Guía de Recomendaciones para la Conservación, Clasificación y Eliminación

Correos Electrónicos Institucionales

www.itei.org.mx
www.seajal.org

itei | INSTITUTO DE TRANSPARENCIA, INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE JALISCO

SEAJAL Sistema Estatal Anticorrupción de Jalisco | Secretaría Ejecutiva

Elaboración:

- Miguel Navarro Flores
  Titular de la Unidad de Transparencia de la SESAJ

- José Raúl Solórzano de Anda
  Coordinador de Informática y Sistemas

Revisión:

- Jazmín Elizabeth Ortiz Montes
  Secretaria Ejecutiva

- Ruth Isela Castañeda Ávila
  Directora de Planeación y Proyectos Estratégicos

- Moctezuma Quezada Enríquez
  Director de Evaluación y Gestión Documental

- Rosa Elena Montaño González
  Directora Jurídica

- Manuel Rojas Munguía
  Director del Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales

- Carlos Antonio Yáñez González
  Director de Protección de Datos Personales

Contenido

Disposiciones generales

1. Esta guía es de carácter general y se recomienda su cumplimiento para el uso adecuado de todas las cuentas de correo electrónico institucional.

2. El correo electrónico institucional está diseñado para facilitar la comunicación y el intercambio de información, contribuyendo de esta manera a alcanzar los objetivos y metas de la institución.

3. Debe evitarse el uso del correo electrónico institucional para propósitos ajenos a las actividades encomendadas por la institución o para asuntos de carácter personal.

4. Las personas servidoras públicas usuarias del correo electrónico institucional, por ningún motivo deberán hacer uso de cuentas no institucionales, personales o comerciales ajenas a la institución para el tratamiento de información pública de cualquier tipo, en ejercicio de sus funciones.

5. Toda la información contenida en las cuentas de correo electrónico institucionales es propiedad de la dependencia.

Objeto y ámbito de aplicación

Objeto: Promover la adecuada organización y conservación de los correos electrónicos institucionales de la Administración Pública, en cumplimiento con las disposiciones aplicables al acceso a la información pública, protección de datos personales y gestión documental.

Ámbito de aplicación: La presente guía de recomendaciones aplica a todas las cuentas de correo electrónico institucional de la Administración Pública, con el fin de garantizar su correcta organización y conservación conforme a las normativas vigentes sobre acceso a la información pública, protección de datos personales y gestión documental.

Naturaleza jurídica del correo electrónico de archivo

Los correos electrónicos y sus documentos adjuntos se consideran información pública de acuerdo con el Criterio del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) SO/008/10 'Correos electrónicos que constituyen documentos susceptibles de acceso a la información' y el Criterio del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI) 003/2010 'Criterios que determinan que las comunicaciones de los integrantes de los sujetos obligados a través de correo electrónico oficial en ejercicio de sus atribuciones u obligaciones son información pública'. Si se solicita acceso a esta información, se seguirá el procedimiento establecido por la Institución.

Los correos electrónicos de carácter estrictamente personal no deben existir en las cuentas institucionales. Únicamente deben estar los mensajes relacionados con las funciones de la dependencia o entidad y con las actividades de las personas en su calidad de servidores públicos, y deben estar sujetos a las recomendaciones de esta guía.

Los correos electrónicos institucionales que puedan ser considerados documentos de archivo deben tratarse de acuerdo con la normativa aplicable en la materia.

Introducción

La conservación, baja y eliminación de correos electrónicos son procesos fundamentales en la gestión documental de cualquier Institución. Estas acciones no solo garantizan la correcta administración de los documentos electrónicos, sino que también contribuyen a mantener la eficiencia y transparencia en el manejo de la información. En este sentido, es crucial establecer recomendaciones claras que permitan una gestión adecuada de los correos electrónicos, asegurando su preservación cuando sea necesario y su eliminación de manera segura cuando hayan cumplido su ciclo de vida útil.

