CECC

CENTRO DE ESTUDIOS
CRISTÓBAL COLÓN

NORMATIVA PARA EL USO DE CORREO ELECTRÓNICO INSTITUCIONAL DEL CENTRO DE ESTUDIOS CRISTÓBAL COLÓN A.C.

ÍNDICE

I.	INTRODUCCIÓN	3
II.	OBJETO	3
III.	ALCANCE	3
IV.	OBJETIVO	4
V.	MARCO LEGAL	4
VI.	SERVICIOS GOOGLE WORKSPACE (GWE)	4
VII.	RESPONSABILIDADES DEL USUARIO	5
A.	Aceptación	5
B.	Confidencialidad	5
C.	Recomendaciones para el uso seguro y eficiente	5
D.	Precauciones	6
E.	Firma del correo electrónico institucional	7
F.	Capacidad	7
G.	Acciones prohibidas	9
H.	Acciones disciplinarias	9
VII.	ALTA DE LA CUENTA	10
A.	Criterios para el nombre de usuario	10
IX.	BAJA DE LA CUENTA	11
X.	DISPOSICIONES PARA MENORES DE EDAD	11
XI.	MODIFICACIONES A LA NORMATIVA	11
XII.	GLOSARIO DE TÉRMINOS	12

INTRODUCCIÓN

El Centro de Estudios Cristóbal Colón (en adelante, el CECC), es una institución educativa particular a cargo de la Orden de las Escuelas Pías de la Provincia de México en la Presencia de Veracruz. Su oferta educativa comprende los niveles de preescolar, primaria, secundaria, bachillerato y universidad.

En la actualidad es importante una normativa para el uso de correo electrónico institucional para garantizar la seguridad, privacidad y eficiencia en el uso de este medio de comunicación. El CECC a través de la Dirección de Tecnologías de Información (en adelante DTI), ofrece a su comunidad educativa el servicio de correo electrónico mediante la asignación de una cuenta institucional.

El correo electrónico de la institución forma parte de los servicios que ofrece Google Workspace for Education (en adelante, GWE) en convenio con el CECC. Al tratarse de servicios tercerizados la disponibilidad del servicio de GWE, así como de la seguridad de la información de los usuarios, es responsabilidad y dominio por completo de Google.

La DTI será encargada de establecer las medidas técnicas que garanticen el correcto funcionamiento del servicio de correo electrónico institucional.

OBJETO

La normativa para el uso del correo electrónico institucional, busca promover el uso seguro, responsable y eficiente en conformidad con el marco legal de México, protegiendo los derechos de los usuarios y garantizando la integridad de la comunidad educativa del CECC.

Busca establecer las responsabilidades, lineamientos, normas y las buenas prácticas que deberán cumplir todos los usuarios del correo electrónico institucional, con el fin de garantizar el correcto uso del mismo y asegurar un mejor aprovechamiento, como una herramienta de trabajo que provee el CECC para beneficio de toda su comunidad.

ALCANCE

La normativa para el uso del correo electrónico institucional se aplica a todos los usuarios que forman parte del CECC y que tienen asignada una cuenta de correo institucional, bajo los dominios: @ucc.mx para universidad y/o @colon.mx para los niveles de preescolar, primaria, secundaria y bachillerato.

OBJETIVO

El correo institucional es una herramienta esencial en el ecosistema educativo del CECC, permitiendo una comunicación eficiente y segura. A través de este medio, se gestionan actividades administrativas, académicas y logísticas, que son fundamentales para la operación diaria de la institución. Esta normativa tiene como objetivo principal establecer pautas claras para el uso correcto del correo, evitando abusos, malos usos y cualquier acción que pudiera comprometer la seguridad de la información.

Al asegurar que todos los miembros de la comunidad educativa utilicen el correo institucional de manera adecuada, se promueve un entorno de confianza garantizando que todas las interacciones sean coherentes con los valores institucionales, los derechos de los usuarios y cumplir con las normativas legales vigentes aplicables. Asimismo, se garantiza que el uso de los servicios ofrecidos a través de GWE esté alineado con los estándares de seguridad y privacidad necesarios en un contexto educativo.

