\*

CLIENTE:\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_

FECHA: viernes 26-01-2024 V1\_\_

HORA DE LLEGADA:\_\_ 09:16 am \_\_\_\_\_

HORA DE SALIDA: \_\_ 06:02 pm \_\_\_\_

ARMANDO LOPEZ

Tlf: 04142871877

04241996098

Trabajos realizados Armando López

SEGURIDAD:

\* SERVERHPG6: Se completó el respaldo manual iniciado ayer en la unidad G: (disco usb XXX). El respaldo automático diario siguió fallando y se reprogramó a las 10:30am para hacer monitoreo hoy. – Se limpió más de 1.200 GB adicionales de XXX de mayo de 2023 para liberar espacio requerido para respaldos actualizados.

\* Revisión y documentación detallada de ataque a VM1SQL desde ip 193.37.69.79 entre el 15 y 16-1-2024 para evaluar cambios al script de powershell para cambios en firewall de Windows para protección de servidores:

1) Ataque de 15-1-2024: 5 intentos en 2 minutos (1:42pm-1:43pm). 2) Ataque 1 de 2 del 16-1-2024: 25 intentos de entrar en VM1SQL en 8 minutos (10:36am-10:43am). 3) Ataque 2 de 2 del 16-1-2024: 14 intentos de iniciar sesión en VM1SQL en 7 minutos (12:29pm-12:35pm). Para el monitoreo anterior se usó la revisión del evento de seguridad 4625 que detecta intentos de logon fallidos.

\* VM1SQL:

- Se creó nuevo script de powershell para modificar Windows firewall evitando ataques rdp: Se creó copia de log de firewall con nombre “pfirewallALO.log” y otros cambios. Se revisó registros de eventos asociados con script de powershell que genera las siguientes actualizaciones de log: **Event Viewer🡪Applications and service logs🡪Microsoft🡪Windows🡪Windows Firewall with Advanced Security🡪Firewall🡪Event id 2005🡪RULE NAME=RDC Brute Force Prevention.**

\* DC4:

- Se inicio respaldo de WSB en nueva carpeta compartida [\\serverhpg6\dc4$](file:///\\serverhpg6\dc4$) con destino en disco XXX

Cliente (recibido): Armando López

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Observaciones:

4 horas 00 minutos facturables ( va(n) 4 hora(s) 00 minutos)

0 horas NO facturables.

**SOPORTE REMOTO**

Rangos de trabajo: 9:16am-1:05pm (3h), 5:02pm-

.