**RESPUESTA A LAS OBSERVACIONES**
**INVITACIÓN 2026**
**SERVICIO INTEGRAL DE CIBERSEGURIDAD**

**RESPUESTA A OBSERVACIÓNES**

**PROPRONENTE: CONTROLES EMPRESARIALES S.A.S.**

***OBSERVACION 1*****:** *Publicación del presupuesto oficial o valor estimado del proceso*
*Observamos que el documento indica que el valor del contrato estará sujeto a las propuestas recibidas. Sin embargo, dentro de los requisitos habilitantes de experiencia se exige acreditar experiencia equivalente al cien por ciento (100%) del valor estimado del proceso expresado en salarios mínimos mensuales legales vigentes. Dado que dicho valor estimado no se encuentra publicado en el documento, respetuosamente solicitamos informar el presupuesto oficial o valor estimado del proceso, con el fin de permitir a los interesados verificar el cumplimiento de los requisitos habilitantes y estructurar adecuadamente su oferta económica.*

**RESPUESTA: La Corporación no cuenta con un presupuesto oficial o valor estimado definido para el proceso, por tal motivo, se invita a los interesados a presentar sus propuestas técnico-económicas de acuerdo con el alcance y las especificaciones descritas en los términos de referencia. La información recibida servirá como insumo para determinar el valor del futuro contrato y la experiencia a soportar estará directamente relacionada con el valor de la propuesta, por lo que se ajusta la invitación en ese sentido.**

***OBSERVACIÓN 2*****:** *Aclaración sobre la forma de pago y posibilidad de facturación parcial*
*Se observa que el documento establece que el pago se realizará de acuerdo con los servicios efectivamente prestados y recibidos a satisfacción. No obstante, no se especifican:*
*• Hitos de pago.*
*• Entregables asociados a cada pago.*
*• Posibilidad de facturación parcial.*
*• Porcentajes de desembolso.*
*• Condiciones para aprobación de cada entregable.*
*Solicitamos aclarar expresamente el esquema de pagos previsto para el contrato, indicando los hitos de ejecución que habilitan la facturación y los porcentajes correspondientes, con el fin de evitar interpretaciones divergentes durante la ejecución contractual.*

**RESPUESTA: Se acepta la observación y se ajusta la invitación. Se incluye facturación mensual de acuerdo con los avances de las obligaciones y pago a los sesenta (60) días previo aval del supervisor del contrato, de acuerdo con el cronograma, los servicios efectivamente prestados, recibidos a satisfacción y debidamente certificados. Para cada pago será requisito la presentación de los informes, soportes y demás documentos exigidos.**

***OBSERVACIÓN 3.*** *Aclaración sobre los tiempos efectivos de pago. El documento señala que los pagos se realizarán dentro de los sesenta (60) días siguientes a la aceptación de la factura y*

*cumplimiento de los requisitos exigidos. Sin embargo, no se establecen plazos máximos para la revisión y aceptación de entregables por parte del supervisor del contrato.*
*Solicitamos informar:*
*• El plazo máximo de revisión de entregables.*
*• El plazo máximo para solicitar ajustes.*
*• El plazo máximo para aceptación o rechazo de productos.*
*Lo anterior con el propósito de contar con certeza sobre el flujo financiero del contrato.*

**RESPUESTA: De acuerdo la obligación No. 3 el contratista deberá definir junto con el supervisor un cronograma para establecer estos plazos y pueda armonizarse con los plazos de facturación.**

***OBSERVACIÓN 4.*** *Definición del alcance y dimensionamiento de la infraestructura objeto de Evaluación. La invitación contempla la evaluación de infraestructura interna y externa, redes, servidores, sistemas operativos, servicios expuestos, firewalls, controles perimetrales y componentes tecnológicos. No obstante, no se identifican parámetros mínimos de dimensionamiento que permitan estimar adecuadamente el esfuerzo requerido. Solicitamos informar, como mínimo:*
*• Número de sedes objeto de evaluación.*
*• Cantidad aproximada de servidores físicos y virtuales.*
*• Cantidad de direcciones IP públicas.*
*• Número de aplicaciones web expuestas.*
*• Número de dispositivos de seguridad perimetral.*
*• Cantidad de usuarios de directorio activo.*
*• Cantidad estimada de activos tecnológicos a evaluar.*
*Esta información es indispensable para garantizar comparabilidad entre ofertas.*

