Ing Bonilla

Coordine para dar cumplimento a estas sugerencias.

25-07-17

REPUBLICA DE HONDURAS
E ESTADO EN EL DESPACHO DE SEGURIDAD
N GENERAL DE LA POLICIA NACIONAL
CCION NACIONAL DE TELEMATICA
NTO 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:* ***Lufergo*** *y* ***Flores.Joel*** *de Lufergo 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

Ing. y técnico en seguridad

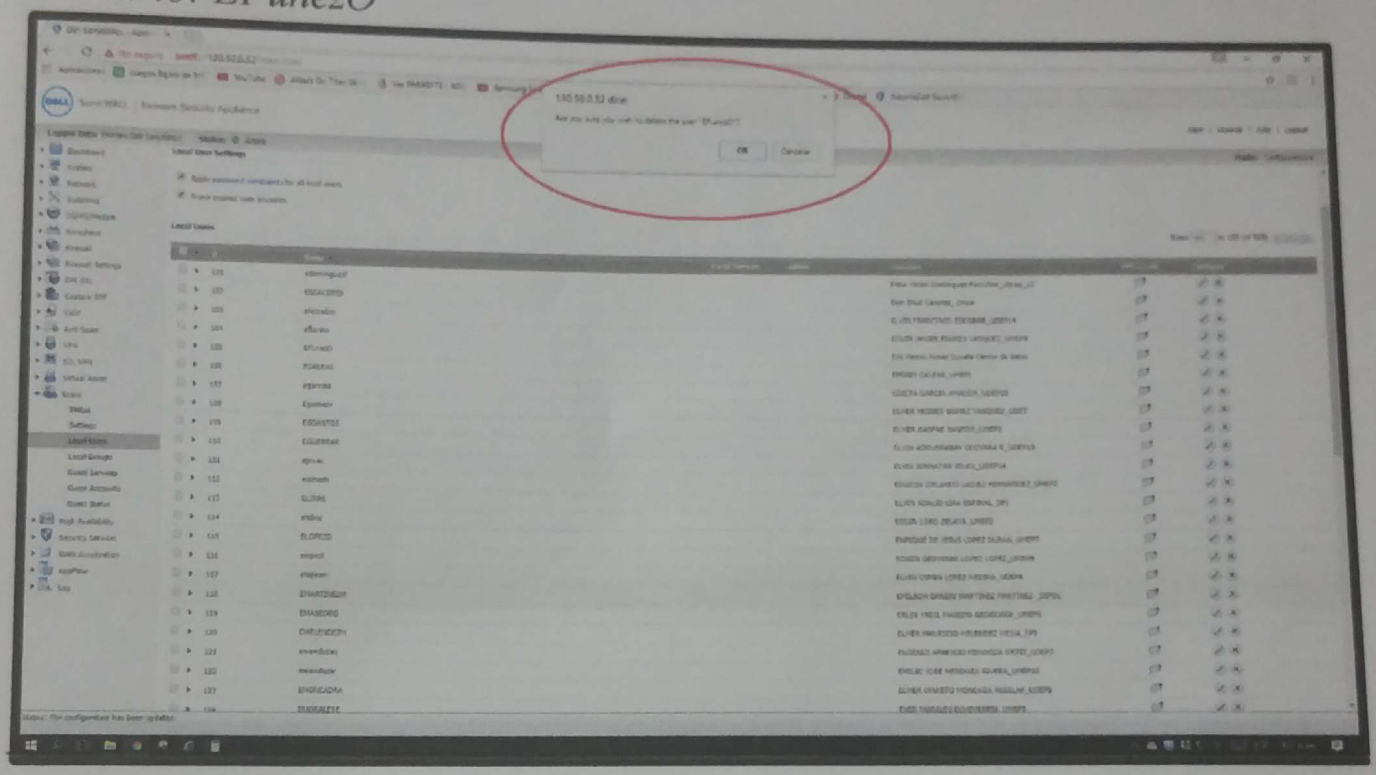
