad<br>Integridad<br>Disponibilidad | Proteger | Seguridad de aplicaciones<br>Seguridad de sistemas y redes | Protección |

Los principios de ingeniería de sistemas seguros deben incluir el análisis de:
a) El rango total de controles de seguridad necesarios para proteger la información y los sistemas contra las amenazas identificadas.
b) Las capacidades de los controles de seguridad para prevenir, detectar o responder ante eventos de seguridad.

c) Los controles de seguridad específicos requeridos por determinados procesos empresariales (por ejemplo: cifrado de información sensible, comprobación de integridad y firma digital de información).
d) Dónde y cómo deberían aplicarse los controles de seguridad (por ejemplo: integrándose con una arquitectura de seguridad y la infraestructura técnica).
e) Cómo los controles de seguridad individuales (manuales y automatizados) trabajan juntos para producir un conjunto integrado de controles.

Los principios de ingeniería de seguridad deben tener en cuenta que:
a) Debe integrarse con una arquitectura de seguridad.
b) Debe considerar la capacidad de la Secretaría para desarrollar y soportar la tecnología elegida.
c) Debe considerar el costo, tiempo y complejidad del cumplimiento de los requisitos de seguridad.
d) Debe considerar las buenas prácticas actuales.

La ingeniería de sistemas seguros debe involucrar:
a) Usar los principios de arquitectura de seguridad, como "seguridad por diseño", "defensa en profundidad", "seguridad por defecto", "denegación por defecto", "fallo seguro", "desconfianza de entradas de aplicaciones externas", "seguridad en el despliegue", "asumir brechas", "privilegios mínimos", "usabilidad y manejabilidad" y "funcionalidad mínima".
b) Revisar el diseño orientado a la seguridad para identificar las vulnerabilidades de seguridad de la información, especificar los controles de seguridad y cumplir los requisitos de seguridad.
c) Documentar y reconocer formalmente los controles de seguridad que no cumplen plenamente los requerimientos (por ejemplo: debido a requerimientos de seguridad predominantes).
d) Reforzar ("hardening") los sistemas.

La Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco debe considerar los principios de "cero confianza" tales como:
a) Asumir que los sistemas de información de la Secretaría ya están violados y, por lo tanto, no dependen solo de la seguridad perimetral de la red.
b) Enfocar en "nunca confiar y siempre verificar" el acceso a los sistemas de información.
c) Cifrar de extremo a extremo las solicitudes a los sistemas de información.
d) Verificar cada solicitud a un sistema de información como si se originara en una red abierta y externa, incluso si estas solicitudes se originaron internamente en la Secretaría (es decir, no confiar automáticamente en nada dentro o fuera de sus perímetros).
e) Utilizar técnicas de "privilegios mínimos" y de control dinámico de acceso. Esto incluye autenticar y autorizar solicitudes de información o a sistemas basados en información contextual, como información de autenticación, identidades de usuario, datos sobre el dispositivo final del usuario y clasificación de datos.

f) Autenticar siempre a los solicitantes y validar siempre las solicitudes de autorización a los sistemas de información en función de la información, incluida la información de autenticación y las identidades de usuario, los datos sobre el dispositivo final del usuario y la clasificación de datos (por ejemplo: aplicando una autenticación reforzada o multifactor).

## A.8.28 Codificación segura

Se debe garantizar que el software se escriba de forma segura, reduciendo así el número de posibles vulnerabilidades de seguridad de la información en el software.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo | Confidencialidad<br>Integridad<br>Disponibilidad | Proteger | Seguridad de aplicaciones<br>Seguridad de sistemas y redes | Protección |

Debe guiarse la codificación segura, acorde al documento SGSI-A.8.28-DOC-16 Estándar de codificación.