**RESPUESTA:**
**Número de sedes objeto de evaluación: 1**
**Cantidad aproximada de servidores físicos y virtuales: 30**
**Cantidad de direcciones IP públicas: 18**
**Número de aplicaciones web expuestas:15**
**Número de dispositivos de seguridad perimetral: 2**
**Cantidad de usuarios de directorio activo: 2206**
**Cantidad estimada de activos tecnológicos a evaluar: 1132**

***OBSERVACIÓN 5.*** *Definición del alcance de las pruebas de penetración El documento contempla actividades de Ethical Hacking y Pentesting; sin embargo, no se especifica:*
*• Modalidad de pruebas (caja negra, caja gris o caja blanca).*
*• Número de objetivos a evaluar.*
*• Alcance autorizado para explotación.*
*• Restricciones operativas.*
*• Ventanas de ejecución.*
*• Procedimientos de escalamiento ante hallazgos críticos.*
*Solicitamos definir estos aspectos con el fin de garantizar uniformidad metodológica entre los proponentes.*

**RESPUESTA**:
**Modalidad de pruebas (caja negra, caja gris o caja blanca): Caja gris**
**Número de objetivos a evaluar: 3338**
**Alcance autorizado para explotación: la necesaria para la caja gris**
**Restricciones operativas: indisponibilidad**
**Ventanas de ejecución: nocturnas y en horario especifico**
**Procedimientos de escalamiento ante hallazgos críticos: Dirección de GI**

***OBSERVACIÓN 6.*** *Aclaración sobre la conformación del equipo de trabajo. La invitación exige diversos perfiles especializados y múltiples certificaciones internacionales.*
*Solicitamos aclarar si:*
*• Cada rol debe ser cubierto por una persona independiente.*
*• Un mismo profesional puede acreditar varios roles.*
*• Las certificaciones exigidas pueden concentrarse en uno o varios integrantes del equipo de trabajo.*
*La aclaración resulta necesaria para determinar correctamente los costos asociados a la ejecución del contrato.*

**RESPUESTA:**

- **Cada rol debe ser cubierto por una persona independiente: Si, cada rol debe ser diferenciado**
- **Un mismo profesional puede acreditar varios roles: No, los roles deben ser diferenciados**
- **Las certificaciones exigidas pueden concentrarse en uno o varios integrantes del equipo de trabajo: Las certificaciones pueden concertarse en uno o varios integrantes del equipo de acuerdo a sus roles.**

***OBSERVACIÓN 7.*** *Justificación de la exigencia de certificación TIER III o ICREA III. Dentro de los requisitos técnicos se solicita certificación TIER III de diseño y construcción o certificación ICREA nivel III vigente.*
*Considerando que el objeto contractual corresponde a una evaluación de ciberseguridad y no a la construcción, operación o certificación de centros de datos, respetuosamente solicitamos informar la justificación técnica de dicha exigencia y su relación directa con el objeto del proceso.*
*Adicionalmente, solicitamos evaluar la posibilidad de aceptar experiencia específica en servicios de ciberseguridad como mecanismo alternativo de acreditación.*

**RESPUESTA: Se acepta la observación y se ajusta la invitación.**

***OBSERVACIÓN 8.*** *Inconsistencia en la información financiera solicitada. Se evidencia una inconsistencia respecto al período de los estados financieros exigidos dentro del proceso, situación que puede generar interpretaciones distintas entre los oferentes. Solicitamos aclarar expresamente cuál es la vigencia financiera aplicable para la evaluación de los requisitos habilitantes.*

**RESPUESTA: Se acepta la observación. Efectivamente, se identificó un error de digitación en el numeral correspondiente a los requisitos habilitantes de capacidad financiera. Para efectos**

**de la verificación de la capacidad financiera de los proponentes, se tendrán en cuenta los estados financieros con corte a 31 de diciembre de 2025, debidamente suscritos por el representante legal y el revisor fiscal o contador público, según corresponda**.

