



SSC

SECRETARÍA DE SEGURIDAD
CIUDADANA

Políticas de uso del correo electrónico institucional y alternativo de la Secretaría de Seguridad Ciudadana del Estado de Tlaxcala.

Pol-Correo-v1.1-2026-07

CONTENIDO

Marco normativo.....	3
Glosario de términos.....	4
Justificación.....	6
Capítulo 1 Responsabilidades del titular de la cuenta de correo electrónico....	7
Capítulo 2 Administración y control de cuentas de correo electrónico por el Departamento De TIC'S.....	9

MARCO NORMATIVO.

Al utilizar el correo electrónico institucional y alterno de la S.S.C., el personal deberá apegarse estrictamente al marco legal establecido en siguientes artículos; 21, párrafo noveno de la Constitución Política de los Estados Unidos Mexicanos; 40 fracciones II, XX y XXI de la Ley General del Sistema Nacional de Seguridad Pública; 7 y 49 de la Ley General de Responsabilidades Administrativas; 78 de la Constitución Política del Estado Libre y Soberano de Tlaxcala; 4, 19 fracciones VI y VII, y 22 fracción V de la Ley de Seguridad Pública y Ciudadana del Estado de Tlaxcala; 23 fracción XIII, XIV y XV del Reglamento Interior de la Secretaría de Seguridad Ciudadana del Estado de Tlaxcala; 3 fracción X inciso c) y 11 del Código de Conducta de las Personas Servidoras Públicas de la Secretaría de Seguridad Ciudadana del Estado de Tlaxcala; 96 y 100 de la Ley de Protección de Datos Personales en Posesiones de Sujetos Obligados del Estado de Tlaxcala; 57, 79, 80, 113 y 121 de Ley de Transparencia y Acceso a la Información Pública para el Estado de Tlaxcala; 316 del Código Penal para el Estado Libre y Soberano de Tlaxcala; artículos 101, 102 y 104 de la Ley de Archivos del Estado de Tlaxcala; así como el Capítulo IX Del correo electrónico de los Lineamientos en Materia de Tecnologías de Información y Comunicaciones de la SSC del Estado de Tlaxcala Versión 2.0., las cuales son señaladas de manera enunciativa más no limitativa, a fin de que surta los efectos legales correspondientes.

GLOSARIO DE TÉRMINOS

Activos (Bienes Intangibles): Recursos no físicos con valor económico e institucional para la S.S.C., en este caso representados por la cuenta de correo, su contraseña y la información contenida en ella.

Archivos Adjuntos: Documentos o datos que se anexan a un correo electrónico para ser transmitidos junto con el cuerpo del mensaje.

Alta Disponibilidad: Capacidad del servicio de correo electrónico para mantenerse operativo, accesible y en funcionamiento de manera continua y sin interrupciones.

Remitente: Persona que genera y envía el mensaje de correo.

Destinatario: Persona o área que recibe el mensaje de correo.

Encabezado: Sección inicial de un mensaje de correo electrónico compuesta por los campos del destinatario y el asunto (*subject*).

Cuerpo del Mensaje: Sección principal de redacción de un correo electrónico que debe contener el saludo formal, el cargo del destinatario y una exposición concisa y relevante.

Firma Institucional: Bloque estandarizado de datos al final del mensaje que identifica al usuario e incluye: nombre, cargo, área, dependencia y número telefónico.

Depuración de Buzón: Proceso periódico de limpieza y eliminación de correos o archivos obsoletos para liberar espacio en el servidor de correo.

Directorio Oficial de Correos Electrónicos: Registro centralizado y actualizado por el Departamento de TIC'S, con todas las direcciones de correo activas de la S.S.C.

Spam (Correo no deseado): Mensajes no solicitados o clasificados como sospechosos por los filtros de seguridad, generados comúnmente por el uso de palabras sensibles, mayúsculas sostenidas, formatos excesivos o enlaces desconocidos.

Proceso de Entrega-Recepción: Procedimiento administrativo formal mediante el cual un servidor público entrega a su sucesor o superior los activos, información y cuentas bajo su resguardo al concluir su encargo.

Confidencialidad: Principio que garantiza que la información transmitida o almacenada solo sea accesible por las personas o sistemas expresamente autorizados.

Credenciales de Acceso: Conjunto de datos de autenticación (nombre de usuario y contraseña) que permiten el acceso individual a la cuenta de correo.

Correo de Recuperación: Dirección de correo alternativa asignada y controlada de forma exclusiva por el Departamento de TIC'S, para restablecer el acceso a una cuenta en caso de pérdida o bloqueo.

