COMPATIBILIDAD Y SEGURIDAD

PLATAFORMA DE CORREO

TIGO

Compatibilidad

La compatibilidad con sistemas operativos y navegadores está restringida por las Políticas de ciclo de vida de proveedores externos; esos productos serán compatibles con una versión de Zimbra como aplicación de aplicación de correo, recomendamos encarecidamente se utilice las últimas versiones de los sistemas operativos y navegadores para garantizar el acceso a las actualizaciones de seguridad.

Consola de administración

Se admiten las siguientes combinaciones de sistema operativo/navegador. Otras versiones podrían funcionar mas no serían compatibles con algunas características.

Windows 8.1
Windows 10
Windows 11

Con la última versión estable de:

Microsoft Edge para Windows 10
Firefox
Google Chrome

MacOS 10.12 o posterior con la última versión estable de:

Firefox
Safari
Google Chrome

Aplicación web versión Classic y modern

Se admiten las siguientes combinaciones de sistema operativo/navegador. Otras versiones podrían funcionar mas no serían compatibles con algunas características.

Windows 8.1
Windows 10
Windows 11

Con la última versión estable de:

Microsoft Edge para Windows 10
Firefox

Google Chrome

MacOS 10.12 o posterior con la última versión estable de:

Firefox
Safari
Google Chrome

Linux (Red Hat, Ubuntu, Fedora o SUSE) con la última versión estable de uno de los siguientes:

Firefox
Google Chrome

Configuración puertos seguros:

Se recomienda configurar el acceso a las cuentas de correo utilizando los protocolos seguros para que la información sea cifrada

Hosts Públicos	Puerto seguro	Protocolo
smtp.une.net.co	465 (SSL)	SMTPS
imap.une.net.co	993 (SSL)	IMAPS
pop.une.net.co	995 (SSL)	POPS
webmail.une.net.co	443	HTTPS

Protección basada en Antispam:

Servicio antispam de FortiGuard
- Reputación global del remitente
- URI de spam y phishing y direcciones de correo electrónico
- Spam Object checksums
- Reglas heurísticas dinámicas

Protección Outbreak
Lista gris para direcciones IPv4, IPv6 y cuentas de correo electrónico (Greylisting)
Reputación local del remitente (basada en IPv4, IPv6 y End Point ID-based)
Análisis de comportamiento (Behavioral Analysis)
Inspección profunda del encabezado del correo electrónico (Deep Email Header Inspection)
Acción flexible y perfiles de notificación
URI de spam de terceros y listas negras en tiempo real (SURBL / RBL)

Chequeo de reputación de ip´s en múltiples RBLs [DNSBL]
Categoría completa FortiGuard URL Filtering (FortiGuard URL Filtering)
Cuarentena
Escaneo PDF y Análisis de Imagen
Listas negras y con excepciones a nivel global, de dominio y de usuario (Black/White Lists)
Filtrado bayesiano (Bayesian Statistic Filtering)
Detección de boletines y boletines sospechosos (Newsletter detection)

Protección basada en Antivirus:

Servicio FortiGuard Antivirus
Acciones de cuarentena, reempaquetado, reemplazo y monitoreo
Escaneo de archivos anidados (Nested Archive Scanning)
Detección de malware
Emulación de código a bordo

Protección basada en contenido

Filtrado basado en diccionario
Diccionarios predefinidos HIPAA, GLBA y SOX
Filtrar por tipo de archivo adjunto y extensiones potencialmente inseguras o ejecutables
Filtrado de palabras prohibidas

Protección basada en Sistema:

Inspección para mensajes entrantes y salientes
Protección de denegación de servicio
Protección Ataque de dirección del destinatario
Protección contra epidemias de Spam
Límite de velocidad de mensajes entrantes y salientes
Cifrado de dirección del remitente falsificado
Cifrado basado en identidad para entrega push / pull de mensajes cifrados
Verificación inversa de DNS (Anti-Spoofing)
Inspección por usuario utilizando atributos LDAP en una base por política (dominio)
Cumplimiento de RFC por correo electrónico
Mantiene la lista de reputación de la remitente local basada en:
- Marco de políticas del remitente (SPF)
- Correo identificado claves de dominio (DKIM)
- Soporte para protocolos criptográficos fuertes, incluidos HTTPS, SMTPS, SSH, IMAPS y POP3S

Consejos de uso y seguridad en tu correo electrónico

- Si no conoces la procedencia de un correo electrónico y desconfías del remitente y su contenido, llévalo a la carpeta de SPAM.

- La técnica de Phishing es una práctica muy habitual entre los cibercriminales que afecta cada vez a más usuarios, consiste en suplantar la identidad para obtener un beneficio económico. Evita entregar tus datos personales, bancarios o contraseñas a través de correos electrónicos cuando alguien te los esté solicitando.

- Utiliza diferentes contraseñas para las cuentas de correo electrónico a las que tienes acceso, y modifica las contraseñas con cierta frecuencia.

- ¡Cuidado con los archivos adjuntos! Si desconoces la procedencia del remitente procura no abrirlos y menos cuando tengan la extensión .exe

- No abras correos con ofertas, regalos o falsas promociones del tipo: “Te ha tocado un viaje a Nueva York con todos los gastos pagados”.

- Borra el historial, la caché de tu navegador periódicamente y evita marcar la opción de guardar contraseñas.

- Pasa el cursor del ratón sobre los enlaces del email antes de abrirlos, para que puedas comprobar si la dirección URL es correcta.

- Asegúrate de cerrar la sesión de correo cada vez que terminas de trabajar.

- Cuidado con las redes wifi-públicas (normalmente sin contraseña). Estás expuesto a que alguien esté capturando información de todos tus datos personales o esté observando tu correo electrónico.

- Utiliza la copia oculta BCC o CCO cuando envíes correos a varias personas, de esta manera se ocultarán sus correos a los demás.

- Utiliza una solución de correo electrónico con cifrado para controlar toda tu información confidencial. Configura tu cuenta de correo utilizando los puertos seguros, pídele ayuda a soporte técnico.

- No publiques tu correo electrónico en sitios web, foros, redes sociales o espacios donde se comparte contenido, ya que estos se han convertido en los principales escenarios de acción de los envíos masivos de spam.

- Ten actualizados tus programas antivirus y tu sistema operativo. En las actualizaciones, muchas veces se incluyen mejoras de seguridad. Con tu software actualizado cerrarás posibles puntos de entrada que ya se conozcan.

- Por otro lado, también es importante llevar a cabo un periodo de formación y educación del usuario en cuanto a seguridad en Internet se refiere, puesto que todo el mundo está capacitado para enviar un correo electrónico, pero no todas las personas saben protegerse de las amenazas no deseadas que hay presentes en la red.