Stephanie Romero

Técnico en seguridad

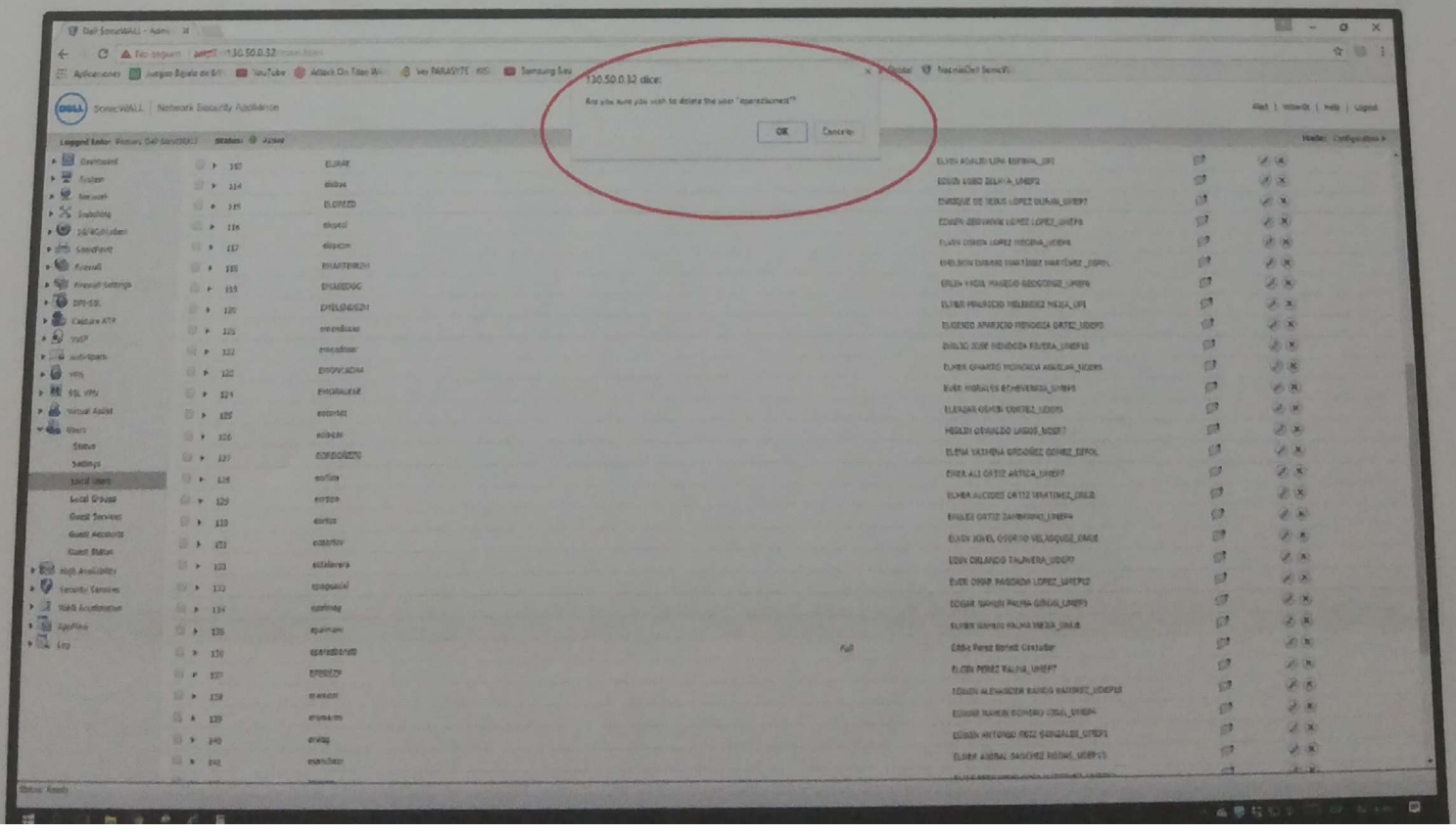
ANEXOS

Eliminación de usuarios

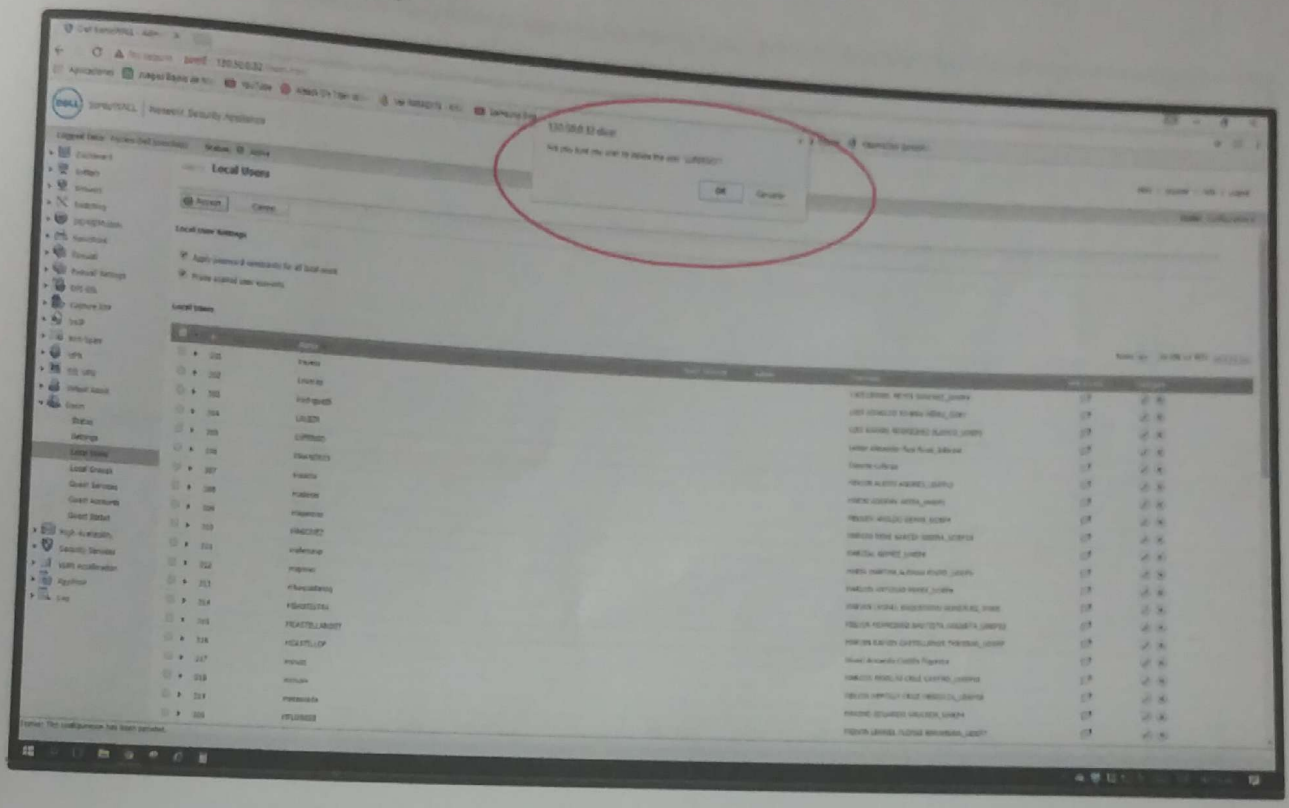
Usuario: EFunezO



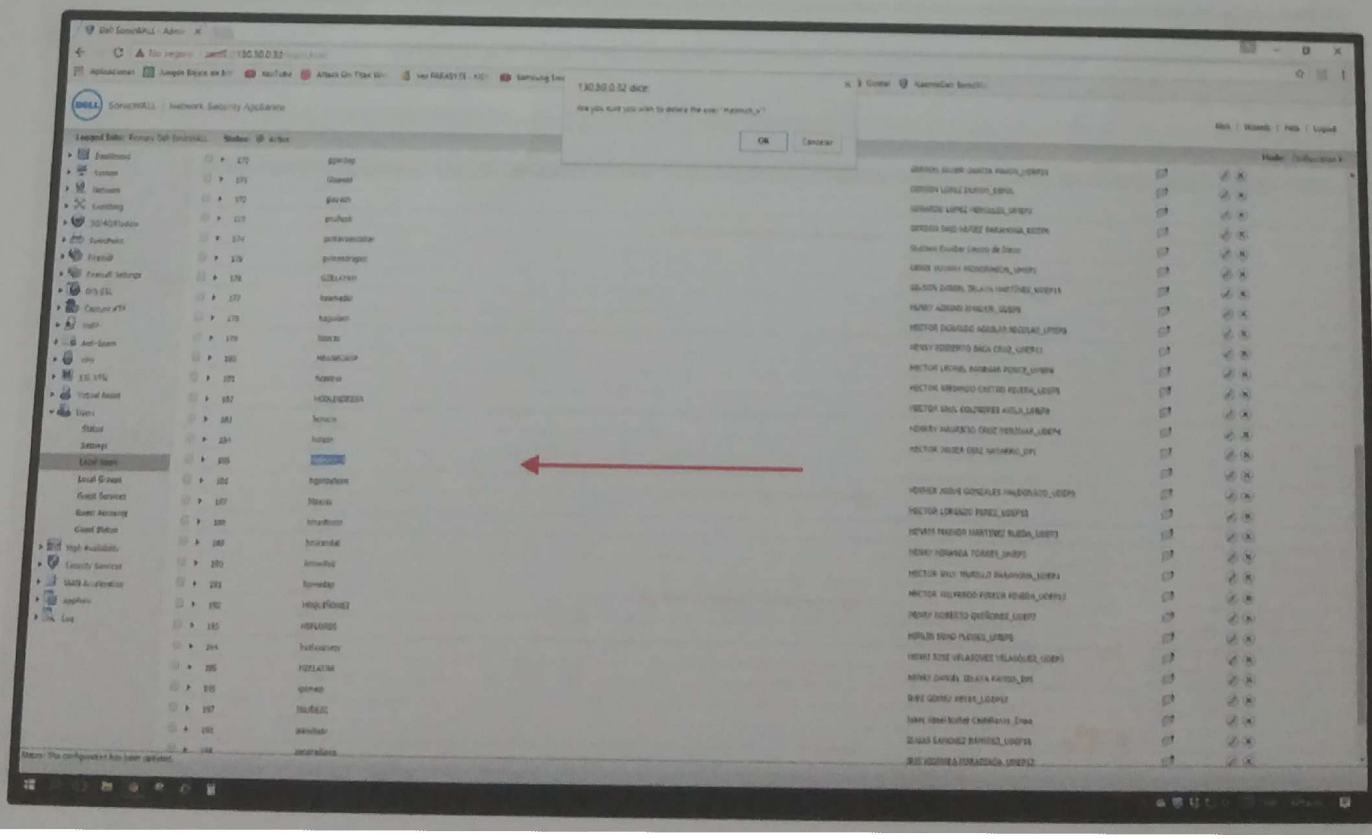
