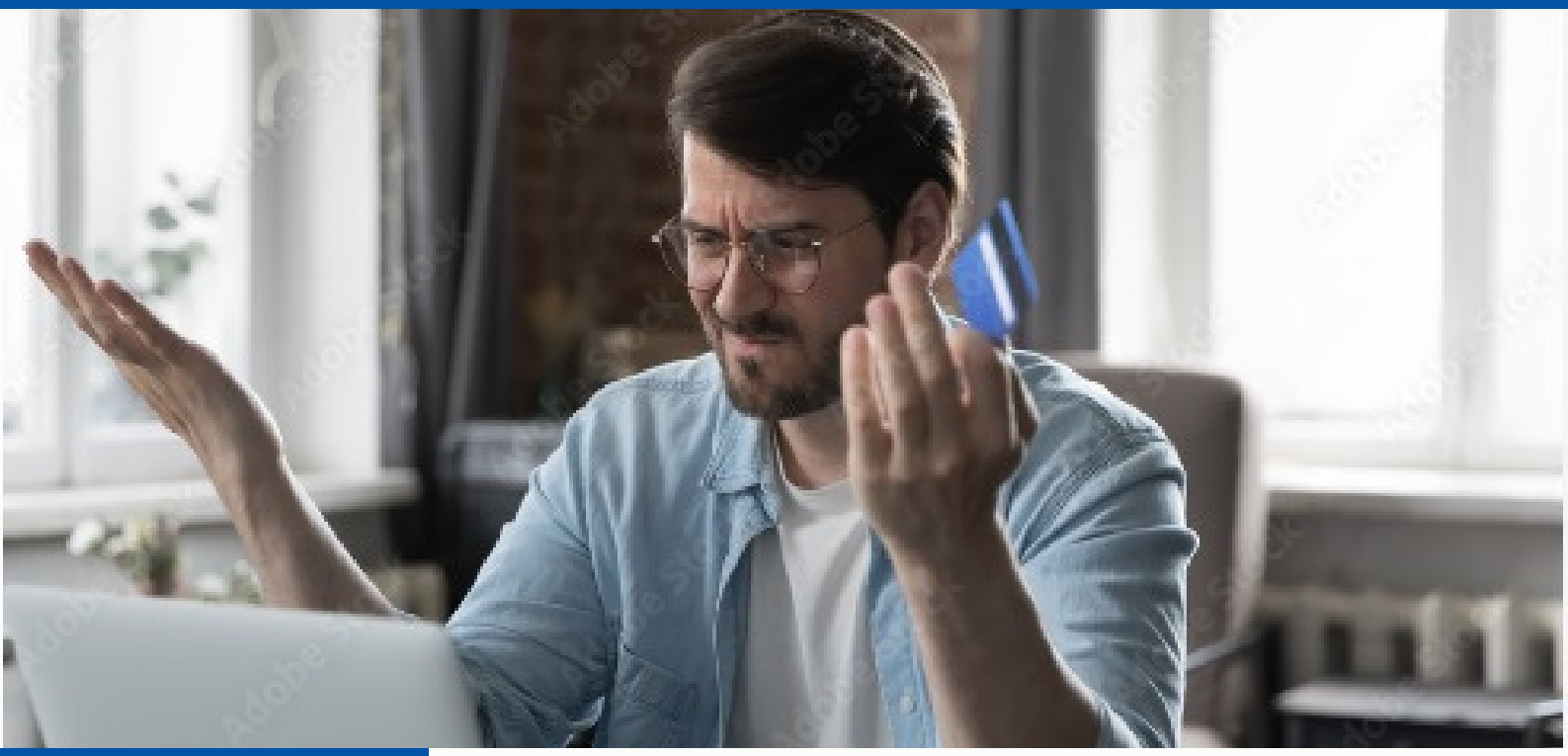
SUBPROCESO DE SEGURIDAD INFORMÁTICA

Boletín Número 10
Agosto - Septiembre 2022

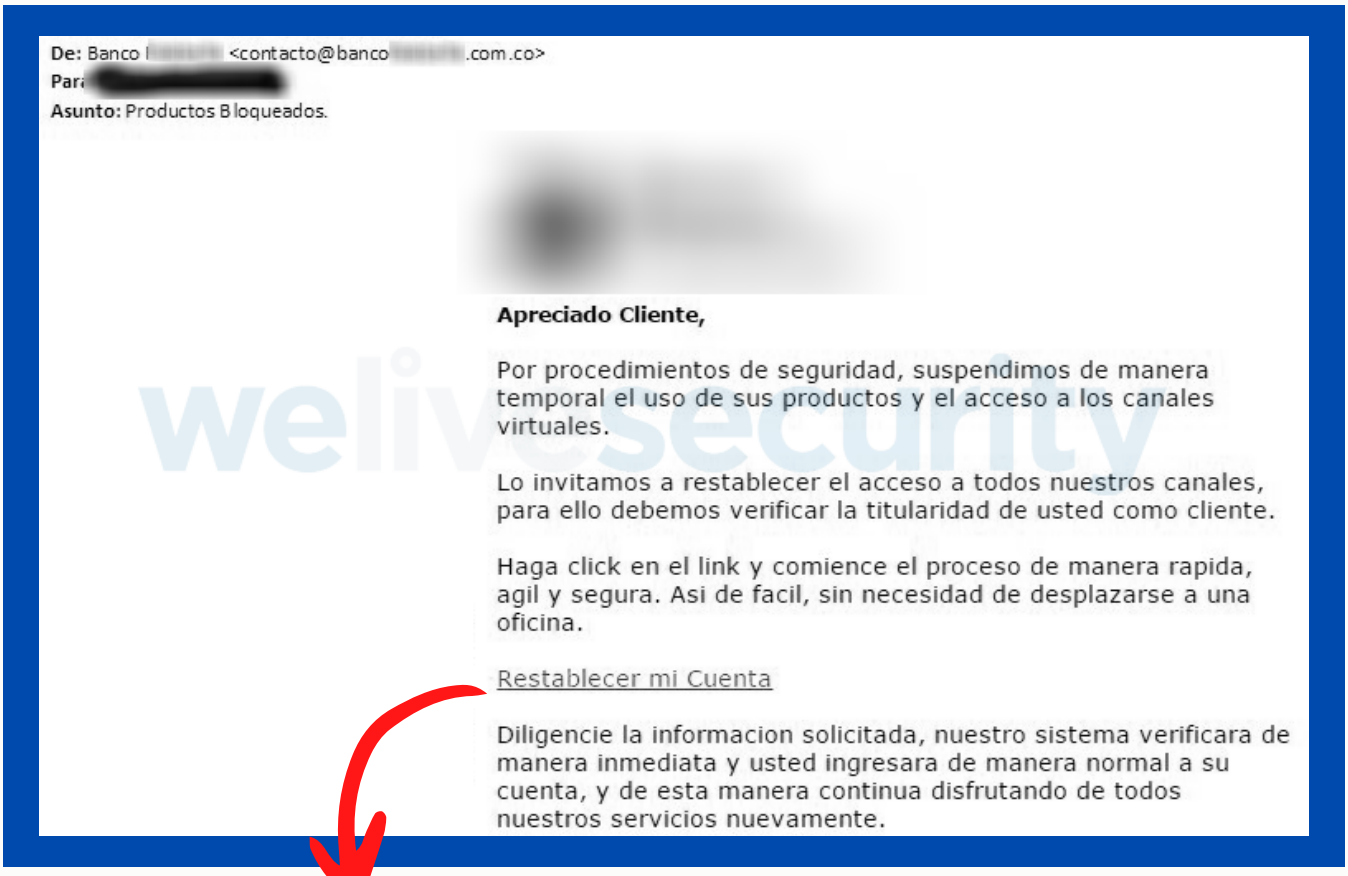


Analicemos: "Tienes pensado pagar la compra del mercado con su tarjeta, y se entera de que estas sin fondos suficientes, al averiguar: ¡el dinero de su cuenta ha sido robado¡

Lo anterior es algo muy común y sucede a diario.

Un clic "inocente" toda su información robada

La suplantación de entidades o "Phishing" es un método de engaño que busca hacer compartir su información personal como usuarios y contraseñas de las tarjetas de crédito, cuentas de correo u otros datos personales. Los ciber-delincuentes obtienen esta información mediante el envío de correos electrónicos fraudulentos con la imagen o información de una institución de confianza trasladando a la persona a un sitio web falso para capturar estos datos y proceder a robar.



" El correo electrónico tiene un contenido bastante convincente incluso a amenazante que incita al usuario a abrir un archivo o llenar un formulario"

¿Cómo funciona?