## Planificación y previo a la codificación

a) Se deben incluir las expectativas específicas de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco y los principios aprobados para la codificación segura que se utilizarán tanto para los desarrollos de código internos como para los subcontratados.
b) Se deben incluir las prácticas y defectos de codificación comunes e históricos que conducen a vulnerabilidades de seguridad de la información.
c) Se deben configurar herramientas de desarrollo, como los entornos de desarrollo integrado (IDE), para ayudar a reforzar el desarrollo de código seguro.
d) Se deben seguir las indicaciones emitidas por los proveedores de las herramientas de desarrollo y entornos de ejecución, según aplique.
e) Se debe considerar el mantenimiento y uso de herramientas de desarrollo actualizadas (por ejemplo: compiladores).
f) Se debe considerar la cualificación de los desarrolladores en el desarrollo de código seguro.
g) Se debe considerar el diseño y arquitectura seguros, incluida la modelación de amenazas.
h) Se debe considerar los estándares de codificación segura y donde sea relevante, exigir su uso.
i) Se debe usar entornos controlados para el desarrollo.

## Durante la codificación

a) Deben considerarse las prácticas de codificación seguras específicas de los lenguajes de programación y técnicas en uso.
b) Deben usarse técnicas de programación seguras como la revisión por pares, las iteraciones de seguridad o el desarrollo basado en pruebas.
c) Deben usarse técnicas de programación estructurada.
d) Debe documentarse el código y eliminar los defectos de programación.
e) Debe prohibirse el uso de técnicas de diseño inseguras (por ejemplo: el uso de contraseñas codificadas, ejemplos de código no aprobado y servicios web no autenticados).

Antes de que el software se ponga en producción, se debe considerar:
f) Evaluar la superficie de ataque y el principio de privilegios mínimos.
g) Analizar los errores de programación más comunes y documentar su mitigación.

## Operación, revisión y mantenimiento

a) Las actualizaciones deben empaquetarse y desplegarse de forma segura.
b) Deben atenderse las vulnerabilidades de seguridad de la información notificadas.
c) Deben registrarse los errores y presuntos ataques, y los registros de eventos (logs) deben revisarse periódicamente para realizar ajustes en el código según sea necesario.
d) Debe protegerse el código fuente contra el acceso no autorizado y la manipulación (por ejemplo, mediante el uso de herramientas de gestión de la configuración, que normalmente proporcionan características como el control de acceso y el control de versiones).

Si utilizan herramientas y bibliotecas externas, la Secretaría debe considerar:
e) Garantizar que las bibliotecas externas se gestionen (por ejemplo, manteniendo un inventario de las bibliotecas utilizadas y sus versiones) y se actualicen periódicamente con ciclos de lanzamiento.
f) Seleccionar, autorizar y reutilizar componentes bien examinados, en particular componentes de autenticación y criptográficos.
g) Las licencias, la seguridad y el historial de los componentes externos.
h) Garantizar que el software sea mantenible, rastreado y provenga de fuentes probadas y de buena reputación.
i) Contar con disponibilidad suficiente a largo plazo de recursos y artefactos de desarrollo.
j) Se debe registrar las cuentas de bibliotecas o librerías a nombre de la DGTIC. No se deben utilizar cuentas personales.

Donde sea necesario modificar un paquete de software, debe validarse:

k) Si se debe obtener el consentimiento del fabricante.
l) El riesgo de que los controles integrados y los procesos de integridad se vean comprometidos.
m) La posibilidad de obtener los cambios requeridos del proveedor como actualizaciones estándar del programa.
n) El impacto si la Secretaría se hace responsable del mantenimiento futuro del software como resultado de cambios.
o) La compatibilidad con otro software en uso.

## A.8.29 Pruebas de seguridad en desarrollo y aceptación

Validar si se cumplen los requisitos de seguridad de la información cuando se implementan aplicaciones o código en el entorno de producción.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo | Confidencialidad<br>Integridad<br>Disponibilidad | Identificar | Seguridad de aplicaciones<br>Aseguramiento de seguridad de la información<br>Seguridad de sistemas y redes | Protección |



### Pruebas de seguridad

a) Deben incluirse pruebas de funciones de seguridad como autenticación de usuarios, restricción de acceso y uso de criptografía.
b) Deben incluirse pruebas de codificación segura.
c) Deben incluirse pruebas de configuraciones seguras, incluida la de sistemas operativos, firewall y otros componentes de seguridad.

