

Ing. Bonilla

Coordine para dar cumplimiento a estas sugerencias.



25-07-17



REPUBLICA DE HONDURAS  
GOBIERNO DE ESTADO EN EL DESPACHO DE SEGURIDAD  
DIRECCION GENERAL DE LA POLICIA NACIONAL  
DIRECCION NACIONAL DE TELEMATICA  
CENTRO DE SEGURIDAD DE LA INFORMACION

Tegucigalpa M.D.C. 21 de JULIO de 2017

INSPECTOR DE POLICIA

**RONALD AUGUSTO PINEL MONCADA**

JEFE DEL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACION  
SU OFICINA

*Por este medio con toda subordinación y respeto me permito saludarle deseándole muchas bendiciones en su vida y sus funciones diarias.*

*El motivo de la misma es para remitirle el informe sobre las anomalías encontradas en el firewall (Sonic Wall 5600), que es el que brinda la seguridad a los servidores en el que se encuentra el sistema NACMIS y Balística, en el cual se pudieron observar varias anomalías que ponen en riesgo la seguridad de la información de dichos sistemas, a continuación, se detalla las diferentes anomalías encontradas:*

- 1. Según el departamento de conectividad, fueron borrados ciertos usuarios que se encontraban en el sistema en fecha anterior, y al verificar el día miércoles 19 de julio de 2017, se encuentra que esos usuarios fueron creados nuevamente.*
- 2. Se encontraron usuarios los cuales pertenecen a personas fuera de la institución como ser: **Luf ergo y Flores. Joel** de Luf ergo y franco (Instructor de Sonic Wall, Consultor, El Salvador), por lo cual el departamento de Conectividad procedió a eliminarlos.*
- 3. Se eliminaron los siguientes usuarios: **EFunezO**, **eperezbonett** (asesor de la embajada, con privilegios de administrador), **juanmaaguilar** (Sub Comisionado Aguilar Godoy, con privilegios de administrador)*
- 4. Se encontró a varios usuarios que no están identificados, lo cual tiene que ser obligatorio por motivos de seguridad e identificación del*

personal de la institución: **cfigueroaq**, **DanCoepol**, **dferreras** y se procedió a eliminar el usuario **Helmich\_x**.

5. Se quitó privilegios de administrador de los usuarios: **Dell.Support** y **MySonicWall**, dejándolos con privilegios básicos donde no pueden efectuar ningún cambio en la configuración.

#### *Recomendaciones*

- Se necesita que el personal que administraba este equipo, proporcione la contraseña del usuario administrador (admin) que viene de fábrica, al departamento de Conectividad para realizar el cambio correspondiente.
- La creación de un usuario de lectura asignado al departamento de Seguridad de la información para la supervisión recurrente de los cambios realizados en la configuración del equipo.
- El usuario de administrador global solo debe ser manejado por una sola persona la cual tendrá la contraseña y no se hará uso de este usuario ya que al usarlo no queda registro de las configuraciones que este hizo.
- Proceder a realizar auditorias de este sistema frecuentemente para monitorear la actividad y configuraciones que hacen los usuarios.