Amenaza constante: El "phisher" lanza el ataque, enviando masivamente correos electrónicos a diferentes destinatarios, utilizando frases para captar la atención del destinatario.

Descuido de datos: El destinatario recibe el mensaje en su correo. Con un texto le solicita al usuario ingresar a una URL con una imagen institucional, registrar datos personales, incluso registrar la clave anterior para proceder con el supuesto cambio.

Acceso "permitido": El atacante ya tiene su contraseña real, en algunos casos cuando damos clic al enlace puede instalarse un malware en su equipo, este brindará acceso al atacante a sus archivos (documentos, fotos, cámaras, micrófonos, e impresoras todos los dispositivos conectados al equipo violando completamente su privacidad.

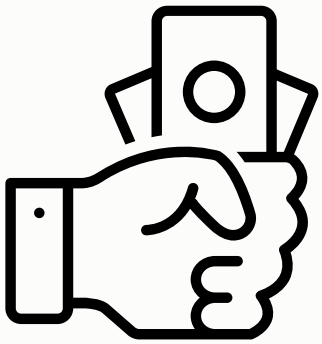
Frases comunes para identificar un Phishing

Acceda al siguiente **enlace** para conocer el estado de su deuda con el banco.

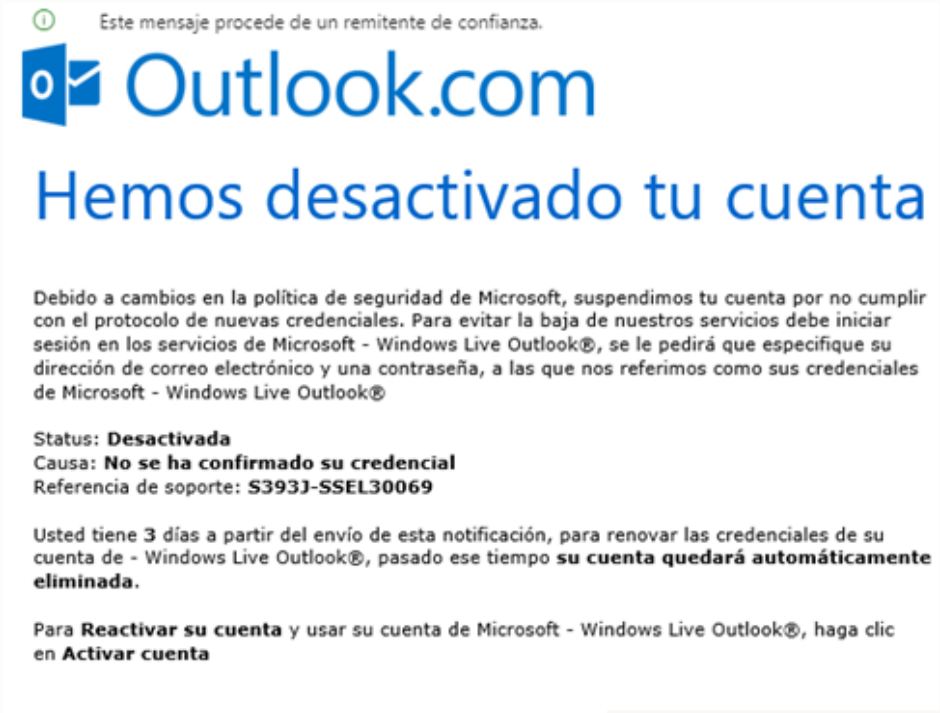
Evite sanciones, revise por favor el **documento anexo.**

Presione **clic aquí** para **descargar** su estado de cuenta.

Tiene una multa de tránsito o una obligación fiscal en la DIAN lista para ser ejecutada jurídicamente, clic para conocer más.



Ejemplos reales y como detectarlos



Este mensaje procede de un remitente de confianza.