***OBSERVACIÓN 9.*** *Contradicción respecto a la aceptación de contratos en ejecución para acreditar experiencia. En una sección del documento se indica que podrán acreditarse contratos en ejecución con certificación del valor ejecutado a la fecha de cierre. Posteriormente se establece que no se aceptarán contratos en ejecución. Solicitamos aclarar de manera expresa cuál de las dos disposiciones prevalece para efectos de acreditar la experiencia habilitante.*

**RESPUESTA: Se acepta la observación y se ajusta a invitación. En consecuencia, la Corporación aclara que sí serán aceptados contratos en ejecución, siempre que el proponente aporte certificación expedida por el contratante en la que conste el tiempo y el valor efectivamente ejecutado a la fecha de cierre del proceso, y que con dicha ejecución se acrediten los requisitos mínimos de experiencia exigidos.**

***OBSERVACIÓN 10.*** *Definición de entregables y criterios de aceptación. Se identifican como productos del contrato informes ejecutivos, informes técnicos, inventario de activos, análisis de vulnerabilidades y roadmap de remediación. Sin embargo, no se establecen:*
*• Formatos mínimos requeridos.*
*• Estructura de los informes.*
*• Criterios objetivos de aceptación.*
*• Tiempos de revisión.*
*• Número máximo de ciclos de ajustes.*
*Solicitamos definir estos aspectos para garantizar una adecuada ejecución contractual y evitar diferencias de interpretación durante el desarrollo del proyecto.*

**RESPUESTA: De acuerdo la obligación No. 3 el contratista deberá definir junto con el supervisor un cronograma para establecer estos plazos y pueda armonizarse con los plazos de facturación.**

***OBSERVACIÓN 11.*** *Definición de propiedad intelectual y uso de resultados. Solicitamos aclarar el tratamiento de la propiedad intelectual asociada a:*
*• Metodologías empleadas.*
*• Herramientas utilizadas.*
*• Scripts de automatización.*
*• Plantillas y formatos de análisis.*
*• Productos derivados del servicio.*
*Lo anterior con el fin de delimitar adecuadamente los derechos y obligaciones de las partes.*

***RESPUESTA: Se aclara que el tratamiento de la propiedad intelectual se encuentra regulado en la minuta contractual, específicamente en las cláusulas Vigésima Sexta – Propiedad de los Resultados y Vigésima Séptima – Derechos de Autor, las cuales establecen el régimen aplicable a los resultados, informes y demás productos derivados de la ejecución del contrato***

**PROPRONENTE: GLOBALTEKSECURITY**

***OBSERVACIÓN 1**. En cuanto a los indicadores financiero, se solicita muy respetuosamente no pedir capital de trabajo. Se solicita pedir razón de cobertura de interés mayor a 4%.*

**RESPUESTA: Nos permitimos informar que la Corporación Salud UN ha definido los indicadores de capacidad financiera considerando la naturaleza, alcance y riesgos asociados al objeto contractual, con el fin de verificar que los proponentes cuenten con la solidez financiera necesaria para asumir las obligaciones derivadas de una eventual contratación.**

***OBSERVACIÓN 2**. Solicita amablemente pedir solo estar certificaciones:*

- *Ethical hacking*
- *Pentesting*
- *Certified Information Security Manager*
- *Certified Digital Forensics Examiner*

**RESPUESTA: No se acepta la observación.**

***OBSERVACIÓN 3**. En cuanto al personal solicitado se solicita que solo tengan en cuenta*

| ROL | EXPERIENCIA PROFESIONAL CERTIFICADA |
|---|---|
| Líder Técnico de Ethical Hacking / Pentesting: responsable de planear y ejecutar las pruebas de penetración internas y externas, el análisis de la superficie de ataque, la identificación de vectores de movimiento lateral y la validación de vulnerabilidades explotables. | 3 años |
| Especialista en Seguridad Ofensiva y Hardening: evaluación de configuraciones de firewalls y seguridad perimetral, revisión de reglas permisivas, segmentación y aislamiento, hardening de servidores, gestión de privilegios, MFA y cuentas de servicio. | 3 años |