Usuario: eperezbonett



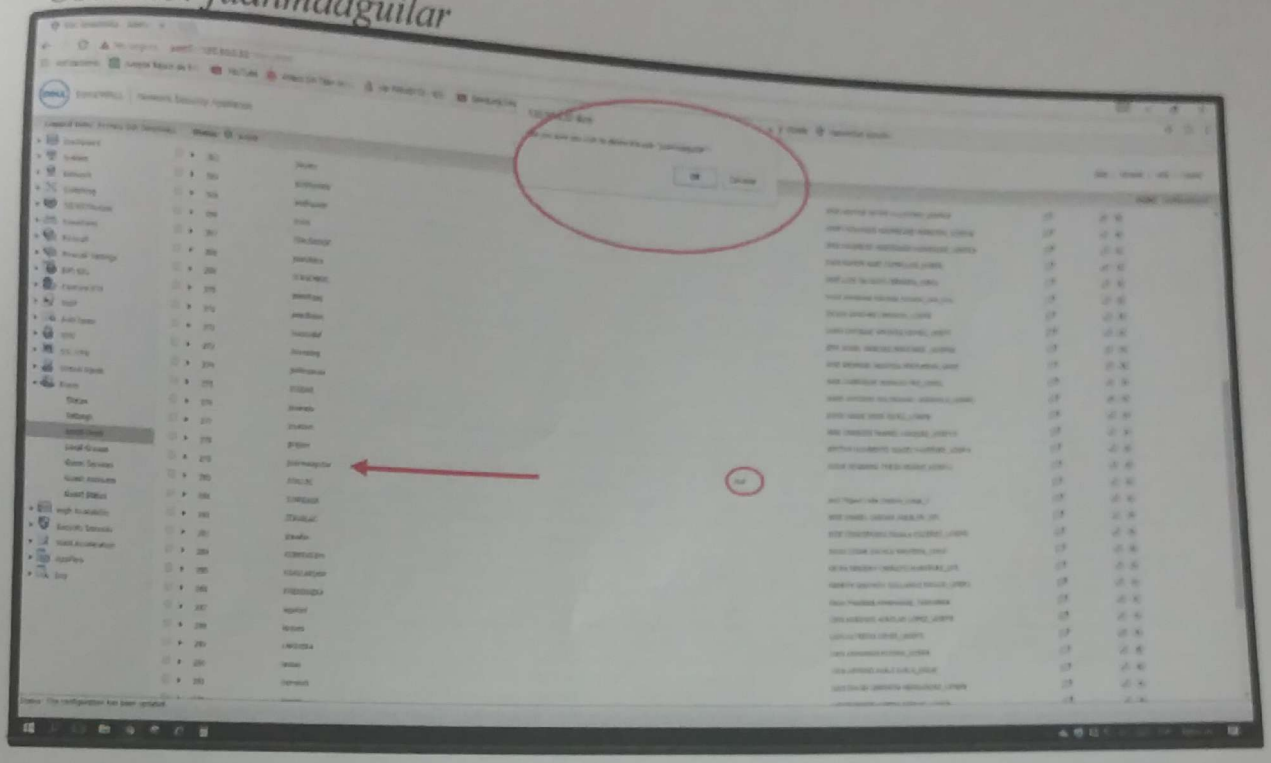
Usuario: LUFERGO



Usuario: Helmich_x



Usuario: juanmaaguilar



Usuarios sin identificación

Usuario: cfigueroaq, DanCoepol y dferreras