### Plan de prueba

a) En la ruta UTIC-SSI "Documentación [Nombre del Sistema]/3.Desarrollo/3.4. Pruebas/3.4.1. Plan de pruebas" de GitLab se encuentran detalladas las actividades y pruebas de desarrollo.
b) Se deben incluir los insumos y productos previstos en una serie de condiciones.
c) Se deben incluir los criterios para evaluar los resultados.
d) Se debe incluir la decisión sobre futuras acciones según sea necesario.

### Pruebas de aceptación

a) Debe realizar actividades de revisión de código para comprobar fallos de seguridad, incluyendo las entradas y condiciones imprevistas.
b) Debe realizar análisis de vulnerabilidades para identificar configuraciones inseguras y vulnerabilidades del sistema.
c) Debe realizar pruebas de penetración para identificar código y diseño inseguros.

## A.8.30 Desarrollo externalizado (outsourcing)

Se debe garantizar que las medidas de seguridad de la información requeridas por la Secretaría se implementen en el desarrollo de sistemas subcontratados.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo<br>Detectivo | Confidencialidad<br>Integridad<br>Disponibilidad | Identificar<br>Proteger<br>Detectar | Seguridad de sistemas y redes<br>Seguridad de aplicaciones<br>Seguridad en la relación con proveedores | Gobernabilidad y Ecosistema<br>Protección |

a) Se deben establecer los acuerdos de licencia, la propiedad del código y los derechos de propiedad intelectual relacionados con el contenido subcontratado.
b) Se deben establecer los requisitos contractuales para diseño seguro, codificación segura y pruebas de seguridad.
c) Se debe establecer la provisión del modelo de amenazas a considerar por los desarrolladores externos.
d) Se deben establecer las pruebas de aceptación de la calidad y precisión de los entregables.
e) Se deben aportar pruebas de que se establecen niveles mínimos aceptables de capacidades de seguridad y privacidad (por ejemplo: informes de garantía).
f) Se deben aportar evidencias de que se han aplicado pruebas suficientes para protegerse contra la presencia de contenidos maliciosos (tanto intencionados como no intencionados) hasta el momento de la entrega.
g) Se deben aportar evidencias de que se han aplicado pruebas suficientes para evitar la presencia de vulnerabilidades conocidas.

h) Se deben establecer los acuerdos de custodia para el código fuente del software (por ejemplo: si el proveedor sale del negocio).
i) Se debe establecer el derecho contractual a auditar los procesos y controles de desarrollo.
j) Se deben establecer los requisitos de seguridad para el entorno de desarrollo.
k) Se debe tener en cuenta la legislación aplicable (por ejemplo: protección de datos personales).

## A.8.31 Separación de entornos de desarrollo, prueba, sandbox y producción

Se debe proteger el entorno de producción y los datos del compromiso de las actividades de desarrollo y prueba.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo<br>Detectivo | Confidencialidad<br>Integridad<br>Disponibilidad | Proteger | Seguridad de aplicaciones<br>Seguridad de sistemas y redes | Protección |