Outlook.com

Hemos desactivado tu cuenta

Debido a cambios en la política de seguridad de Microsoft, suspendimos tu cuenta por no cumplir con el protocolo de nuevas credenciales. Para evitar la baja de nuestros servicios debe iniciar sesión en los servicios de Microsoft - Windows Live Outlook®, se le pedirá que especifique su dirección de correo electrónico y una contraseña, a las que nos referimos como sus credenciales de Microsoft - Windows Live Outlook®

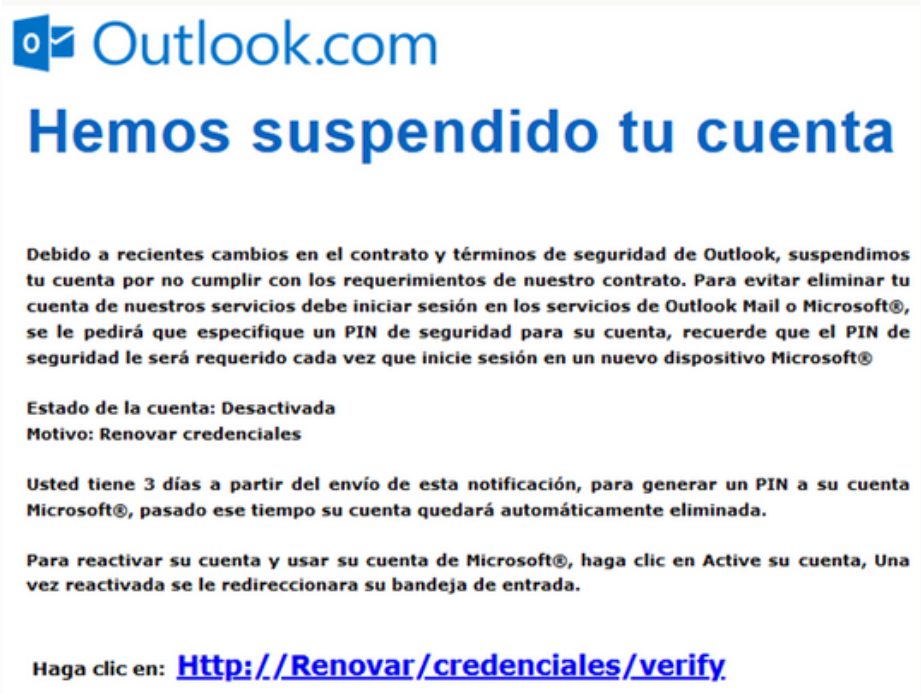
Status: **Desactivada**
Causa: **No se ha confirmado su credencial**
Referencia de soporte: **S393J-SSEL30069**

Usted tiene **3** días a partir del envío de esta notificación, para renovar las credenciales de su cuenta de - Windows Live Outlook®, pasado ese tiempo **su cuenta quedará automáticamente eliminada.**

Para **Reactivar su cuenta** y usar su cuenta de Microsoft - Windows Live Outlook®, haga clic en **Activar cuenta**

1. Siempre recibirás un correo llamativo que busca atraer su atención.

2. Revisa el remitente. Los correos institucionales siempre llegan de cuentas oficiales @empresa.edu.co.



Outlook.com

Hemos suspendido tu cuenta

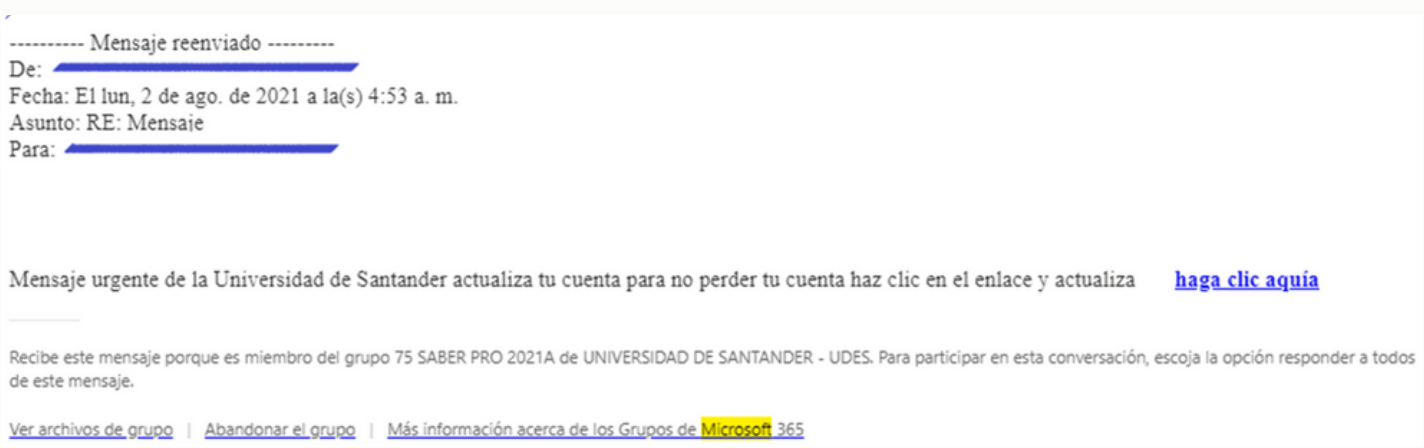
Debido a recientes cambios en el contrato y términos de seguridad de Outlook, suspendimos tu cuenta por no cumplir con los requerimientos de nuestro contrato. Para evitar eliminar tu cuenta de nuestros servicios debe iniciar sesión en los servicios de Outlook Mail o Microsoft®, se le pedirá que especifique un PIN de seguridad para su cuenta, recuerde que el PIN de seguridad le será requerido cada vez que inicie sesión en un nuevo dispositivo Microsoft®