Estructura Orgánica: Esquema administrativo e institucional bajo el cual se crean y asignan los nombres de las cuentas de correo electrónico.

Integridad: Garantía de que la información contenida y enviada por correo electrónico se mantiene completa, exacta y sin alteraciones no autorizadas.

Información Sensible / Reservada: Datos o documentación oficial cuya divulgación no autorizada puede vulnerar la seguridad, la privacidad de terceros o la reputación institucional.

Resguardo de Contraseña: Obligación de proteger la clave de acceso mediante su modificación periódica y la prohibición de compartirla con terceros.

ISO/IEC 27001:2022: Norma internacional que establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

ISO/IEC 27017:2015: Guía de controles de seguridad de la información específica para la prestación y uso de servicios en la nube.

ISO/IEC 27018:2019: Código de práctica para la protección de datos personales e identificación personal (PII) en servicios de computación en la nube pública.

ISO/IEC 27701:2019: Extensión de seguridad para la gestión de la privacidad de la información (PIMS).

ISO/IEC 22301:2019: Norma para la gestión de la continuidad del negocio, garantizando que el servicio continúe operando ante incidentes o emergencias.

ISO/IEC 20000-1:2018: Estándar internacional para la gestión de servicios de tecnologías de la información (TI).

ISO 9001:2015: Norma sobre Sistemas de Gestión de la Calidad que asegura un servicio eficiente y en constante mejora.

CSA STAR CCM v4.0 (Cloud Security Alliance - Cloud Controls Matrix): Marco de controles de seguridad en la nube diseñado para evaluar la seguridad de los proveedores de servicios en la nube.

JUSTIFICACIÓN.

Actualmente, las áreas Staff y las Direcciones que integran la Secretaría de Seguridad Ciudadana (SSC) del Gobierno del Estado de Tlaxcala, requieren del uso del correo electrónico como una herramienta fundamental para el desarrollo de sus actividades cotidianas, garantizando la seguridad, confidencialidad, integridad y alta disponibilidad en el envío y recepción de la información.

Las presentes políticas de uso del correo electrónico se establecen para concientizar a las y los usuarios sobre los riesgos asociados a la utilización de los recursos tecnológicos puestos a su disposición, considerando que las acciones contrarias a estas disposiciones pueden derivar en responsabilidades legales, administrativas, económicas, o bien, en afectaciones a la imagen institucional. Por ello, el cumplimiento de estas políticas es obligatorio para todo el personal, con el fin de mitigar el riesgo de prácticas inadecuadas.

Para respaldar estas medidas de seguridad y asegurar el funcionamiento óptimo del servicio, los servidores de correo electrónico cuentan con certificaciones internacionales de conformidad bajo las normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0.

El acceso a los correos electrónicos institucionales y alternos se realiza a través de las siguientes direcciones oficiales:

- Portal institucional: <https://ssctlaxcala.awsapps.com/mail>
- Portal alterno: <https://www.gmail.com>

CAPÍTULO 1

RESPONSABILIDADES DEL TITULAR DE LA CUENTA DE CORREO ELECTRÓNICO.

1. **Manejo confidencial de la información:** Tratar toda la información bajo los principios de confidencialidad y reserva, sujetándose a las políticas institucionales de operación, seguridad y control de acceso a los sistemas.
2. **Resguardo de credenciales:** Salvaguardar la contraseña de acceso, cambiarla periódicamente y evitar compartirla bajo ninguna circunstancia. El resguardo estricto y el uso correcto de esta información son responsabilidad exclusiva del titular.
3. **Uso exclusivamente laboral:** Emplear el correo electrónico institucional y alternativo de forma estricta para asuntos laborales. Queda prohibido su uso para fines personales.
4. **Responsabilidad del contenido emitido:** Asumir la responsabilidad total sobre la información transmitida a través del correo electrónico institucional por parte del usuario remitente.
5. **Prohibición de envíos masivos e indebidos:** Queda prohibido el envío masivo de materiales personales o ajenos a la institución, así como el uso inadecuado de la cuenta para difamar, acosar, amenazar o vulnerar los derechos de terceros.
6. **Prohibición de divulgación de material inapropiado:** Abstenerse de publicar, distribuir o divulgar información o material inadecuado, difamatorio, obsceno o ilegal que ponga en riesgo la reputación o integridad de la institución.
7. **Verificación de remitentes:** Comprobar la autenticidad y confiabilidad del remitente de cualquier correo recibido antes de responder o enviar información sensible.
8. **Principios de uso:** Hacer uso del correo institucional guiándose por los principios de racionalidad, respeto, responsabilidad, integridad y seguridad de la información.
9. **Mantenimiento y respaldo del buzón:** Depurar y respaldar periódicamente la información contenida en el correo electrónico, asegurando el espacio disponible para el correcto envío y recepción de mensajes.

