INCIDENTE

Se evidencia conexiones maliciosas que reportaban a IPs que están comprometidas con un tipo de vulnerabilidad de ejecución remota de código (RCE) denominada Log4Shel.

CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

ATAQUES TÉCNICOS/ Aprovechamiento de vulnerabilidades informáticas/ Daños, pérdida o puesta en riesgo de la información de la ANDJE, por aprovechamiento de vulnerabilidades de los sistemas de información.

CRITICIDAD DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

IMPACTO= MEDIO

URGENCIA= BAJO

CRITICIDAD= BAJO

VALORACIÓN DEL INCIDENTE

IMPACTO: MEDIO

AFECTACIÓN DE LA TRIADA:

Tipo de Activo: Software
Nombre del Activo: Servidor
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				Incidente-1
Menor				
Insignificante	Incidente-1	Incidente-1	Incidente-1	

RESPUESTA:

Remediación vulnerabilidad encontrada.