Estado de la cuenta: Desactivada
Motivo: Renovar credenciales

Usted tiene 3 días a partir del envío de esta notificación, para generar un PIN a su cuenta Microsoft®, pasado ese tiempo su cuenta quedará automáticamente eliminada.

Para reactivar su cuenta y usar su cuenta de Microsoft®, haga clic en Active su cuenta, Una vez reactivada se le redireccionara su bandeja de entrada.

Haga clic en: Http://Renovar/credenciales/verify



---------- Mensaje reenviado ---------
De: [redacted]
Fecha: El lun, 2 de ago. de 2021 a la(s) 4:53 a. m.
Asunto: RE: Mensaje
Para: [redacted]

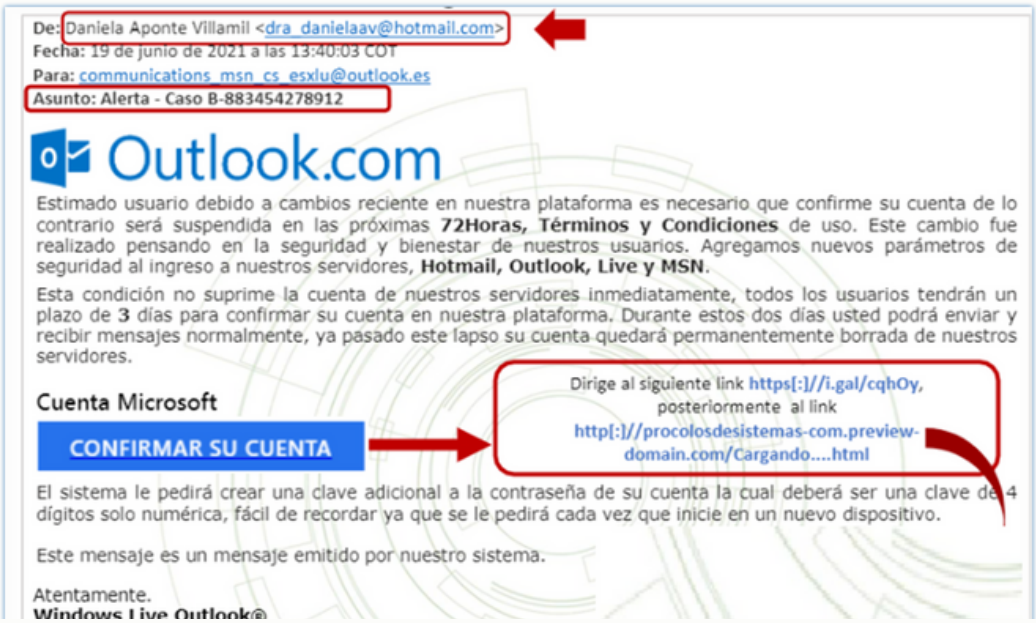
Mensaje urgente de la Universidad de Santander actualiza tu cuenta para no perder tu cuenta haz clic en el enlace y actualiza haga clic aquía

