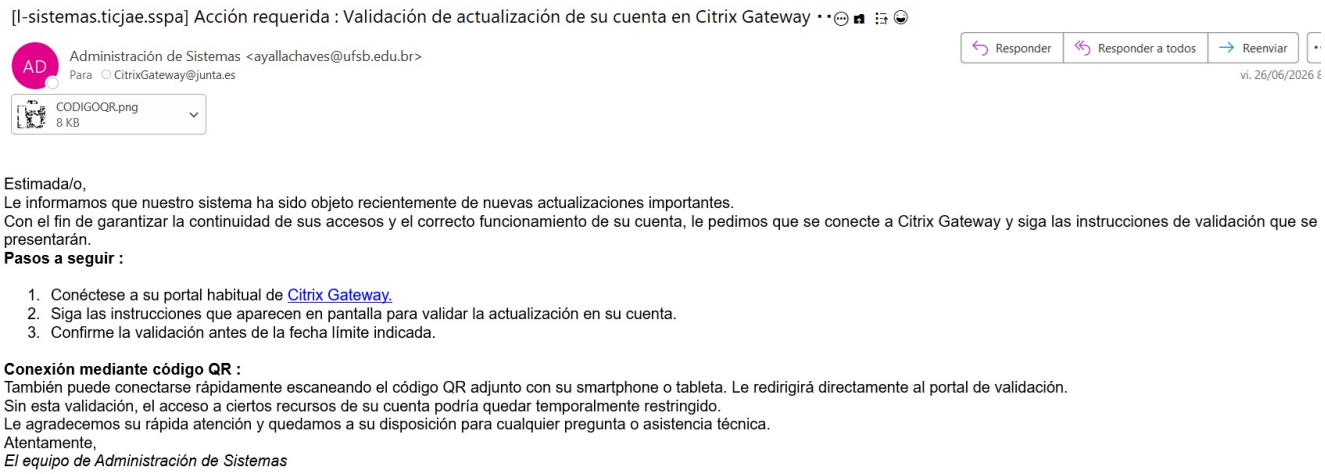
Campaña activa de correos fraudulentos: Mantente alerta

Estimados compañeros:

Os informamos que se ha detectado una campaña de **correos fraudulentos** (*phishing*) con códigos QR dirigida al personal del Servicio Andaluz de Salud. El **objetivo** de estos mensajes es **obtener de forma ilícita** las credenciales corporativas (**usuario y contraseña**).

El **aspecto del mensaje** es el siguiente:


[I-sistemas.ticjae.sspa] Acción requerida : Validación de actualización de su cuenta en Citrix Gateway

AD Administración de Sistemas <ayallachaves@ufsb.edu.br>
Para CitrixGateway@junta.es

Responder | Responder a todos | Reenviar

vi. 26/06/2026

CODIGOQR.png
8 KB

Estimada/o,
Le informamos que nuestro sistema ha sido objeto recientemente de nuevas actualizaciones importantes.
Con el fin de garantizar la continuidad de sus accesos y el correcto funcionamiento de su cuenta, le pedimos que se conecte a Citrix Gateway y siga las instrucciones de validación que se presentarán.
Pasos a seguir :

1. Conéctese a su portal habitual de Citrix Gateway.
2. Siga las instrucciones que aparecen en pantalla para validar la actualización en su cuenta.
3. Confirme la validación antes de la fecha límite indicada.

Conexión mediante código QR :
También puede conectarse rápidamente escaneando el código QR adjunto con su smartphone o tableta. Le redirigirá directamente al portal de validación.
Sin esta validación, el acceso a ciertos recursos de su cuenta podría quedar temporalmente restringido.
Le agradecemos su rápida atención y quedamos a su disposición para cualquier pregunta o asistencia técnica.
Atentamente,
El equipo de Administración de Sistemas

Es previsible que este tipo de intentos continúen en los próximos días, por lo que os pedimos que extreméis las precauciones. Para ello, os recordamos algunas **recomendaciones básicas de seguridad** ante estos casos:

1. **Analiza el contexto del mensaje.** Sospecha de solicitudes urgentes o poco habituales sin contrastarlo por otras vías.
2. **Revisa siempre la dirección del remitente.** Desconfía de mensajes que provengan de cuentas no corporativas o con dominios inusuales.
3. **No respondas jamás** a mensajes sospechosos.
4. **No escanees códigos QR ni abras enlaces ni archivos adjuntos** de remitentes desconocidos o que te generen dudas.
5. **No introduzcas tus credenciales** corporativas **desde enlaces o QR.**
6. Recuerda que **el SAS nunca solicita contraseñas por correo ni** mediante códigos **QR**.
7. **Accede siempre a las aplicaciones y sistemas corporativos** exclusivamente **desde** los **enlaces y sitios oficiales habituales**.
8. **Avisa inmediatamente**. Notifica estos mensajes fraudulentos. Consulta cómo hacerlo aquí: Consulta ayudaDIGITAL-AvisarPhishing

Muchas gracias por vuestra colaboración.

Comunicación

Dirección General de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud