POLÍTICA DE CONTROL DE ACCESOS

Referencia documental	SGSI-A.5.15-DOC-11
Versión	09
Publicado	26 de julio de 2023
Última revisión	05 de marzo de 2025
Clasificación	Confidencial

Copia no controlada

Este documento es propiedad de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

POLÍTICA DE CONTROL DE ACCESOS

Control de cambios

Versión	Fecha	Revisó	Cambios
01	26/07/2023	Jorge José Jiménez del Cueto	Nuevo
02	15/09/2023	Jorge José Jiménez del Cueto	Se actualiza método de firmado
03	16/10/2023	Jorge José Jiménez del Cueto	Se actualiza el punto A8.5 en el inciso h)
04	24/10/2023	Jorge José Jiménez del Cueto	Se modifica el control 5.15 Control de acceso, agregando un nuevo inciso, b) Los accesos lógicos serán provistos acompañados de una carta responsiva "SGSI-DOC-A.5.15-16 Modelo de carta responsiva".
			Se agrega el control A.5.16 Gestión de identidades, con el punto, • Las cuentas que sufran cambios en alcances y/o privilegios, deberán actualizarse en las cartas responsivas asociadas.
			Se agrega el control A.5.18 Derechos de acceso, indicando un punto de quién y cada cuanto hará la revisión, y otro punto indicando por dónde, qué y a quién se enviará lo resultante.
05	31/05/2024	Jorge José Jiménez del Cueto	Cambia la codificación del nombrado de archivos. Actualización del formato. Revisión del documento.
06	16/07/2024	Jorge José Jiménez del Cueto	Se agrega la sección alcance.
07	28/08/2024	Jorge José Jiménez del Cueto	En el A.5.15 Control de acceso, se agrega el control de acceso roles y privilegios.
08	21/10/2024	Jorge José Jiménez del Cueto	Se agregan los procedimientos asociados en los puntos: A.5.16 Gestión de identidades. A.5.18 Derechos de acceso.

Copia no controlada

Este documento es propiedad de la Secretaria de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

			A.8.2 Derechos de accesos privilegiados Se actualiza formato con la imagen gubernamental de la nueva administración.
09	05/03/2025	Jorge José Jiménez del Cueto	Se actualiza el formato con la imagen institucional y el nombre de la nueva dependencia.

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] Maribel López Almeida **Operador del SGSI**	**[Firma Digital]** Jorge José Jiménez del Cueto **Responsable del SGSI**	**[Firma Digital]** Edmundo Rosique Valenzuela **Representante de la alta dirección**

Copia no controlada

Este documento es propiedad de la Secretaria de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

POLÍTICA DE CONTROL DE ACCESOS

Índice

Copia no controlada

Este documento es propiedad de la Secretaria de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

POLÍTICA DE CONTROL DE ACCESOS

Introducción

Estos lineamientos ayudan a establecer una estructura sólida para la gestión y protección de la información de autenticación en un sistema, contribuyendo a la seguridad y privacidad de los usuarios y de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco, así como la implementación de medidas para prevenir el acceso no autorizado, fortaleciendo la seguridad en el entorno digital.

Objetivo

Establecer una estructura sólida para la gestión y protección de accesos en los sistemas, contribuyendo a la seguridad y privacidad de los usuarios y de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco, así como la implementación de medidas para prevenir el acceso no autorizado, fortaleciendo la seguridad en el entorno digital.

Alcance

La Política de Control de Accesos de la organización está diseñada para proteger la confidencialidad, integridad y disponibilidad de la información de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco, mediante el establecimiento de controles adecuados sobre el acceso a los sistemas de información y datos.

A.5.15 Control de acceso

Se debe garantizar el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y control de acceso	Protección

Copia no controlada

Este documento es propiedad de la Secretaria de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

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, circular, portal interno de la DGTIC y gestor documental.

b) Los accesos lógicos serán provistos acompañados de una carta responsiva SGSI-A.5.15-DOC-16 **Modelo de carta responsiva**.

c) Para los controles de control de accesos físicos se deberá consultar el SGSI-A.7-DOC-03 **Manual De Controles Físicos** en el apartado de ***Entrada física.***

d) Para los controles de accesos lógicos se deberá consultar el SGSI-A-5-15-DOC-39 **Control de Acceso Roles y Privilegios.**

e) Esta política debe revisarse por lo menos una vez al año.