Organización de Correos Electrónicos Institucionales

Creación de Mensajes de Correo Electrónico

Se debe incluir al menos un asunto y la firma institucional, que contenga nombre, cargo y número telefónico de oficina o un Código QR para identificación rápida del remitente.

Desde la configuración de la cuenta, se debe agregar una firma que incluya la leyenda:

"El contenido de este correo electrónico es información pública y susceptible de solicitud de información. Existe la posibilidad de que este correo electrónico contenga datos personales de acuerdo con lo establecido en el artículo 3, fracciones IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, así como información confidencial de conformidad al artículo 21 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

En ese tenor y atendiendo a lo establecido por el artículo 72 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, el receptor de los datos personales deberá tratar los mismos comprometiéndose a garantizar su confidencialidad y únicamente utilizarlos para los fines que le fueron transferidos. Además de que adquiere el carácter de responsable. El tratamiento de esta información deberá cumplir en todo momento con las disposiciones de las leyes antes señaladas, por lo que cualquier transferencia o tratamiento de los datos por personas o entidades distintas a las dirigidas se encuentra prohibido; salvo las excepciones contempladas en los artículos 15 y 75 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios."

Documentos de Archivo

En el ámbito gubernamental, no se considerarán documentos de archivo los correos electrónicos y sus adjuntos que sean de comprobación administrativa inmediata, documentos de trabajo o de apoyo informativo, esto de acuerdo a la Ley de Archivos del Estado de Jalisco y sus Municipios, artículo 3, fracción XV:

"XV. Documento de archivo: aquel que registra un hecho, acto administrativo, jurídico, fiscal o contable producido, recibido y utilizado en el ejercicio de las facultades, competencias o funciones de los sujetos obligados, con independencia de su soporte documental;"

Casos de uso específico:

Aquí hay algunos casos de uso específicos que pueden ayudar a las personas servidoras públicas a identificar qué correos electrónicos deben conservar, clasificar o eliminar:

Comunicaciones Oficiales: Identificar correos electrónicos que contienen comunicaciones oficiales, como decisiones gubernamentales, directrices de políticas, instrucciones para la implementación de programas, entre otros. Estos correos electrónicos deben conservarse y archivarse adecuadamente según los requisitos legales y regulatorios.

Solicitudes de Información: Identificar correos electrónicos que contienen solicitudes de información pública. Estos correos electrónicos deben conservarse y tratarse de acuerdo con los procedimientos establecidos por la institución, para garantizar la transparencia y el cumplimiento de las leyes de acceso a la información.

Contratación y Adquisiciones: Identificar correos electrónicos relacionados con procesos de contratación y adquisiciones, como solicitudes de propuestas, evaluaciones de ofertas, decisiones de adjudicación, entre otros. Estos correos electrónicos deben conservarse para garantizar la integridad de los procesos y la rendición de cuentas.

Comunicaciones Internas: Identificar correos electrónicos que contienen comunicaciones internas dentro de la organización gubernamental, como memorandos, circulares, informes de estado, actualizaciones de proyectos, entre otros. Estos correos electrónicos pueden clasificarse y archivarse según su relevancia y utilidad para futuras referencias.

Comunicaciones Externas Sensibles: Identificar correos electrónicos que contienen información sensible o confidencial con entidades externas, como información personal, datos financieros, información de seguridad, entre otros. Estos correos electrónicos deben ser tratados con cuidado y conservarse de acuerdo con las normas del documento seguridad de la institución.

Organización de Mensajes

Una forma efectiva de gestionar los mensajes en una cuenta de correo electrónico es mediante la creación de carpetas o etiquetas, y deberá estar de conformidad al Cuadro General de Clasificación Archivística vigente. Estas herramientas permiten organizar los mensajes enviados y recibidos de manera estructurada, facilitando su búsqueda y acceso posterior. Al crear carpetas o etiquetas, es importante utilizar nombres descriptivos que reflejen claramente el contenido de los mensajes que se almacenarán en ellas, lo que ayudará a mantener un sistema de organización coherente y fácil de entender.