MARCO LEGAL

Esta normativa para el uso de correo electrónico institucional, tiene fundamentos en el marco normativo que contempla leyes vigentes y que regulan el derecho a la información, la protección de datos personales, y el funcionamiento de instituciones educativas. Siendo las siguientes:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- Ley General de los Derechos de Niñas, Niños y Adolescentes.
- Ley General de Educación.
- Reglamento General de Alumnos Universidad Cristóbal Colón.

SERVICIOS GOOGLE WORKSPACE (GWE)

Los servicios que están incluidos en la cuenta de correo institucional para todos los usuarios son:

- Gmail
- Google Drive
- Google Meet
- Google Calendar
- Google Docs, Sheets y Slides
- Google Chat

RESPONSABILIDADES DEL USUARIO

A. Aceptación

La utilización del servicio de correo electrónico institucional proporcionado por el CECC al usuario implica que el usuario de la cuenta de correo electrónico al hacer uso de ella declara que:

- Conoce y acepta plenamente las normas de uso y condiciones que se especifican en el presente documento.
- Conoce y acepta los términos de servicio y política de privacidad de Google los cuales se encuentran publicados en la dirección https://policies.google.com
- Acepta cumplir con cualquier disposición que la DTI haga sobre el uso de los servicios y recursos de GWE, las cuales serán comunicadas a través de los medios oficiales del CECC.
- Acepta que utilizará la cuenta para fines laborales, administrativos y/o académicos relacionados con el CECC, excluyendo cualquier uso personal que pueda interferir con las responsabilidades educativas o laborales.
- Asume completa responsabilidad del uso de su cuenta, así como de la información que se transmita mediante la misma, deslindando al CECC, a su personal y a sus colaboradores de cualquier responsabilidad derivada de su utilización.
- Acepta que la DTI se reserva el derecho de crear, modificar, deshabilitar o eliminar las cuentas de correo institucional, en las cuales se evidencie un uso inadecuado o que incurran en el incumplimiento de las políticas plasmadas en el presente documento.
- En el caso de los menores de edad, sus tutores o representantes legales son los responsables de supervisar el uso correcto del correo institucional.

B. Confidencialidad

El usuario de la cuenta de correo electrónico institucional es responsable de mantener la confidencialidad de su cuenta, la protección de la contraseña, la privacidad de los datos a los que tiene acceso y el uso adecuado en todas las actividades que se efectúen bajo su cuenta de correo institucional, esto incluye:

- **Protección de contraseñas:** No debe compartir sus credenciales de acceso con nadie, y se recomienda el uso de autenticación en dos pasos para mejorar la seguridad de las cuentas. El personal de la DTI no cuenta con la posibilidad de consultar la contraseña de un usuario ni de acceder a la información, mensajes y archivos almacenados dentro de la cuenta.

- **Manejo de información sensible:** La información relacionada con la institución, los alumnos o el personal (como datos académicos, financieros, personales, por mencionar algunos) debe manejarse con la máxima confidencialidad. Cualquier divulgación no autorizada puede constituir una violación grave a la política de la institución y a la normativa mexicana en materia de protección de datos.

El CECC se compromete a cumplir con el marco legal aplicable para el tratamiento y protección de datos personales de los usuarios.

C. Recomendaciones para el uso seguro y eficiente

El uso seguro y eficiente del correo institucional es indispensable para proteger la información confidencial y sensible de la institución, así como para garantizar la productividad y eficiencia en la comunicación. Un uso inadecuado del correo electrónico institucional puede llevar a problemas de

seguridad, perdida de datos y disminución de la productividad, por lo que es importante seguir las siguientes recomendaciones:

• **Formalidad y respeto:** Los correos electrónicos deben ser redactados de manera clara y profesional, evitando el uso de lenguaje inapropiado o informal. Es esencial mantener una actitud de respeto hacia los destinatarios.