A.5.16 Gestión de identidades

Permitir la identificación única de las personas y los sistemas que acceden a la información de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco y otros activos asociados y permitir la asignación adecuada de derechos de acceso.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y control de acceso	Protección

- Las cuentas que sufran cambios en alcances y/o privilegios, deberán actualizarse en las cartas responsivas asociadas.
- Las cuentas que sufran una baja, no requieren actualización en la carta responsiva; solo se deshabilita el usuario en el directorio activo.
- El acceso a la Dirección General de Tecnologías de Información y Comunicaciones; así como al Centro de Datos de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco debe gestionarse de acuerdo a los procedimientos “SGSI-A.5.16-DOC-17 Procedimiento de acceso por biométrico a la DGTIC de la SAF” y “SGSI-A.5.16-DOC-20 Procedimiento de acceso por biométrico al centro de datos de la SAF”.

Copia no Controlada

Este documento es propiedad de la Secretaria de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

A.5.17 Información de autenticación

Garantizar la autenticación adecuada de la entidad y evitar fallos en los procesos de autenticación.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y control de acceso	Protección

Asignación y gestión de información de autenticación

a) Se definirán contraseñas o NIPs generados (si es posible, automáticamente) durante los procesos de alta, deben ser secretos, no adivinables y únicos para cada usuario. Los usuarios deben cambiar estas contraseñas después del primer uso.
b) Se verificará la identidad del usuario antes de proporcionar la información de autenticación, ya sea por sustitución o autenticación temporal para cuenta existente, a través de gestor documental por parte del jefe inmediato y/o asistencia del personal de DGTIC.
c) La información de autenticación, incluyendo la temporal, se transmitirá de forma segura, preferiblemente a través de canales autenticados y protegidos, como correo electrónico, gestor documental, evitando el uso del mismo cuerpo del mensaje para enviar tanto usuario como contraseña.
d) Los usuarios darán acuse de recibo de la información de autenticación para garantizar que la han recibido y están al tanto de las responsabilidades asociadas.
e) Se cambiarán inmediatamente las contraseñas predeterminadas proporcionadas por los fabricantes o proveedores después de la instalación de sistemas o software.
f) Se usarán métodos de almacenamiento de los registros de autenticación de manera segura, garantizando su confidencialidad a través del uso de una bóveda de contraseñas, método aprobado para la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco.

Responsabilidades del usuario

a) Mantendrá con carácter confidencial las contraseñas u otra información secreta de autenticación. La información secreta personal no debe compartirla con nadie, solo se puede compartir, la información de autenticación vinculada a múltiples usuarios o entidades no personales, con personas autorizadas.
b) Cuando se utilicen contraseñas como información de autenticación, definirá contraseñas seguras (hasta donde el sistema lo permita) con:
    i.frases de contraseña,

Copia no controlada

Este documento es propiedad de la Secretaria de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

ii.caracteres en mayúsculas,
iii.caracteres en minúsculas,
iv.caracteres numéricos,
v.caracteres especiales,
vi.longitud mínima de 12 caracteres.

c) Evitará usar palabras obvias relacionadas con su información personal, combinaciones débiles o secuenciales, ni contraseñas anteriormente usadas.
d) No utilizar las mismas contraseñas en diferentes servicios y sistemas.