-
10. **Estructura formal del correo:** Redactar los mensajes incluyendo los elementos básicos esenciales:
- **Encabezado:** Destinatario y asunto claro.
 - **Cuerpo del mensaje:** Nombre del destinatario y su cargo, mensaje conciso y relevante.
 - **Archivos adjuntos** (cuando aplique).
 - **Firma institucional:** Nombre, cargo, área, dependencia y número telefónico.
11. **Prevención de filtros de spam:** Evitar prácticas que puedan clasificar los correos enviados como correo no deseado (*spam*), tales como:
- Uso excesivo de palabras clave sensibles («*gratis*», «*oferta limitada*», «*garantizado*», etc.).
 - Formatos o diseños exagerados (uso predominante de mayúsculas, colores brillantes, exceso de signos de exclamación o fuentes no profesionales).
 - Inclusión de enlaces sospechosos o a sitios web de dudosa reputación.
12. **Restablecimiento de contraseña:** Solicitar la reposición de contraseña por pérdida u olvido por escrito al Departamento de TIC'S, detallando los motivos y firmado por el titular del área correspondiente.
13. **Patrimonio institucional y entrega-recepción:** Reconocer que la cuenta de correo, la contraseña y la información contenida constituyen una bien intangible propiedad de la S.S.C., por lo que forman parte de los activos a entregar en el proceso de entrega-recepción.
14. **Notificar el desuso de correos electrónicos.** Informar por escrito al Departamento de TIC'S, cuando un correo electrónico ya no se utilice, con el fin de eliminarlo del directorio y del servidor de correos si aplicara.
15. **Restricción sobre el correo de recuperación:** Queda estrictamente prohibido modificar el correo de recuperación asignado. Para el restablecimiento o recuperación de contraseñas de los correos alternos, el Departamento de TIC'S establece de manera exclusiva la cuenta soportetecnico.ces@gmail.com como único medio oficial autorizado.

CAPÍTULO 2

ADMINISTRACIÓN Y CONTROL DE CUENTAS DE CORREO ELECTRÓNICO POR EL DEPARTAMENTO DE TIC'S.

16. **Facultad exclusiva de creación y asignación:** El Departamento de TIC'S es el único órgano facultado para crear, configurar e instituir cuentas de correo electrónico (ya sean institucionales o alternas) a solicitud de las Áreas Staff y Direcciones que integran la SSC.
17. **Asignación de correos electrónicos:** Para la asignación de nuevos correos electrónicos, así como el nombre de estas, serán con base a la estructura orgánica de la institución.
18. **Administración de la cuenta de recuperación:** Para las cuentas de correo alternas bajo el dominio @gmail.com, el Departamento de TIC'S utilizará la cuenta de recuperación suportetecnico.ces@gmail.com, con el fin de brindar soporte técnico, gestionar el restablecimiento de contraseñas y garantizar la continuidad del servicio ante eventuales contingencias.
19. **Actualización y difusión del Directorio Oficial:** Mantener actualizado y remitir periódicamente vía correo electrónico, el "Directorio Oficial de Correos Electrónicos de la S.S.C.", a todas las áreas integrantes de la institución.
20. **Depuración y gestión de cuentas inactivas:** Queda facultado para suspender, bloquear y, en su caso, depurar o eliminar las cuentas de correo electrónico institucional que permanezcan inactivas o cuyos titulares se hayan dado de baja laboral, con el fin de optimizar el espacio de almacenamiento y posibilitar la reasignación.
21. **Capacitación y asistencia técnica:** Brindar asistencia, soporte técnico y capacitación continua sobre el uso correcto, seguro y eficiente del correo electrónico institucional al personal de las áreas que así lo requieran.

Tlaxcala, Tlax., a 27 de julio de 2026

Vo. Bo.



PODER EJECUTIVO
SECRETARÍA DE SEGURIDAD CIUDADANA
CAPITÁN DE NAVIO TM. P.D.E.M.
ALBERTO MARTÍN PEREA MARRUFO
SECRETARIO DE SEGURIDAD CIUDADANA

REVISO



CLAUDIA RAQUEL FLORES
ASCENCIO
DIRECTORA ADMINISTRATIVA DE LA
S.S.C.

ELABORO



JEFE DE DEPARTAMENTO DE
TECNOLOGÍAS DE INFORMACIÓN Y
COMUNICACIONES DE LA S.S.C.