INCIDENTE

Se evidencia conexiones externas (IPs de Francia y Turquía) e intentos de accesos no autorizados.

CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

ATAQUES TÉCNICOS/ Escaneo de redes/ Daños, pérdida o puesta en riesgo de la información de la ANDJE, por escaneo de redes.

CRITICIDAD DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

IMPACTO= MEDIO

URGENCIA= MEDIO

CRITICIDAD= MEDIO

VALORACIÓN DEL INCIDENTE

IMPACTO: MEDIO

AFECTACIÓN DE LA TRIADA:

Tipo de Activo: Software
Nombre del Activo: SharePoint
Confidencialidad: Media
Integridad: Muy Alta
Disponibilidad: Alta

Impacto\criterio	Incumplimiento Legal	Sanciones	Pérdida de Imagen	Afectación a la Operación de la ANDJE
Catastrófico				
Mayor				

Moderado				
Menor			Incidente-1	Incidente-1
Insignificante	Incidente-1	Incidente-1		

RESPUESTA:

- Validación direcciones IP
- Habilitación NAT desde la LAN de computadores hacia el servidor de SHAREPOINT.
- Verificar lista usuarios que tienen privilegios de administración.
- Validación configuración métodos POST y PUT.
- Bloqueo direcciones IP.
- Modificación regla Executable file posting from external source