• **Frecuencia de revisión:** Los usuarios deben revisar su correo institucional con regularidad para mantenerse al tanto de las comunicaciones importantes. La falta de respuesta oportuna puede tener repercusiones académicas o laborales.

• **Uso responsable de adjuntos:** Los archivos adjuntos deben enviarse sólo cuando sea necesario, y preferentemente en formatos accesibles para todos los destinatarios. Los documentos grandes deben compartirse mediante Google Drive para no saturar las bandejas de entrada.

• **Organización:** Para gestionar adecuadamente la bandeja de entrada, se recomienda el uso de filtros, etiquetas y otras herramientas proporcionadas por Gmail.

• **Seguridad de menores:** La información personal de alumnos menores de edad debe ser tratada con mucha atención. Los usuarios académicos y/o administrativos deben proteger su privacidad y bienestar para cumplir con las leyes y regulaciones aplicables sobre la protección de datos personales de menores de edad.

D. Precauciones

Es fundamental que los usuarios del correo electrónico institucional tomen precauciones para proteger la información confidencial y sensible del CECC, así como para garantizar la seguridad y eficiencia en la comunicación. Algunas de las precauciones más importantes incluyen:

• **Verificación de remitentes sospechosos:** Los ciberdelincuentes suelen falsificar direcciones de correo electrónico para que parezcan confiables. Aunque el nombre que aparece en el campo “De” (remitente) puede parecer familiar (por ejemplo, un colega o un profesor), siempre debes revisar la dirección completa. Si notas dominios mal escritos o extraños, es un indicador de phishing (por ejemplo, en lugar de @gmail.com, puedes ver algo como @gmal.com)

• **Verificación avanzada de enlaces:** Pasa el cursor sobre los enlaces sin hacer clic. Esto revelará la URL real en la parte inferior del navegador o correo. Si ves una dirección que no coincide con el remitente legítimo o parece ser una cadena de caracteres extraños (por ejemplo, http://192.52.34.6/randomfolder), no lo abras.

• **Verificación de archivos adjuntos:** Si recibes un archivo comprimido (.zip, .rar) o un ejecutable (.exe, .bat), debes evitar abrirlo a menos que lo esperes de una fuente confiable.

Los documentos de Office como .docx o .xls también pueden contener macros maliciosos, que son pequeños programas embebidos en el archivo que ejecutan malware una vez abierto. Para mayor seguridad, desactiva las macros en tu software de Office, o utiliza las versiones de Google Docs para abrir estos archivos.

Documentos PDF: Aunque los PDFs se perciben como más seguros, algunos también pueden contener scripts maliciosos. Si un PDF proviene de una fuente sospechosa, abre el archivo en Google Drive, ya que este entorno es más seguro que descargar el archivo localmente.

• **Desconfía de mensajes urgentes o amenazas:** Los ciberdelincuentes utilizan tácticas de ingeniería social para manipularte. Mensajes con palabras como "urgente", "acción requerida inmediata", "tu cuenta ha sido bloqueada", o "tu cuenta será suspendida" son señales de alerta. Los correos legítimos del CECC no suelen presionarte para que tomes decisiones rápidas.

• **Autenticidad en solicitudes de datos personales:** Ningún correo legítimo te pedirá contraseñas, números de tarjeta de crédito o información personal. Si recibes una solicitud así, aunque parezca que viene de un administrador o soporte técnico del CECC, es casi seguro que se trata de un intento de phishing.

• **Mantén el sistema y el navegador actualizados:** Asegúrate de que tu sistema operativo y navegador Web están configurados para recibir actualizaciones automáticas. Las actualizaciones corrigen vulnerabilidades que los ciberdelincuentes podrían explotar a través de correos maliciosos. Por ejemplo, vulnerabilidades en los navegadores web podrían permitir la ejecución de código malicioso simplemente con hacer clic en un enlace.