Además, la capacidad de crear carpetas o etiquetas también puede utilizarse para priorizar mensajes importantes, separar mensajes de comprobación inmediata o a los correos que se deberán de conservar, clasificar y eliminar.

Esta funcionalidad es especialmente útil para mantener una bandeja de entrada ordenada y evitar la acumulación de mensajes sin clasificar. La organización de mensajes mediante carpetas o etiquetas es una práctica recomendada para mejorar la eficiencia, la gestión, conservación y clasificación de la información en el correo electrónico.

Baja, conservación y eliminación de correos electrónicos

La baja, conservación y eliminación adecuada de los correos electrónicos debe realizarse conforme al catálogo de disposición documental, un aspecto fundamental en la gestión de la información institucional. Este proceso implica la identificación, clasificación y almacenamiento de los correos electrónicos con valor documental, así como la eliminación segura de aquellos que no son necesarios para la organización. Una correcta gestión de la baja, conservación y eliminación de los correos electrónicos garantiza la transparencia, la integridad de los registros y el cumplimiento de las normativas internas.

Por lo anterior, la persona usuaria de la cuenta es responsable de identificar el tipo de mensajes de correo electrónico, clasificándolos en mensajes de correos electrónicos considerados documentos de archivo y mensajes de correo electrónico no considerados como documentos de archivo.

Mensajes de correo electrónico considerados documentos de archivo:

Los mensajes de correo electrónico que se consideran documentos de archivo son aquellos que contienen información relevante y necesaria para respaldar las actividades y decisiones institucionales. Entre ellos se encuentran comunicaciones oficiales, acuerdos, informes, solicitudes y otros documentos de importancia legal, administrativa o histórica para la organización. Estos mensajes deben ser almacenados en las carpetas o etiquetas correspondientes al tema.

Es fundamental identificar y clasificar adecuadamente estos correos electrónicos, ya que deben ser conservados y gestionados de acuerdo con las normativas aplicables. Para ello, se utilizan instrumentos archivísticos como el catálogo de disposición documental, los cuadros de clasificación y los inventarios documentales, que ayudan en la correcta identificación y manejo de estos correos.

Los correos con valores archivísticos secundarios, como los evidénciales, testimoniales o informativos, también deben ser preservados adecuadamente, ya que pueden ser cruciales para fines de transparencia, rendición de cuentas y cumplimiento normativo.

Mensajes de correo electrónico no considerados como documentos de archivo:

Estos mensajes contienen información que no está relacionada con las facultades, competencias o funciones de las personas servidoras públicas, spam, información no solicitada, correos de comprobación administrativa inmediata o documentos de apoyo informativo que no forman parte del archivo de la Institución.

Conservación, baja y eliminación de los correos electrónicos:

La conservación, baja y eliminación de los correos electrónicos es responsabilidad única de la persona usuaria de la cuenta de correo electrónico. Es importante que cada usuario gestione adecuadamente su bandeja de entrada conforme al Cuadro General de Clasificación Archivística.

1. **Conservación de los correos electrónicos:** Una vez identificados los correos electrónicos y ubicados en las carpetas o etiquetas correspondientes, se recomienda conservar los mensajes clasificados como documentos de archivo dentro de la cuenta de correo electrónico del usuario.

   Es fundamental organizarlos adecuadamente mediante la creación de carpetas o etiquetas específicas que reflejen su clasificación conforme al Cuadro General de Clasificación Archivística. Esta práctica facilita el acceso y la gestión de estos mensajes, garantizando su disponibilidad cuando sea necesaria su consulta o respaldo de la información.