**RESPUESTA: No se acepta la observación.**

***OBSERVACIÓN 4:** En cuanto a la experiencia se solicita respetuosamente que se pidan contratos después del 1 de enero 2010*

**RESPUESTA: No se acepta la observación. La Corporación mantiene el requisito de experiencia establecido en la invitación, por considerar que el período allí definido permite acreditar experiencia reciente, suficiente y pertinente para la adecuada ejecución del objeto contractual**

**PROPONENTE: GRUPO GTDCOLOMBIA**

***OBSERVACIÓN 1** ¿Confirmar la cantidad total de activos a incluir en el servicio, así como los tipos de tecnología involucrados? (Ejemplo: bases de datos, servidores, estaciones de trabajo, firewalls, etc.)*

**RESPUESTA: Aclaramos la cantidad total de activos a incluir en el servicio 3338, incluidos bases de datos, servidores, estaciones de trabajo y firewalls.**

***OBSERVACIÓN 2**: Confirmar las versiones específicas de los activos a incluir en los servicios.*

**RESPUESTA: Las versiones específicas de los activos a incluir Linux y windows 2002-2025.**

***OBSERVACIÓN 3.** Confirmar cantidad de escaneos a realizar y su periodicidad.*

**RESPUESTA: Es contrato establece una única actividad por tanto no tiene periodicidad establecida.**

***OBSERVACIÓN 4**. ¿Se requiere personal para apoyo en la gestión de hardening?*

**RESPUESTA: Si se requiere personal para apoyo en la gestión de hardening.**

***OBSERVACIÓN* 5.** *¿Podrías confirmarme la cantidad de activos a evaluar y los tipos de tecnología involucrados en las pruebas? (Ejemplo: aplicaciones web, móviles, APIs, infraestructura, etc.) Infraestructura, aplicaciones web*

**RESPUESTA: Son 3338-equipos de seguridad perimetral servidores equipos de comucacion ap, swich, router, aplicaciones Base de datos.**

***OBSERVACIÓN 6**. ¿Qué tipo de pruebas se requiere ejecutar? (Caja negra, caja gris o caja blanca)*

**RESPUESTA: La prueba que se requiere es de caja gris**

***OBSERVACIÓN 7**. ¿Son activos internos o externos?, confirmar cantidad de cada uno.*

**RESPUESTA: Son 15 server externos, además equipos servidores y app Onpremise**

***OBSERVACIÓN 8**. ¿Cuántas pruebas al año se deben realizar y sobre cuántos activos en cada una de ellas?*

**RESPUESTA: Se debe realizar una prueba a los activos ya descritos**

***OBSERVACIÓN 9.** En caso de incluir activos transaccionales, por favor confirmar la cantidad y la periodicidad de las pruebas necesarias*

**RESPUESTA: Se debe realizar una prueba a los activos ya descritos**

***OBSERVACIÓN 10**. ¿Requieren análisis de vulnerabilidades?*

**RESPUESTAS: Si se requiere análisis de vulnerabilidades**

**PROPONENTE: IDENTIAN**

***OBSERVACIÓN 1**. El pliego exige, como requisito habilitante, que el oferente cuente con certificación TIER III de diseño y construcción (Uptime Institute) o ICREA Nivel III vigente, dentro de un proceso cuyo objeto contractual corresponde a servicios de Ethical Hacking / Pentest y Hardening.*

*Las certificaciones TIER III e ICREA Nivel III evalúan exclusivamente la infraestructura física de un centro de datos: redundancia eléctrica, sistemas de refrigeración, rutas de mantenimiento concurrente y niveles de disponibilidad. Su objeto es certificar el diseño y construcción de una edificación destinada a alojar equipos de cómputo críticos, no la competencia, metodología o idoneidad de un proveedor para ejecutar pruebas de seguridad ofensiva.*
*El objeto contractual del presente proceso (Ethical Hacking, Pentest y Hardening) no involucra el alojamiento de infraestructura del oferente ni la prestación de servicios de colocation o data center. Se trata de un servicio profesional de evaluación de seguridad, cuya idoneidad se acredita mediante:*