Sistema de gestión de contraseñas

Si la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco cuenta con el recurso y este lo permite:

a) Los usuarios seleccionarán y cambiarán sus propias contraseñas y contarán con un procedimiento de confirmación para corregir errores de entrada.
b) Cumplirán con las contraseñas seguras de acuerdo con las recomendaciones de buenas prácticas mencionadas en las Responsabilidades del usuario.
c) Cambiarán sus contraseñas en el primer inicio de sesión.
d) Cumplirán los cambios de contraseña según sea necesario, por ejemplo, después de un incidente de seguridad, tras la terminación o cambio de puesto cuando sean los casos compartidos, entre otros casos.
e) Impedirá la reutilización de contraseñas anteriores.
f) Evitará el uso de diccionarios, contraseñas comunes, nombres de usuario comprometidos o combinaciones de contraseñas de sistemas pirateados.
g) No mostrará contraseñas en la pantalla mientras se introducen.
h) Almacenará y transmitirá (en los casos que aplique) las contraseñas de forma protegida para evitar usos no autorizados.

A.5.18 Derechos de acceso

Garantizar que el acceso a la información y otros activos asociados se defina y autorice de acuerdo con los requisitos del negocio.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y control de acceso	Protección

Copia no controlada

Este documento es propiedad de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

a) La revisión de usuarios y privilegios de la DGTIC de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco, la realizará el operador del SGSI por lo menos una vez al año, validando las cartas responsivas contra lo reflejado en el servidor de Directorio Activo.
b) Se enviarán por correo los hallazgos a los jefes de la DGTIC, mostrando con imágenes las evidencias en caso de discrepancias entre las cartas responsivas y el Directorio Activo o en su defecto, sólo será indicado que no existen anomalías o accesos no autorizados.
c) El acceso a internet a través de la red de la Secretaría de Administración y Finanzas será de acuerdo al procedimiento "SGSI-A.5.18-DOC-34 Procedimiento de acceso a internet".
d) La revocación de los accesos se deben realizar de acuerdo a los procedimientos "SGSI-A.5.18-DOC-35 Procedimiento de revocación de acceso a servicios", "SGSI-A.5.18-DOC-37 Procedimiento de revocación de acceso remoto VPN" y "SGSI-A.5.18-DOC-36 Procedimiento de revocación de acceso a internet".

A.8.2 Derechos de accesos privilegiados

Se debe asegurar que solo los usuarios autorizados, los componentes y servicios de software cuenten con derechos de acceso privilegiados.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y control de acceso	Protección

a) Esta política aplica para los siguientes sistemas: TPAY, base de datos, Firewall, Servidores.
b) En la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco, se deben tener identificados los usuarios con privilegios mediante Matriz de roles, que se maneja en el Directorio Activo para acceso como son VPN y acceso a servidores Windows. Para el caso de servidores Linux y los usuarios de Base de Datos, se debe tener identificados mediante una Matriz de roles por privilegios e inventario de usuarios.
c) La asignación de derechos altamente privilegiados debe tener una vigencia de máximo de 30 días, excepto las cuentas de VPN cuya vigencia es de 6 meses, posterior a ese tiempo, se deberá pedir nuevamente el acceso.
d) Para poder solicitar un acceso altamente privilegiado debe notificarse al jefe inmediato por gestor documental este a su vez solicitarlo al titular de la Dirección General de Tecnologías de la Información y Comunicaciones quien será el único que la autorice.

Copia no controlada

Este documento es propiedad de la Secretaria de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

e) El área de Sistemas e Infraestructura, proporcionará el acceso respondiendo en el mismo asunto del gestor documental desde donde se notificó, mostrando la vigencia de la cuenta.
f) Debe limitarse el uso de cuentas sin personalizar (por ejemplo: root, admin, administrador, etc.) y cuando sea imperante utilizarlas debe notificarse a las siguientes áreas: la Dirección General de Tecnologías de Información y Comunicaciones y sus subdirecciones.
g) Se debe tener un registro de auditoría (logs) de uso de estas cuentas mediante el sistema de almacenamiento autorizado por la DGTIC.
h) Los accesos a los servicios proporcionados por esta dependencia a través de protocolos de comunicación como SSH, SFTP, SCP, JDBC por mencionar algunos se deben realizar de acuerdo al procedimiento "SGSI-A.8.2-DOC-06 Procedimiento de solicitud de acceso a servicios".