2. **Baja de los correos electrónicos de la cuenta institucional:** Para realizar la baja de correos electrónicos de la cuenta institucional, se pueden considerar las siguientes opciones:

   Archivado local: Guardar una copia de los correos electrónicos en su formato nativo en el disco duro de la computadora o en dispositivos de almacenamiento externo. Esta opción es útil para acceder a los correos electrónicos sin conexión a internet, garantizando así su disponibilidad en todo momento.

   Almacenamiento en servidores locales: Utilizar servidores locales para almacenar los correos electrónicos en su formato nativo. Esta opción ofrece un mayor control sobre la seguridad y la accesibilidad de los datos, asegurando que la información esté protegida y sea fácilmente accesible para futuras consultas.

   Una vez, realizada la baja de los correos electrónicos, ya sea de manera local o en algún servidor, se sugiere que los correos electrónicos no deberán exceder ahí más

de 30 días, la persona responsable de archivo de trámite deberá revisar la carpeta compartida entre los días 1 al 5 de cada mes, con la finalidad de organizarlos en dicha carpeta y en su caso, cargarlos en el expediente generado en el Sistema de Gestión Documental o en algún repositorio de información digital y deberá verificar el adecuado vaciado y acomodo de las carpetas, donde atenderá los plazos de conservación establecidos en el Catálogo de Disposición Documental vigente.

3. **Eliminación de los correos electrónicos de la cuenta institucional**: Esta recomendación asegura que los mensajes y documentos que ya no tienen valor administrativo, legal, o histórico sean removidos de manera adecuada, liberando espacio y optimizando los recursos financieros y el rendimiento del sistema de correo electrónico. A continuación, se describen las pautas para llevar a cabo la eliminación segura y responsable de correos electrónicos institucionales.

Recomendaciones para la eliminación segura y responsable de correos electrónicos institucionales

Para llevar a cabo la eliminación segura y responsable de correos electrónicos institucionales, es esencial seguir ciertas recomendaciones, mismas que aseguren la integridad y confidencialidad de la información, las cuales consisten en:

1. **Identificación y Clasificación conforme al Cuadro General de Clasificación Archivística y el Catálogo de Disposición Documental.**

   a. **Clasificación de los correos electrónicos:**

      i. Apoyo informativo (transitorio).
      ii. Comprobación administrativa inmediata
      iii. Documentos de Trabajo (Eliminación de la cuenta de correo electrónico una vez transcurrido el periodo de permanencia)

   b. **Revisión periódica:** Realizar una revisión periódica de los correos electrónicos para identificar aquellos que ya no son necesarios.

2. Estrategias de retención

a. **Períodos de conservación en la cuenta del correo electrónico:** Respetar los períodos de conservación mínimos antes de proceder a la eliminación, los cuales deben estar en conformidad con el Catálogo de Disposición Documental.

3. Técnicas de eliminación

a. **Eliminación**: Borrar manualmente los correos electrónicos que han sido clasificados como eliminables, asegurándose de vaciar la papelera de reciclaje o la carpeta de elementos eliminados

b. Se recomienda, que los correos electrónicos sin valor Institución, sean eliminados una vez que hayan cumplo con los plazos establecidos por el Catálogo de Disposición Documental, que serán desde su creación y/o recepción, respectivamente.

4. Registro de eliminación

a. **Documentación**: Mantener un registro detallado de los correos electrónicos eliminados, incluyendo la fecha de eliminación, el motivo y cualquier otra información relevante.

5. Capacitación del personal

a. **Formación:** Proveer capacitación continua al personal sobre las recomendaciones de esta guía.

b. **Concientización**: Aumentar la conciencia acerca de la importancia de la eliminación segura y responsable de la información.

Al seguir estas recomendaciones, se garantiza que la eliminación de correos electrónicos se realice de manera eficiente, segura y conforme a las regulaciones vigentes.

Se recomienda, que la totalidad de los mensajes de correo electrónico deberán cumplir con el periodo de permanencia establecido por el grupo interdisciplinario de archivo de la institución para fines de acceso a la información. Este período se contará a partir de la fecha de creación, primera recepción o primer envío en los buzones de cada persona usuaria de la cuenta.