*Sin más que informar respetuosamente.*

***DIOS***

***PATRIA***

***SERVICIO***

Carlos Lima

Stephanie Romero

***Ing. y técnico en seguridad***

***Técnico en seguridad***

### Eliminación de usuarios

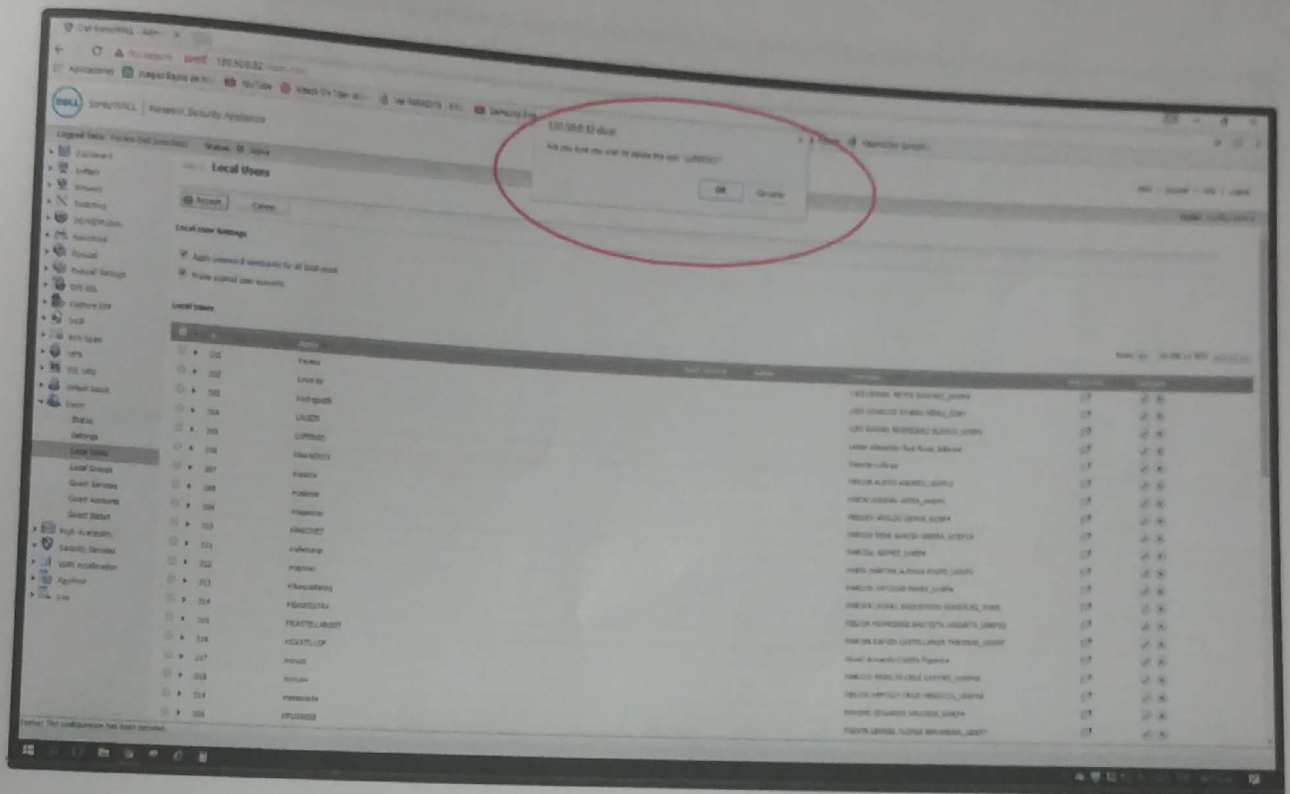
The screenshot shows the Windows Security application window. On the left, the 'Local Users' section is selected under 'Users & Groups'. The main pane displays a list of local users. A red circle highlights a confirmation dialog box that appears when attempting to delete a user. The dialog box contains the text: 'Are you sure you want to delete the user 'Flavio12'?' and has 'OK' and 'Cancel' buttons. The background list of users includes columns for Name, Type, Status, and Location.

Name	Type	Status	Location
Administrator	Administrator	Enabled	Local
Guest	Guest	Disabled	Local
Flavio12	User	Enabled	Local
...	...	...	...

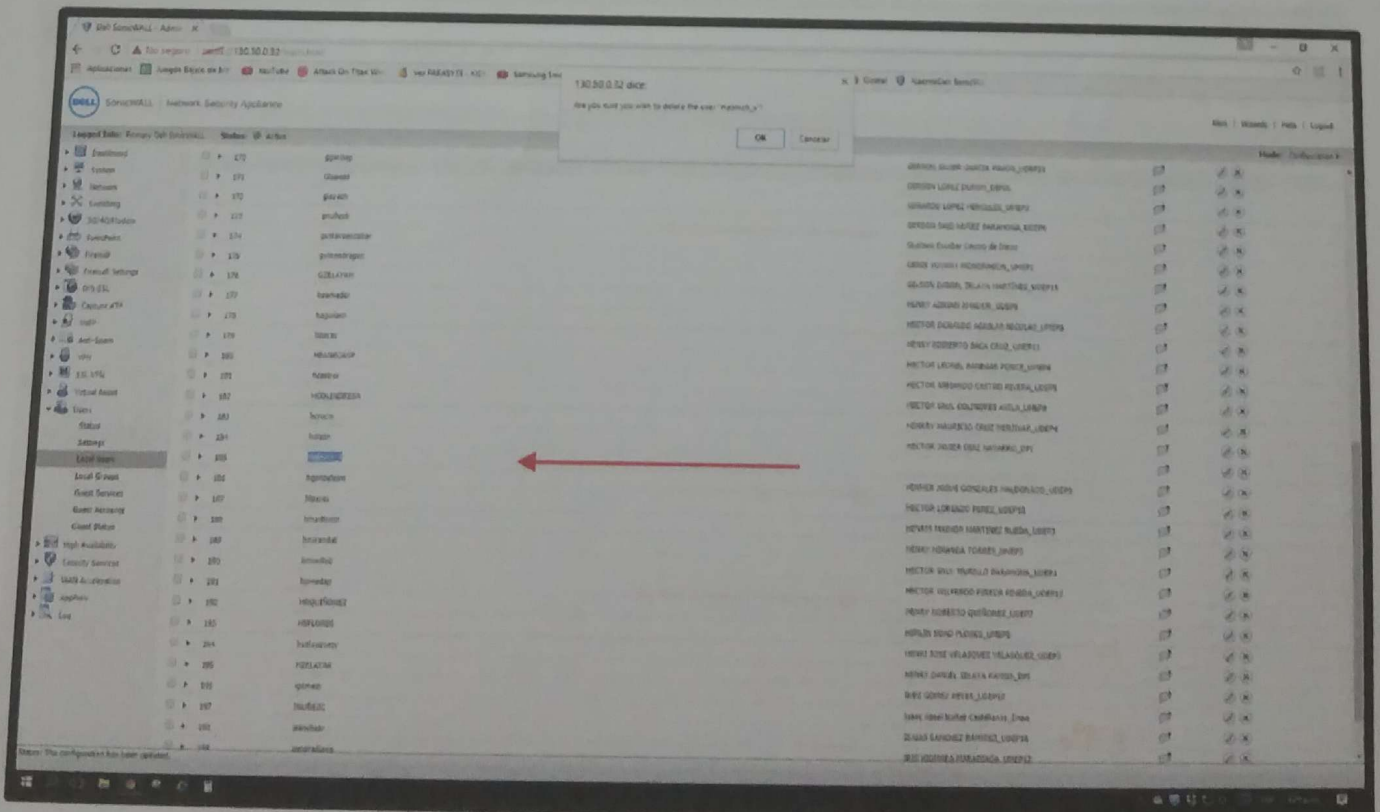
The screenshot displays a remote desktop session of a Windows 10 machine. The taskbar at the top shows several open applications, including a file explorer, VLC media player, YouTube, and a web browser. The active window is a web browser displaying a network security application interface. A red circle highlights a dialog box in the center of the screen, which contains the text: "Are you sure you wish to delete the user 'apersonal'?" with "OK" and "Cancel" buttons. The background interface shows a sidebar on the left with navigation options like "Dashboard", "Users", "Groups", and "Settings". The main area displays a list of users, and the right sidebar shows a list of users with checkboxes for selection. The browser's address bar shows the URL "130.50.0.12:4040".