E. Firma del correo electrónico institucional

La firma de correo electrónico institucional es un elemento importante en la comunicación electrónica en el ámbito laboral y académico. Se aplica a todos los usuarios que forman parte del CECC y que tienen asignada una cuenta de correo institucional, se adjunta al final de todos los mensajes y sirve para identificar al usuario de la cuenta.

La firma de correo electrónico institucional es asignada por el CECC a los usuarios, se establece un modelo genérico de diseño de firma institucional con el objetivo de establecer una identidad visual de la institución, como se muestra a continuación:

Ejemplo

No está permitido añadir información adicional o segundos logotipos, y deberá ir acompañada de la política de privacidad institucional vigente autorizada.

F. Capacidad

Como parte de la política institucional para el uso eficiente de los recursos tecnológicos, a cada cuenta de usuario en Google Workspace se le asignará un espacio de almacenamiento estándar de 20 GB en Google Drive. Esta medida tiene como objetivo garantizar una administración ordenada y equitativa del espacio disponible, promoviendo al mismo tiempo buenas prácticas en la gestión de archivos digitales.

No obstante, se reconoce que ciertas funciones administrativas, académicas o de gestión de proyectos institucionales pueden requerir un volumen mayor de almacenamiento debido a la naturaleza y alcance de sus responsabilidades. Por ello, se contempla la posibilidad de ampliar el espacio asignado de manera excepcional para cuentas que justifiquen esta necesidad.

La asignación de un mayor espacio estará sujeta a los siguientes lineamientos:

- **Solicitud formal:** El titular de la cuenta deberá presentar una solicitud justificada ante la DTI, especificando los motivos por los cuales se requiere una ampliación del almacenamiento.

- **Evaluación de la necesidad:** La DTI evaluará cada solicitud considerando criterios como la frecuencia de uso, el tipo de archivos almacenados, el rol del usuario en la institución y la duración del requerimiento.

- **Asignación temporal o permanente:** Según la evaluación, el espacio adicional podrá ser otorgado de forma temporal (para atender una necesidad puntual) o permanente (cuando la función del usuario así lo exija).

- **Revisión periódica:** Las cuentas con espacio ampliado estarán sujetas a revisiones periódicas para verificar el uso adecuado de los recursos asignados.

Se exhorta a todos los usuarios a hacer uso responsable del espacio de almacenamiento, privilegiando la organización, eliminación de archivos innecesarios y la utilización de formatos optimizados para reducir el consumo de recursos.

Si se excede la cuota de almacenamiento establecida, pueden ocurrir varios inconvenientes que afectan tanto el acceso como el uso de tu cuenta, como los siguientes:

- **No podrás enviar ni recibir correos electrónicos:** No podrás enviar mensajes y los correos entrantes serán rechazados, lo que significa que las personas que intenten enviarte un correo recibirán una notificación de error de “buzón lleno”.

- **No se podrán sincronizar los archivos de Google Drive:** No podrás subir ni sincronizar nuevos archivos. Esto incluye archivos creados en Google Docs, Sheets, Slides u otras aplicaciones de Google Workspace.

- **No se podrán hacer copias de seguridad en Google Photos:** Las fotos y videos que intentes respaldar en Google Photos no se cargarán hasta que liberes espacio.

- **La cuenta puede verse limitada en otras áreas:** Otras aplicaciones de GWE, como Google Calendar o Keep, podrían experimentar problemas si intenta almacenar nueva información.

- **Riesgo de perder acceso a nuevos datos:** Si la cuota de almacenamiento sigue siendo excedida por mucho tiempo, corres el riesgo de perder acceso a nuevos datos, ya que el sistema no puede almacenar más información en tu cuenta.

Recomendaciones para evitar problemas de exceder la capacidad máxima de almacenamiento:

- **Liberar espacio:** Elimina correos electrónicos innecesarios (particularmente aquellos con archivos adjuntos grandes), borra archivos grandes en Google Drive, y revisa tu almacenamiento en Google Photos

para eliminar contenido redundante.