Los mensajes de correo electrónico recibidos que contienen información ajena a las facultades, competencias o funciones del usuario de la cuenta, así como spam, publicidad, información no solicitada y mensajes de carácter meramente informativo, no forman parte del archivo de la Institución. Estos mensajes podrán eliminarse de manera inmediata sin necesidad de seguir ningún procedimiento adicional.

En consecuencia, los mensajes de correo electrónico institucional que formen parte del archivo de la Institución no podrán eliminarse de la bandeja de correo institucional hasta que se haya cumplido su periodo de conservación, conforme al Catálogo de Disposición Documental.

Recomendaciones para realizar Respaldos Electrónicos para Servidores Públicos en Caso de Baja

Cuando la persona servidora pública se da de baja por cualquier motivo, es crucial realizar respaldos electrónicos adecuados de los correos y archivos considerados documentos de archivo. En este sentido, el personal de tecnologías de la información y comunicación de cada institución o entidad será el área encargada de apoyar en la realización de estos respaldos, del registro y la documentación. A continuación, se presenta algunos pasos y consideraciones importantes:

Identificación de documentos de archivo: Antes de la baja de la persona responsable de la cuenta, es necesario realizar una verificación para validar la identificación y clasificación de los correos y archivos que se consideran documentos de archivo según las normativas establecidas por la institución.

En el supuesto, de que la identificación y clasificación no es la adecuada, el superior jerárquico designará a una persona responsable para proceder con la clasificación correspondiente para garantizar la conservación y el manejo adecuado de la información. Además, se podrá entonces seguir el apartado de “Transferencia de responsabilidades” recomendado por esta guía para la persona servidora pública saliente.

Realización de respaldos: Realizar respaldos electrónicos de los documentos de archivo de forma segura y siguiendo las pautas establecidas por la institución.

Es recomendable utilizar medios de almacenamiento confiables para proteger la información.

Registro y documentación: Mantener un registro detallado de los documentos respaldados, incluyendo información como fecha de respaldo, tipo de documento y ubicación del respaldo.

Almacenamiento seguro: Almacenar los respaldos electrónicos en un lugar seguro y protegido contra riesgos como incendios, inundaciones y robos, además, considerar la posibilidad de utilizar servicios de almacenamiento en la nube con altos estándares de seguridad.

Conservación: Seguir las pautas de retención de datos establecidas por el catálogo de disposición documental de la institución para determinar cuánto tiempo se conservarán los respaldos electrónicos antes de su eliminación.

Transferencia de responsabilidades: En caso de que el servidor público sea reemplazado, es esencial asegurar la transferencia adecuada y documentada de los respaldos electrónicos y la responsabilidad de su custodia, ya sea a la persona servidora pública entrante o al superior jerárquico.

Sobre el derecho a la información, derechos ARCO y Portabilidad

Cuando la Unidad de Transparencia de la Institución, reciba una solicitud de acceso a la información relacionada con mensajes de correo electrónico institucional, esta deberá atenderse de acuerdo con el periodo de permanencia establecido en el catálogo de disposición documental. Los correos electrónicos podrán entregarse en formato PDF o en su formato nativo, según corresponda. Los documentos adjuntos se proporcionarán en su formato original. En caso de que la información contenga datos personales, estos se entregarán en versión pública, protegiendo así la privacidad de los individuos involucrados. La persona titular de los datos personales podrá ejercer sus derechos de acceso, rectificación, cancelación u oposición (ARCO) a través de los mecanismos establecidos por la Institución, garantizando la protección de su información personal.