A.8.3 Restricción de acceso a la información

Se debe garantizar solo el acceso autorizado y evitar el acceso no autorizado a la información y otros activos asociados.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y control de acceso	Protección

a) Se encuentra prohibido el acceso a los sistemas de forma anónima, por defecto o con intenciones de evadir la identidad del acceso. La única excepción son los medios que cuentan con información clasificada como pública (por ejemplo: la página de internet).
b) Todo sistema de información deberá contar con mecanismos de acceso por usuario, contraseña y de ser posible de forma adicional otros mecanismos de autenticación.
c) Los sistemas (en función de sus posibilidades) deben controlar a qué información puede acceder cada usuario, incluida la actividad a realizar (solo lectura, revisor, ejecutor, etc.).
d) Se debe de tomar en cuenta los niveles de clasificación de información para segregar a los usuarios y restringir accesos como sea necesario.

A.8.4 Acceso al código fuente

Bloquear la introducción de funcionalidades no autorizadas, evitar cambios involuntarios o maliciosos y mantener la confidencialidad de la propiedad intelectual valiosa.

Copia no controlada

Este documento es propiedad de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y control de acceso Seguridad de aplicaciones Configuración segura	Protección

a) Debe estar estrictamente controlado el acceso al código fuente y a los elementos asociados a repositorios de código; GitLab en entornos de preproducción y producción, y a las herramientas de desarrollo IDES Jaspersoft, Visual Studio Code, Android Studio, Net 7, Ionic 6, Angular 17.
b) Principio de necesidad de saber: solo los usuarios autorizados deben tener acceso al código fuente.
c) Principio de mínima autorización: los usuarios solo deben tener acceso al código fuente que necesitan para realizar sus tareas.
d) Principio de separación de funciones: las personas que tienen acceso al código fuente no deben ser las mismas personas que son responsables de su implementación.
e) El acceso directo al código fuente se encuentra estrictamente prohibido a menos que se realice a través de las herramientas GitLab.

A.8.5 Autenticación segura

Se debe garantizar que un usuario o una entidad se autentiquen de forma segura, cuando se concede acceso a sistemas, aplicaciones y servicios.

Tipo de control	Propiedades de Seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Identidad y control de acceso	Protección

a) Cuando un medio o sistema de información haga tratamiento de información clasificada como confidencial o reservada, deberá contar con otros métodos de autenticación, por ejemplo; biometría, OTP, certificados digitales, Token de un solo uso, etc.
b) Cuando se utilicen diferentes mecanismos de autenticación, puede utilizarse las siguientes combinaciones: lo que sabe, lo que tiene y lo que es, de tal forma que al combinarse se convierta en una autenticación segura.

Copia no controlada

Este documento es propiedad de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.

c) Los sistemas de información no deben mostrar indicios de autenticación o información que aluda a revelar usuarios o contraseñas.
d) No se deben mostrar mensajes de ayuda en los sistemas de información, por ejemplo; códigos de error, o que indique que parte de los datos ingresados es correcta o incorrecta.
e) Cuando sea posible, los medios de autenticación deberán contener mecanismos contra ataques de fuerza bruta, por ejemplo: herramientas CAPTCHA.
f) Los sistemas de información no deben mostrar la contraseña cuando es ingresada.
g) Cuando el inicio de sesión tenga que viajar de un servicio a otro, el canal debería estar cifrado, por ejemplo; el uso de HTTPS o SFTP.
h) Para los sistemas críticos deberá existir una vigencia de **sesión máxima de 2 minutos**, posteriormente debe cerrarse la sesión y forzar a iniciar de nuevo por inactividad.

Cumplimiento y Responsabilidad

Todos los empleados, proveedores y partes interesadas deben cumplir con esta política de control de acceso. 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 control de acceso.

Copia no controlada

Este documento es propiedad de la Secretaría de Administración y Finanzas del Gobierno del Estado de Tabasco. Queda estrictamente prohibida su reproducción parcial o total sin autorización por escrito. Cualquier documento impreso que no sea el original o las copias controladas, así como cualquier archivo electrónico que no provenga de las fuentes oficiales y no sea el respaldo original, se considera como COPIA NO CONTROLADA.