- **Gestionar las versiones de archivos:** En Google Drive, puedes eliminar versiones anteriores de archivos para reducir el espacio ocupado.

Para saber cuánto espacio de almacenamiento has ocupado, da clic en la opción "Almacenamiento" del menú de Google Drive.

G. Acciones prohibidas

Es fundamental conocer y respetar las prohibiciones del uso del correo electrónico institucional para evitar prácticas indebidas y garantizar un entorno digital seguro y respetuoso, las acciones prohibidas se clasifican de acuerdo con la gravedad de la acción cometida y pueden ser cualquiera de las siguientes:

1. Acciones prohibidas leves

- Uso no autorizado: Está prohibido utilizar el correo para actividades personales no relacionadas con la institución, así como para fines comerciales, políticos o actividades con ánimo de lucro que no hayan sido autorizados.
- Distribución de material no autorizado: Está prohibido el envío de archivos que violen derechos de autor o que infrinjan leyes de propiedad intelectual o que viole derechos de terceros.
- Cadenas y Spam: Crear, transmitir o contestar mensajes de correo electrónico que constituyan cadenas, mensajes SPAM o HOAX, virus o programas destinados a dañar el equipo de cómputo de terceros o del CECC.

2. Acciones prohibidas graves

- Contenido ofensivo o discriminatorio: Está estrictamente prohibido, enviar, publicar, distribuir o divulgar cualquier mensaje y/o imágenes con material inapropiado, sacrílego, difamatorio, ilícito, obsceno, indecente, peligroso, amenazante, ilegal, abusivo, hostigador, tortuoso, invasivo del derecho de privacidad, que incite al odio, que contengan lenguaje ofensivo, violento, discriminatorio o de cualquier forma ofensiva a terceros.

- **Ciberacoso:** Difamar, insultar, acechar, amenazar o cualquier forma de acoso, incluyendo el ciberbullying, será tratada como una falta grave y será sancionada de acuerdo con las normativas institucionales y legales.

- **Suplantación de identidad (phishing):** realizar phishing, suplantar o acceder a cuentas ajenas o enviar correos haciéndose pasar por otra persona es una violación grave de esta normativa.

- **Actividades ilegales:** Enviar mensajes para la creación o distribución de información con contenido ilegal o fraudulento.

- Cualquier otra que sea incompatible con las finalidades del CECC y en general, cualquier contravención de las finalidades en esta normativa.

H. Acciones disciplinarias

El incumplimiento de la normativa para el uso del correo electrónico institucional puede tener graves consecuencias por lo que es importante que los usuarios comprendan las acciones que pueden ser tomadas de acuerdo con la gravedad de la acción prohibida cometida y pueden ser cualquiera de las siguientes:

- **Advertencias:** El usuario puede recibir una advertencia verbal o escrita, si la acción se considera leve.

- **Suspensión temporal del acceso:** El usuario puede tener suspensión temporal del acceso a su correo institucional y demás servicios GWE, si la acción se considera leve.

- **Revocación definitiva:** El usuario puede tener la revocación permanente del acceso al correo institucional y demás servicios de GWE, si la acción se considera grave.

- **Sanciones:** El usuario puede enfrentar sanciones dependiendo la gravedad de la acción y con base al siguiente criterio:

  Alumno de Colegio Cristóbal Colón: a lo que disponga la Dirección General de Colegios.
  Alumno de Universidad: a lo que disponga el Reglamento General de Alumnos.
  Personal académico y administrativo: a lo que dispongan las autoridades del CECC.

- **Acciones legales**: El CECC se reserva el derecho de tomar acciones legales por el uso indebido del correo institucional en el que constituyan un delito.

Las acciones no previstas en la normativa para el uso del correo electrónico institucional serán resueltas por las autoridades competentes del CECC.

La DTI si detecta que existe un peligro grave e inminente de la red institucional o cualquier anomalía que muestre indicios de incumplimiento de la normativa para el uso del correo electrónico institucional por parte del usuario, podrá suspender temporalmente o proceder a la revocación definitiva del correo institucional y lo pondrá de conocimiento ante las autoridades competentes del CECC para tomar las acciones disciplinarias correspondientes. El CECC no será responsable de la información perdida o repercusiones que pueda tener el usuario derivado de lo anterior.