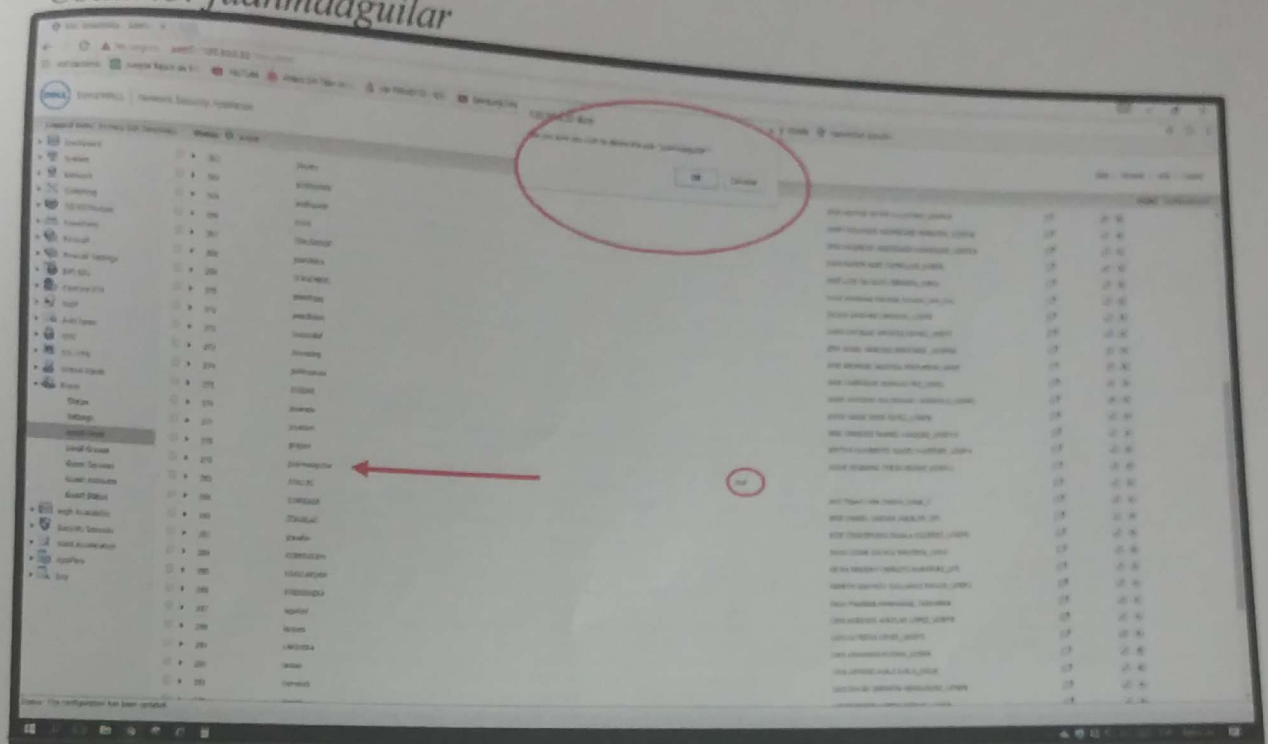
Usuario: LUFERGO



Usuario: Helmich\_x



Usuario: juanmaaguiar



Usuarios sin identificación

Usuario: cfigueroaq, DanCoepol y dferreras