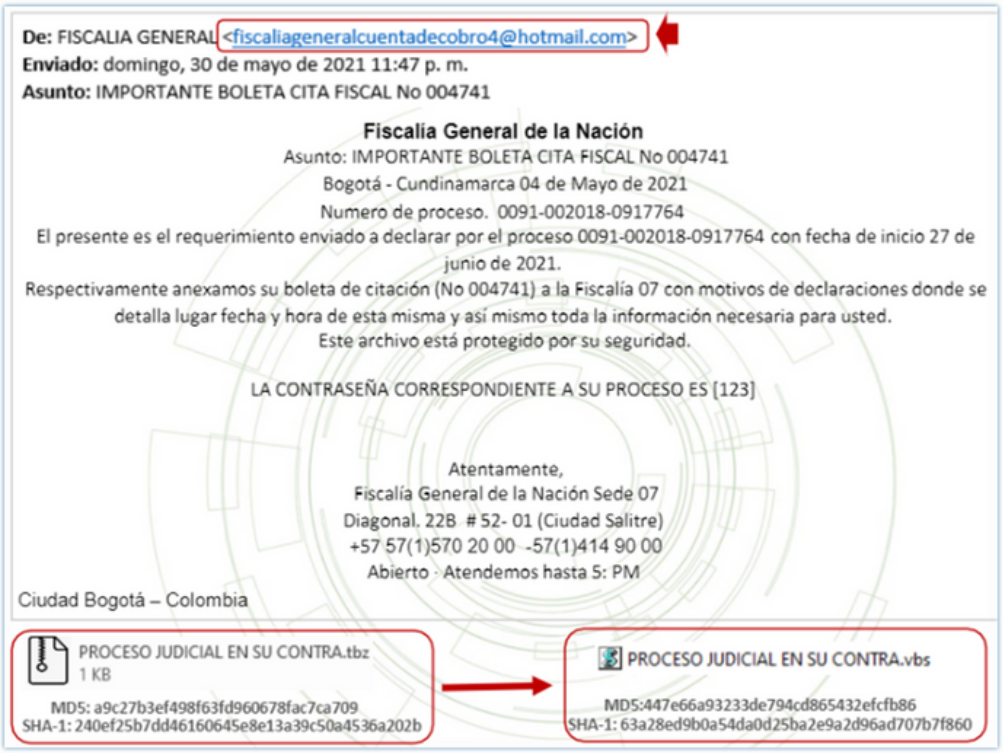
Recibe este mensaje porque es miembro del grupo 75 SABER PRO 2021A de UNIVERSIDAD DE SANTANDER - UDES. Para participar en esta conversación, escoja la opción responder a todos de este mensaje.

Ver archivos de grupo | Abandonar el grupo | Más información acerca de los Grupos de Microsoft 365

Ejemplos reales y como detectarlos

3. Las entidades de gobierno o privadas no suelen utilizar correos @hotmail, @live, @gmail. Si tiene duda del origen pueden contactar a la empresa que menciona ser remitente del correo.





4. No descargues archivos a su equipo personal o laboral sin antes verificar el origen del correo, de igual manera no relacione sus datos personales en enlaces a páginas que llegan por correo que le generen duda.

ACCIONES PREVENTIVAS

Remitentes confiables: Ninguna entidad solicita datos personales mediante correo electrónicos. Es importante revisar el correo de origen el cual debe ser de una cuenta oficial.

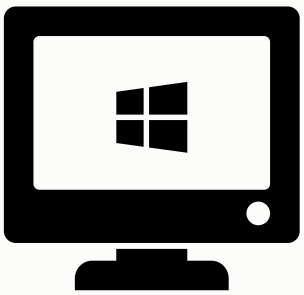
Enlace sospechoso: No abra el enlace desde su correo electrónico, si tiene dudas cópielo y ábralo desde su navegador.

Verificar: Si el correo le genera dudas comuníquese con la línea de atención del remitente. para ello copie la dirección de origen y reportela.

No des Clic: Si el correo es dudoso no des clic, reporta al área de seguridad informática.

Revisa tus cuentas: de manera constante procede a actualizar tus datos de correo en las cuentas bancarias.

Actualiza de manera constante el sistema operativo de tu equipo y el antivirus.



"Se parte de la solución, protege tu información personal y la de tu empresa"

¡Recueda¡

¡SI PRESENTAS DUDAS O ALGUNA SITUACIÓN SOSPECHOSA CONTÁCTANOSi

Subproceso de Seguridad informática UDES

- En Bucaramanga:
  Correo: seguridadinformatica@udes.edu.co
  Teléfono: (607) 6516500 Ext 1005 - 1001
- En Valledupar
  Correo: lortiz@valledupar.udes.edu.co
  Teléfono: (605) 5730073 Ext 129
- En Cúcuta:
  Correo: wpena@udes.edu.co
  Teléfono: (607) 5748717 Ext 4196