ALTA DE LA CUENTA

La solicitud de alta de la cuenta de correo electrónico institucional debe realizarse a través del iCECC en el apartado “Institucional”, en la opción “Soporte técnico”, con base al siguiente criterio:

- Alumno de Colegio Cristóbal Colón: la dirección del área a la que pertenece el alumno.
- Alumno de Universidad: el jefe de área o coordinador del programa académico del alumno.
- Personal académico y/o administrativo: el jefe de área o jefe de departamento de pertenencia.

Para dar de alta una cuenta de correo electrónico institucional se requiere el nombre completo y un correo electrónico personal del titular.

Las cuentas para proyectos especiales o grupos se asignan previo acuerdo entre la DTI y el área solicitante.

A. Criterios para el nombre de usuario

La conformación del nombre del correo institucional se realiza con base a los siguientes criterios:

- **Alumno de Colegio Cristóbal Colón:** Se utiliza su matrícula y con el dominio correspondiente al área de colegio. Ejemplo 202490999@colon.mx

- **Alumno de Universidad:** Se utiliza su matrícula y con el dominio correspondiente al área de universidad. Ejemplo 202490999@ucc.mx

- **Personal académico y/o administrativo:** podrá asignarse con alguno de los siguientes criterios:

Se utiliza la primera letra del nombre y el primer apellido. Ejemplo para alguien llamado Juan Pérez sería: jperez@ucc.mx o jperez@colon.mx según corresponda. La DTI se reserva el derecho de asignar el nombre de cuenta que considere conveniente o en caso de existir una duplicidad de nombres.

Se utiliza el nombre del puesto o departamento de pertenencia. Ejemplo: juridico@ucc.mx

BAJA DE LA CUENTA

La baja de la cuenta de correo electrónico institucional implica la eliminación o desactivación de una cuenta de correo y puede darse bajo los siguientes supuestos:

- **Baja del alumno en el CECC**: El alumno ha sido dado de baja de colegio o universidad.
- **Terminación laboral del usuario académico y/o administrativo:** el usuario ha finalizado su relación laboral con el CECC.
- **Cambio organizativo del usuario:** El usuario ha cambiado de puesto o departamento y se le asigna un nuevo correo electrónico institucional dándose de baja el anterior.
- **Inactividad del usuario en la cuenta de correo electrónico:** La DTI se reserva el derecho de dar de baja las cuentas de correo electrónico institucional que no tengan actividad por un periodo continuo de 30 días calendario.
- **Incumplimiento de la normatividad para el uso del correo electrónico institucional:** El usuario ha incumplido en una o más de las obligaciones o condiciones descritas en el presente documento.

DISPOSICIONES PARA MENORES DE EDAD

Los alumnos menores de edad requieren una protección conforme al marco legal en México. Entre las medidas implementadas para su protección se incluyen:

- **Supervisión parental:** Los padres o tutores podrán solicitar informes acerca del uso que sus hijos hacen del correo institucional, en función de su deber de velar por su bienestar.
- **Monitoreo y protección:** el CECC implementará mecanismos de supervisión y monitoreo del uso del correo electrónico por parte de los menores de edad, para detectar y prevenir situaciones de acoso, ciberbullying o cualquier otra forma de abuso.

MODIFICACIONES A LA NORMATIVA

El CECC se reserva el derecho de modificar en cualquier momento, la presente normativa, entrando en vigor a partir de su publicación.

El usuario al hacer uso continuo del correo electrónico institucional acepta estar obligado a las disposiciones de la normativa para el uso del correo electrónico institucional. El desconocimiento de los presentes lineamientos no libera al usuario de las responsabilidades establecidas en ellos por el mal uso que hagan del correo electrónico institucional.

