ANEXO 1 ESPECIFICACIONES TÉCNICAS

Ítem	Descripción
1	**Herramienta de Análisis de Vulnerabilidades Tenable debe contar con**
1.1	Suscripción a los módulos Vulnerability Management, PCI ASV, Web App Scanning, Lumin.
1.2	Consola de administración centralizada de gestión.
1.3	Orientación al análisis de vulnerabilidades basada en riesgos.
1.4	Facilitar la creación de planes de remediación y seguimiento.
1.5	Programación de escaneo de vulnerabilidades, bajo demanda, automáticos y periódicos.
1.6	Permitir la clasificación de falsos positivos en la plataforma.
1.7	Actualización automática de la base de datos de vulnerabilidades de acuerdo a los estándares internacionales definidos.
1.8	Ejecutar escaneos internos y externos.
1.9	Permitir acceso a proveedores y personal de la entidad a la plataforma para la gestión de vulnerabilidades.
2	**Herramienta de pruebas de seguridad informática debe contar con:**
2.1	Automatizar tareas comunes y repetitivas relacionadas con pruebas de seguridad informática.
2.2	Capacidades de autodestrucción programables para agentes en diferentes niveles (producto, espacio de trabajo, módulo/RPT). Esto significa que ningún agente quede abandonado después de la prueba.
2.3	Contar con agentes que simplifiquen las interacciones con los equipos remotos. Tambien poder indicarle que desea hacer con el equipo remoto .
2.4	Permitir varios evaluadores de seguridad y tener la capacidad de interactuar en la misma sesión, lo que brinda la posibilidad de compartir datos de forma segura y delegar tareas de evaluación.
2.5	Capacidades de informes automatizados para un registro consistente y exhaustivo de interacciones que se pueden utilizar para planificar y priorizar los esfuerzos de remediación y demostrar el cumplimiento de regulaciones como PCI DSS , GDPR .
2.6	Permita genera informes bajo el marco MITRE ATT&CK ™, matriz de tácticas y técnicas de ataque conocidas que pueden ayudar a clasificar los ataques y priorizar aún más los riesgos.
2.7	Generar mapa de ataques facilitando una descripción gráfica en tiempo real. Además mostrar cadenas de ataques, cambios de rumbo.
2.8	Realizar pruebas y verificar que se hayan aplicado parches de seguridad u otros controles compensatorios y que se hayan corregido las vulnerabilidades de seguridad.
3	**Obligaciones en los Servicios Profesionales**
3.1	El CONTRATISTA debe ejecutar la administración integral y completa de las soluciones relacionadas al objeto contractual.
3.2	El CONTRATISTA debe realizar la Gestión integral de vulnerabilidades con las distintas areas de COLPENSIONES: - Establecimiento de planes de trabajo (cronogramas). - Seguimiento de planes trabajo. - Entrega de informes de avance de la gestion de vulnerabilidades. - Acompañamiento en la evaluación del impacto en la remediación de vulnerabilidades.
3.3	El CONTRATISTA debe entregar un informe técnico mensualmente (quinto dia hábil del mes) relacionado al estado de la gestion integral de vulnerabilidades avances, bloqueantes, mejoras, etc.
3.4	El CONTRATISTA debe apoyar en la gestión a los administradores de TI y/o supervisores de contratos de COLPENSIONES la respectiva remediación de las mismas.
3.5	El CONTRATISTA debe referenciar las herramientas utilizadas en el análisis de vulnerabilidades, las cuales deben estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.
3.6	El CONTRATISTA debe realizar análisis de vulnerabilidades periodico durante la ejecución del contrato, verificando nuevas vulnerabilidades y seguimiento a las vulnerabilidades identificadas en los análisis anteriores.
3.7	El CONTRATISTA debe generar un Informe con el reporte completo de brechas/vulnerabilidades encontradas, probabilidad e impacto de la amenaza, riesgo y estado de la vulnerabilidad, esfuerzo o complejidad de remediación, incluyendo el listado de las herramientas libres o licenciadas empleadas durante las pruebas. Las vulnerabilidades deben ser relacionadas con los activos de información identificados por los procesos en las Matrices de Activos de Información correspondientes y de acuerdo al análisis de riesgos establecer un nivel de criticidad.
3.8	El CONTRATISTA debe realizar un análisis diferencial como parte del contrato frente al análisis que será provisto por COLPENSIONES, resultado del último ejercicio realizado en el contrato de vulnerabilidades anterior.
3.9	El CONTRATISTA debe generar el reporte de remediación, gestionado con los administradores de TI y/o supervisores de contratos de COLPENSIONES, registrando el avance de implementación y/o la aceptación de los riesgos. Entregar un cuadro de seguimiento que permita monitorear el avance en las remediaciones realizadas por el área de tecnología.
3.10	El CONTRATISTA debe generar por solicitud de COLPENSIONES un resumen y presentación ejecutiva por cada análisis de vulnerabilidad realizado, dirigidos hacia la alta dirección, en donde se den a conocer los hallazgos más relevantes y su impacto en el evento de materializarse.
3.11	El CONTRATISTA debe ejecutar pruebas de vulnerabilidades de código dinámico y estático con herramienta propia de Colpensiones Fortify y hacer entrega y seguimiento de los informes de acuerdo los requerimientos realizados por COLPENSIONES.