*• Certificaciones individuales de los profesionales ejecutores: OSCP, OSCE, CEH, GPEN, eWPT, CRTO u otras equivalentes reconocidas en el sector.*
*• Certificaciones organizacionales de gestión de seguridad de la información, como ISO 27001, directamente relacionadas con la naturaleza del servicio solicitado.*
*• Metodologías reconocidas de pruebas de seguridad ofensiva (OSSTMM, PTES, OWASP Testing Guide), o acreditaciones como CREST, cuando la entidad busque un estándar adicional de calidad.*

*Exigir TIER III/ICREA III para este objeto contractual no guarda relación de proporcionalidad ni de pertinencia técnica con el servicio a contratar, y tiene el efecto de restringir injustificadamente la pluralidad de oferentes, dado que dicha certificación es poseída por un número muy reducido de centros de datos en el país y no por las empresas especializadas en seguridad ofensiva, que son las naturalmente idóneas para este tipo de contrato.*

*Solicitud*

*Con fundamento en lo anterior, solicitamos respetuosamente:*
*• Eliminar del numeral la exigencia de certificación TIER III de diseño y construcción o ICREA Nivel III, por no corresponder al objeto contractual del proceso, por el contrario, robustecer el proceso con los perfiles requeridos para la ejecución del servicio.*
*• En su lugar, incorporar como requisitos habilitantes condiciones proporcionales y pertinentes al servicio de Ethical Hacking / Pentest y Hardening, tales como certificaciones vigentes de los profesionales asignados a la ejecución (Lead Cybersecurity Professional Certification LCSPC, Cyber Security Foundation CSFPC, Certificación Auditor Líder ISO 27001:2022, Certificación Auditor Interno ISO 27001:2022, CISM - Certified Information Security Manager, CEH Certified Ethical Hacker,ITIL V4 fundaments) y/o certificación ISO 27001 vigente del oferente.*

**RESPUESTA: Se acepta la observación y se ajusta la invitación.**

***OBSERVACIÓN 2**. El pliego de condiciones establece que el proponente debe acreditar un capital de trabajo equivalente al 30% del valor anual del contrato, calculado como la diferencia entre activo corriente y pasivo corriente.*

*Solicitamos respetuosamente considerar que dicho indicador sea evaluado como un valor absoluto mínimo, en lugar de un porcentaje sobre el valor del contrato. Esto en razón a que el capital de trabajo refleja la capacidad operativa y de respaldo financiero real del proponente, la cual no guarda necesariamente una relación proporcional con el valor del contrato a ejecutar.*

*Solicitud*
*Bajo esta modalidad, el requisito quedaría redactado de la siguiente manera: "El proponente deberá acreditar un capital de trabajo mayor o igual a $500.000.000 COP, calculado como la diferencia entre el activo y el pasivo corrientes del último estado financiero auditado."*

*Esta fórmula es consistente con la práctica de otros procesos de contratación pública en Colombia y permite evaluar de manera objetiva la solidez financiera del proponente, sin restringir innecesariamente la participación de empresas especializadas con capacidad técnica y financiera demostrada.*

**RESPUESTA: Nos permitimos informar que la Corporación Salud UN ha definido los indicadores de capacidad financiera considerando la naturaleza, alcance y riesgos asociados al objeto contractual, con el fin de verificar que los proponentes cuenten con la solidez financiera necesaria para asumir las obligaciones derivadas de una eventual contratación.**

**El indicador de capital de trabajo definido como Activo Corriente menos Pasivo Corriente, con un valor igual o superior al 30% del valor ofertado.**

***OBSERVACIÓN 3.** Solicitamos muy amablemente aclarar las siguientes preguntas sobre el alcance Hardening: Firewalls: ¿Cuántos firewalls hay, de qué fabricante/modelo, y qué función cumple cada uno (perimetral, interno, segmentación entre VLANs)?*