GLOSARIO DE TÉRMINOS

Baja. Acción que permite a un usuario dejar de recibir correos electrónicos de una lista de distribución o de un remitente específico.

Ciberdelincuentes. Persona que utiliza el correo electrónico como herramienta para cometer delitos informáticos.

Comportamiento sospechoso. Acciones que sugieren que una cuenta ha sido comprometida, utilizada para fines no autorizados o que el usuario ha sido víctima de un engaño.

Gmail. Herramienta principal para el envío y recepción de correos electrónicos oficiales. A través de esta plataforma, los usuarios tienen acceso a una dirección de correo que utiliza el dominio de la institución, lo que garantiza la autenticidad y oficialidad de las comunicaciones.

Google Calendar. Permite la planificación y coordinación de eventos, reuniones y citas importantes. Esta herramienta facilita la gestión del tiempo para todas las actividades educativas y administrativas.

Google Chat. Herramienta para la mensajería instantánea que puede ser utilizada para comunicaciones rápidas y colaborativas entre miembros de la comunidad educativa.

Google Docs, Sheets y Slides. Plataformas que permiten la creación y edición colaborativa de documentos, hojas de cálculo y presentaciones. Al ser herramientas colaborativas, es importante que los usuarios respeten la propiedad intelectual de los documentos y trabajen de manera ética y responsable.

Google Drive. Almacenamiento en la nube para documentos, carpetas y otros archivos. Permite compartir archivos con otros miembros de la institución o externos, facilitando la colaboración en proyectos y la distribución de materiales. Es importante que los usuarios gestionen adecuadamente los permisos de acceso para proteger la información confidencial.

Google Meet. Herramienta para la realización de videoconferencias y reuniones virtuales. Los usuarios deben utilizar Google Meet para clases, reuniones administrativas, conferencias y otros eventos que requieran la participación a distancia.

Google Workspace for Education (GWE). Paquete de herramientas de Google que permite a los centros educativos proteger sus entornos de aprendizaje, mejorar el impacto de la enseñanza y preparar al alumnado para el futuro.

iCECC. Portal web Institucional el cual tiene la finalidad de facilitar a los alumnos, docentes y empleados del CECC llevar a cabo distintos procesos, seguimiento y/o trámites de manera integrada y accesible, a través de una serie de recursos, funcionalidades, sistemas y servicios.

Información confidencial. Datos personales o privados que, si son revelados sin autorización, podrían causar daño o perjuicio a la persona o empresa involucrada.

Macro. Herramienta que permite automatizar tareas repetitivas al grabar una serie de acciones y luego ejecutarlas con un solo comando.

Mensajes HOAX. Son correos electrónicos falsos que intentan engañar a los usuarios para que crean información falsa, a menudo con fines maliciosos.

Mensajes SPAM. Son correos electrónicos no solicitados, a menudo comerciales, que se envían en masa a una gran cantidad de destinatarios.

Personal académico. Usuarios que laboran en el CECC y se dedican a la docencia, la investigación, la extensión y difusión de la cultura, y otras actividades académicas.

Personal administrativo. Usuarios que laboran en el CECC y se dedican a actividades administrativas y/o de operación.

Phishing. Técnica de ingeniería social consistente en el envío de correos electrónicos para suplantar la identidad de remitentes válidos.

Proyectos especiales. Un proyecto especial consiste en diseñar algo que permita resolver un problema o para realizar una innovación del CECC.

Suspensión. Acción de detener temporalmente la capacidad de una dirección de correo electrónico para enviar o recibir mensajes.

URL. (Localizador de Recursos Uniforme). Una URL es una dirección que es dada a un recurso único en la Web.

Usuario. Persona a quien se le asigna una cuenta de correo electrónico institucional pudiendo ser con alguno de los siguientes dominios: @colon.mx y/o @ucc.mx.

La presente normativa fue aprobada por

este **Centro de Estudios** el día **28 de abril de 2025**

y entrará en vigor a partir de su publicación

y difusión oficial por los medios institucionales.