Boletín 14

Abril-Junio

Universidad de Santander UDES

VIGILADA MINEDUCACIÓN | SNIES 2832

ACREDITACIÓN INSTITUCIONAL ALTA CALIDAD UDES MIN EDUCACIÓN

POLÍTICAS INSTITUCIONALES DE SEGURIDAD INFORMÁTICA PARTE 2

Acceso a red o Uso de internet

Cuentas de Usuario (su uso y privacidad)

Acceso a red o uso de internet

No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

No está permitido el acceso y el uso de servicios P2P como ares, Kazaa, emule y otros similares, que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias de la Universidad de Santander.

Está prohibido descargar de manera fraudulenta archivos protegidos por la autoridad intelectual de derecho de autor, cualquier descarga será responsabilidad total de la persona que realiza la misma y vendrá sujeto a sanciones.

El área de Seguridad informática realizará el monitoreo permanente de: tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros.

Acceso a red o uso de internet

Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilicitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

El uso de internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la Universidad de Santander.

Para la conexión a las aplicaciones o servidores se debe realizar por comunicaciones seguras como protocolos SFTP, SSH, HTTPS.

Para realizar conexión remota a los equipos corporativos se debe efectuar por mecanismos seguros como VPNS (ipsec o SSL).

Cuentas de Usuario (su uso y privacidad)

Todos los accesos a los diferentes sistemas de la UDES, son controlados mediante credenciales de usuario y contraseña, las cuales son de responsabilidad y uso exclusivo del usuario al cual han sido asignadas.

Si se requiere hacer uso de los sistemas institucionales, se solicitará formalmente al administrador del sistema correspondiente, las credenciales de acceso.

La longitud mínima de caracteres permisibles en una contraseña se establece en 8 caracteres y la longitud máxima de caracteres permisibles en una contraseña se establece en 16 caracteres, siendo esta una combinación alfanumérica, mayúscula y minúscula.

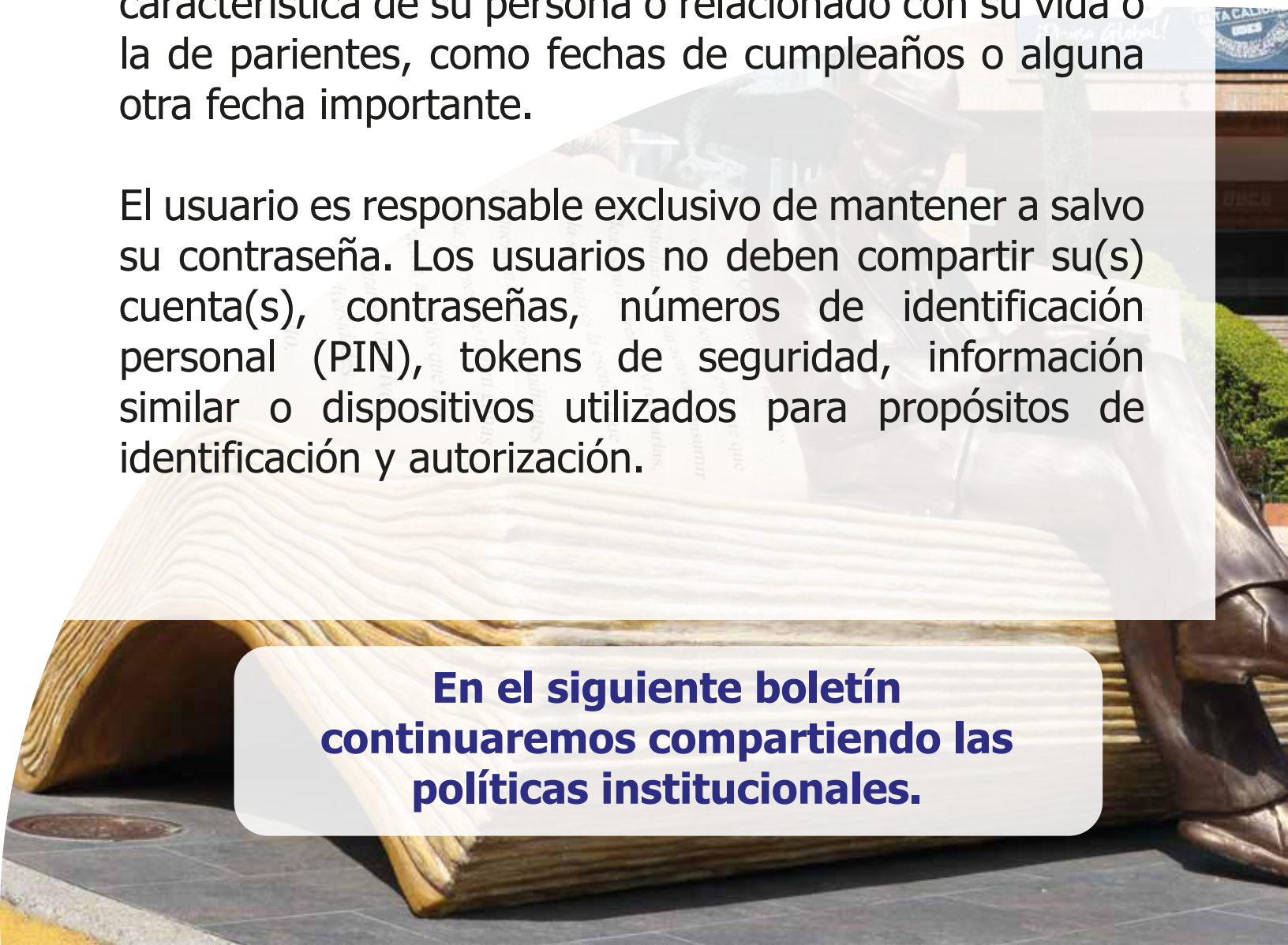
Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta sea guardada en un lugar seguro.

Cuentas de Usuario (su uso y privacidad)

El subproceso de seguridad informática velará por la privacidad de las comunicaciones personales, para lo cual monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes.

El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.

El usuario es responsable exclusivo de mantener a salvo su contraseña. Los usuarios no deben compartir su(s) cuenta(s), contraseñas, números de identificación personal (PIN), tokens de seguridad, información similar o dispositivos utilizados para propósitos de identificación y autorización.



En el siguiente boletín continuaremos compartiendo las políticas institucionales.

Contáctanos

Si presentas dudas o detectas alguna situación sospechosa puedes comunicarte con el subproceso de seguridad informática UDES:

Bucaramanga
seguridadinformatica@udes.edu.co
Teléfono (607) 6516500 ext. 1005-1001

Valledupar
lortiz@valledupar.udes.edu.co
Teléfono: (605) 5730073 ext. 129

Cúcuta
wpena@udes.edu.co
Teléfono: (607) 5748717 ext. 4196