a) Se deben separar adecuadamente los sistemas de desarrollo y producción y operarlos en diferentes dominios (por ejemplo, en entornos virtuales o físicos separados).
b) Se deben definir, documentar y aplicar normas y autorización para el despliegue de programas informáticos en los ambientes de Desarrollo, Preproducción, Sandbox hasta Producción;
c) Se deben probar los cambios de sistemas y aplicaciones de producción en un entorno de Preproducción y Sandbox, antes de aplicarlos a los sistemas de Producción.
d) No se debe probar en entornos de Producción, excepto en circunstancias que hayan sido definidas y aprobadas.
e) Los compiladores, editores y otras herramientas o utilerías de desarrollo no deben ser accesibles desde los sistemas de Producción.
f) Se deben mostrar etiquetas de identificación del entorno en los menús para reducir el riesgo de error.
g) No se debe copiar información confidencial o reservada en los entornos de sistemas de Desarrollo, Preproducción y Sandbox.
h) En todos los casos, los entornos de Desarrollo, Preproducción y Sandbox deben protegerse considerando que:
i) Se deben parchar y actualizar todas las herramientas de desarrollo, integración y prueba (incluidos constructores, integradores, compiladores, sistemas de configuración y librerías) en los entornos de Desarrollo, Preproducción y Sandbox.
j) Se debe controlar el acceso a los entornos de Desarrollo, Preproducción y Sandbox.

## A.8.32 Gestión del cambio

Se debe preservar la seguridad de la información al ejecutar cambios.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo | Confidencialidad<br>Integridad<br>Disponibilidad | Proteger | Seguridad de aplicaciones<br>Seguridad de sistemas y redes | Protección |

a) Se debe planificar y evaluar el impacto potencial de los cambios teniendo en cuenta todas las dependencias.
b) Cuando el cambio tenga un impacto importante para el entorno TPAY de la Secretaría, debe utilizarse el formato SGSI-A.8.32-DOC-17 FORMATO PARA SOLICITUD DE CAMBIO.
c) Debe existir una autorización de cambios.
d) Se deben comunicar los cambios a las partes interesadas pertinentes.
e) Deben existir pruebas y aceptación de las pruebas para los cambios.
f) La aplicación de cambios debe incluir los planes de despliegue.
g) Deben existir consideraciones de emergencia y contingencia, incluidos los procedimientos alternativos.
h) Se deben mantener registros de los cambios que incluyan todo lo anterior.
i) Se deben garantizar que la documentación operativa y los procedimientos de los usuarios, se modifiquen según sea necesario para seguir siendo apropiados.
j) Se debe garantizar que los planes de continuidad de las TIC y los procedimientos de respuesta y recuperación se modifiquen según sea necesario para seguir siendo apropiados.

## A.8.33 Información de prueba

Se debe garantizar la relevancia de las pruebas y la protección de la información operativa utilizada para las pruebas.

| Tipo de control | Propiedades de Seguridad de la información | Conceptos de ciberseguridad | Capacidades operativas | Dominios de seguridad |
|---|---|---|---|---|
| Preventivo | Confidencialidad<br>Integridad | Proteger | Protección de la información | Protección |

a) Se deben aplicar a los entornos de Prueba los mismos procedimientos de control de acceso que los aplicados al entorno de Producción.
b) Se debe disponer de una autorización independiente cada vez que se copie la información operativa en un entorno de Prueba.
c) Se deben guardar registros de eventos (logs) de la copia y el uso de la información operativa para proporcionar una pista de auditoría.
d) Se debe proteger la información confidencial o reservada mediante la eliminación o el enmascaramiento si se utiliza para las pruebas.
e) Se debe eliminar apropiadamente la información operativa de un entorno de Prueba inmediatamente después de que se complete la prueba para evitar el uso no autorizado de la información de prueba.
f) La información de prueba debe almacenarse de forma segura (para evitar la manipulación, que de otro modo puede dar lugar a resultados no válidos) y solo debe utilizarse para fines de prueba.

## Cumplimiento y Responsabilidad

Todos los empleados, proveedores y partes interesadas deben cumplir con esta política de desarrollo seguro. La responsabilidad de implementar y hacer cumplir esta política recae en los propietarios de la información, los responsables de seguridad de la información y la dirección de la DGTIC de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco.

## Revisión y Actualización

Esta política será revisada por lo menos una vez al año para garantizar su eficacia y relevancia, y se actualizará según sea necesario para cumplir con los requisitos legales, reglamentarios y contractuales aplicables al desarrollo seguro.