

Bogotá, noviembre 5 de 2021

**RESPUESTAS A PREGUNTAS RECIBIDAS CONVOCATORIA PUBLICA No.
012 PARA CONVOCATORIA ANÁLISIS DE VULNERABILIDADES**

Las pruebas de ethical hacking para las aplicaciones internas ¿tienen explotación?

RTA: Nos gustaría que pudieran cotizar los servicios con y sin explotación para tener los dos escenarios.

¿Las pruebas de intrusión son con explotación de vulnerabilidades?

RTA: Nos gustaría que pudieran cotizar los servicios con y sin explotación para tener los dos escenarios.

¿El análisis de aplicaciones Web, es web penetration testing? o solo análisis de vulnerabilidades sin explotación a las IPs donde se encuentran los aplicativos? ¿Cuál es el tamaño de las aplicaciones Web?

RTA: Nos gustaría que pudieran cotizar los servicios con y sin explotación para tener los dos escenarios.

cuantas son aplicaciones Web, cuantas son aplicaciones internas, cuantos servidores y cuantas direcciones IP serán objeto del proyecto?

RTA:

Aplicaciones WEB: 10 aproximadamente

Aplicaciones internas: 10

Servidores: 32

IP's: 10

¿Qué tipo de ejercicios de ingeniería social requieren y para cuantos empleados?

RTA: Esperamos que ustedes nos indiquen qué actividades de ingeniería social serían las necesarias para poder detectar las principales vulnerabilidades en este sentido contemplando unas 15 personas aproximadamente.

¿Con respecto a la revisión del área de tecnología, se refieren al análisis de riesgos bajo ISO27001?

RTA: Una consultoría en la que puedan identificar vulnerabilidades asociados al funcionamiento del área en cuanto a procesos y personas.

¿Con respecto a OSINT que fuentes desean evaluar y de que tipo?

RTA: No tenemos definido un listado, esperamos su recomendación de acuerdo a lo que es la Junta y lo que puede resultar relevante evaluar. Es decir, ustedes pueden determinar este alcance.

¿El análisis de vulnerabilidades de red para cuantos activos es?

RTA: Aproximadamente son 40 activos.

¿Se requiere hacer re-test de verificación?

RTA: No se requiere

¿De ser afirmativa la respuesta anterior, cuánto tiempo se estima para la mitigación de vulnerabilidades?

RTA: No se requiere

¿Al ser aplicativos en producción, el servicio debe ser en horario no hábil? o es posible en horario hábil?

RTA: Si puede programarse en horario hábil indicando la ventana de afectación.

De las 15 Apps son públicas y cuantas privadas

RTA: Aproximadamente 60% privadas y 40% públicas, algunas son mixtas, la idea es que nos puedan apoyar a identificar esto en el análisis.