



Reglamentos de acceso y uso de las herramientas en línea – correo y Microsoft Teams

Universidad de San José pone a disposición de los estudiantes el correo electrónico institucional con las diferentes herramientas tecnológicas internas paquetes de office en línea y Microsoft Teams. Adjuntamos los detalles del uso correcto de las herramientas y paquetes brindados para los estudiantes.

1. Uso del Correo Electrónico y Plataformas Teams

Es responsabilidad de los usuarios:

- 1.1.** Usar su cuenta con fines académicos.
- 1.2.** Usar un lenguaje apropiado en sus mensajes de correo como el uso de las plataformas de Microsoft Teams.
- 1.3.** al ingresar por primera vez el usuario es responsable de su contraseña por lo que se recomienda cambiar la contraseña y registrar los datos de recuperar acceso.
- 1.4.** El correo (e-mail) no tiene garantía de ser privado. Recuerde que existen personas que se dedican a tratar de "capturar" información que viaja a través de Internet, con spyware , troyanos y diferentes tipos de herramientas, por lo que se recomienda manejar un antivirus en sus equipos
- 1.6** En general, se aconseja al menos revisar el asunto (subject) antes de responder un mensaje y asegúrese que los mensajes que responda vayan dirigidos a usted.
- 1.7** Sea cuidadoso cuando envíe su correo. Hay algunas direcciones que pueden ir a un grupo, pero que parece ser la de una persona.
- 1.8** Ninguna persona está autorizada a solicitar sus credenciales, si tiene duda sobre alguna solicitud a su cuenta debe de enviar un correo a soporte@grupogach.com

- 1.9** El uso de la plataforma Microsoft Teams es para uso académico, reuniones entre estudiantes, el uso incorrecto de la plataforma será notificado a la coordinación académica para su respectivo proceso.

- 1.10** Cada usuario es responsable de los accesos y credenciales.

- 4.11.** No envíe ni conteste cadenas de correo o cualquier otro esquema de "pirámide" de mensajes.

- 4.12.** No use su cuenta para fines comerciales ni para inscribirse en ningún sitio web salvo que este sea para uso estrictamente académico.

- 4.13.** No se debe transmitir virus o programas de uso mal intencionado.

- 4.14.** Los usuarios no deben leer correo ajeno ni generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola. Ya que esto puede ser procesado legalmente.

- 4.15.** Se prohíben las violaciones de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.

- 4.16.** No se debe introducir software malicioso en la red o en los servidores (virus, worms, ráfagas de correo electrónico no solicitado, etcétera).

- 4.17.** No revele la clave o código de su cuenta, ni permita su uso a terceros

- 4.18.** El usuario debe evitar suscribirse a cualquier lista de correo que genere mensajes cuyo contenido no tenga que ver con las funciones académicas

- 4.19.** Se prohíbe el uso del correo electrónico con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil, sin importar el idioma, la periodicidad o tamaño del mensaje.

4.22. Se prohíbe el uso de comandos o programas o el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

4.23. Se prohíbe el envío de mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado ese tipo de material (e-mail spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).

4.24. Es obligación de los usuarios reportar al personal del departamento de T.I sopORTE@usanjosecr.com cualquier tipo de irregularidad o abuso de estos servicios, para evitar que esto le vuelva a suceder.

4.25. El usuario se asegurará de no responder a todas las personas cuando se envíen comunicados generales o para un grupo específico de personas, a excepción de que esta sea la finalidad de la respuesta.

4.26. El Departamento de T.I se reserva el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para su seguridad, lo que no incluye acceso al contenido de los correos.

4.28. Si se requiere realizar una auditoría de ingreso, a nivel del sistema se aplica una auditoría de ingreso por dirección de IP, días de ingreso registro. Si un usuario ingreso con una Cuenta de otro estudiante sin autorización las direcciones de IP quedan almacenadas por un periodo de 15 días