Mejores Prácticas de Seguridad Correos Electrónicos Institucionales

Las siguientes recomendaciones ayudarán a proteger la información confidencial que obra en los correos electrónicos institucionales, las cuales tienen como finalidad garantizar la seguridad y privacidad de la información, a continuación, se enlistan algunos consejos de seguridad:

Contraseñas seguras: Utilizar contraseñas complejas y únicas para cada cuenta de correo electrónico. Las contraseñas deben tener al menos 8 caracteres y contener una combinación de letras, números y caracteres especiales.

Verificación en dos pasos: Habilitar la verificación en dos pasos para agregar una capa adicional de seguridad. Esto requerirá un código de verificación adicional además de la contraseña para acceder a la cuenta.

No compartir contraseñas: Nunca compartir contraseñas por correo electrónico ni almacenarlas en archivos no cifrados, mantener las contraseñas seguras y privadas.

Evitar enlaces y archivos adjuntos sospechosos: No hacer clic en enlaces ni abrir archivos adjuntos de correos electrónicos desconocidos o sospechosos, ya que podrían contener malware o ser phishing.

Actualizaciones regulares: Mantener el software de correo electrónico y el sistema operativo actualizados para protegerse contra vulnerabilidades conocidas.

Cifrado de correos electrónicos: Utilizar servicios de correo electrónico que ofrezcan el cifrado de extremo a extremo para proteger el contenido de los correos electrónicos y garantizar que solo el destinatario previsto pueda leerlos.

Al seguir estos consejos de seguridad, se puede mejorar la protección de la información confidencial en los correos electrónicos Institucionales y reducir el riesgo de vulneración.

De la Interpretación

La interpretación de la presente guía le corresponde al Grupo Interdisciplinario en materia de archivo de cada institución.

Glosario

Acceso a la Información: Derecho fundamental que permite a las personas obtener información pública de los sujetos obligados.

Archivo: Conjunto de documentos producidos y recibidos por una institución en el ejercicio de sus funciones, conservados para servir como testimonio de sus actividades y para la consulta de interesados.

Asunto: Breve descripción del contenido de un correo electrónico.

Catálogo de Disposición Documental: Instrumento archivístico que establece los plazos de conservación y disposición final de los documentos de una institución.

Correo Electrónico: Mensaje digital enviado a través de una red de computadoras.

Cuenta de Correo Electrónico: Dirección electrónica única que se utiliza para enviar y recibir mensajes a través de Internet.

Cuadro General de Clasificación Archivística: Instrumento archivístico que establece la organización jerárquica de los documentos de una institución.

Datos Personales: Cualquier información relacionada con una persona física identificada o identificable.

Documento: Registro de información en cualquier soporte (papel, electrónico, etc.) que se produce o recibe en el ejercicio de las atribuciones y funciones de una institución.

Eliminación de Correos Electrónicos: Acción de eliminar permanentemente un correo electrónico de una cuenta.

Firma Institucional: Conjunto de datos asociados a un mensaje de correo electrónico que permiten verificar la identidad del remitente.

Información Pública: Toda información generada, recibida, recopilada o producida por cualquier institución de la administración pública federal, estatal y municipal, en ejercicio de sus funciones, en cualquier soporte físico o digital.

Organización de Correos Electrónicos: Proceso de clasificación y almacenamiento de correos electrónicos de manera eficiente y segura.

Persona Servidora Pública: Persona física que desempeña un empleo, cargo o comisión en la administración pública.

Protección de Datos Personales: Principios y medidas que se adoptan para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Respaldo Electrónico: Copia de seguridad de los datos almacenados en una cuenta y/o dispositivo electrónico.

Seguridad de la Información: Conjunto de medidas y controles que se adoptan para proteger la información contra amenazas como el acceso no autorizado, la divulgación no autorizada, la alteración, la destrucción o la pérdida.

Soporte Documental: Medio físico o digital en el que se encuentra registrada la información contenida de un documento.

Usuario: Persona que utiliza una cuenta de correo electrónico.

Valores Archivísticos: Características que hacen que un documento sea de interés para la investigación, la gestión administrativa o la memoria histórica.