**RESPUESTA: 2 firewalls fortigate, renta Fortigate 120 g, su función es perimetral entre VLANs.**

***OBSERVACIÓN 4.** ¿Nos darán acceso de solo lectura a la consola de administración para revisar reglas, o nos entregarán un export de la configuración?*

**RESPUESTA: Si se dará acceso de solo lectura a la consola de administración.**

***OBSERVACIÓN 5:** Reglas excesivamente permisivas ¿Cuántas reglas tiene aproximadamente cada firewall?*

**RESPUESTA: El Firewall tiene aproximadamente 156 reglas.**

***OBSERVACIÓN 6** ¿Hay un proceso de limpieza/revisión periódica de reglas o nunca se ha hecho?*

**RESPUESTA: Si existe un proceso de limpieza/revisión de reglas**

***OBSERVACIÓN 7*** *Segmentación y aislamiento. ¿Existe diagrama de red actualizado (VLANs, zonas DMZ, separación producción/pruebas/administración)?*

**RESPUESTA: Si existe diagrama de red actualizado**

***OBSERVACIÓN 8*** *¿Los 43 servidores están distribuidos en distintos segmentos o todos en la misma red plana?*

**RESPUESTA: Los servidores están en distintos segmentos de red**

***OBSERVACIÓN 9*** *Hardening de servidores ¿Qué sistemas operativos y versiones manejan?*

**RESPUESTA: 2012-2025- linux y windows**

***OBSERVACIÓN 10*** *¿Existe un baseline o estándar de hardening ya aplicado (CIS, STIG, guías del fabricante)?*

**RESPUESTA: No Existe**

***OBSERVACIÓN 11*** *Servicios innecesarios. ¿Tienen inventario de servicios/puertos activos por servidor, o hay que levantarlo durante la evaluación?*

**RESPUESTA: Si se tiene inventario de servicios/puertos activos**

***OBSERVACIÓN 12.*** *Exposición de puertos. ¿Cuáles son los rangos IP internos y externos en alcance?*

**RESPUESTA: Interno 24,26 y externo 29,30**

***OBSERVACIÓN 13*** *¿Hay servicios expuestos a internet que el cliente ya identifiqué como críticos?*

**RESPUESTA: Si hay servicios expuestos críticos**

***OBSERVACIÓN 14.*** *Configuración de acceso administrativo ¿Cómo gestionan cuentas administrativas (Active Directory, bóveda de contraseñas tipo CyberArk/Vault, cuentas locales sueltas)? Necesitamos acceso para revisar políticas de contraseñas, expiración de cuentas y permisos asignados.*

**RESPUESTA: Las cuentas activas administrativas se gestionan por medio de Active Directory**

***OBSERVACIÓN 15*** *Uso de MFA ¿En qué puntos está implementado MFA hoy (VPN, RDP, consolas admin, accesos en la nube)?*

**RESPUESTA: Se ha implementado MFA en correo electrónico y aplicaciones web expuestas**

***OBSERVACIÓN 16*** *¿Hay algún acceso administrativo sin MFA?*

**RESPUESTA: Sí. Actualmente la Corporación cuenta con autenticación multifactor (MFA) habilitada únicamente para el servicio de correo electrónico.**

***OBSERVACIÓN 17*** *Gestión de privilegios ¿Existe una solución PAM o el modelo de privilegios es manual?*

**RESPUESTA: Si existe solución PAM**

***OBSERVACIÓN 18*** *¿Aplican el principio de mínimo privilegio o hay cuentas con admin/root por defecto?*

**RESPUESTA: No se aplica el principio de mínimo privilegio ni cuentas admin/root**

***OBSERVACIÓN 19*** *Gestión de cuentas de servicio. ¿Cuántas cuentas de servicio existen?*

**RESPUESTA: Existen 3 cuentas de servicio**

***OBSERVACIÓN 20*** *¿Cómo se gestionan sus credenciales (rotación, almacenamiento, expiración)?*

**RESPUESTA: Las credenciales se gestionan por expiración**

***OBSERVACIÓN 21*** *Logs y monitoreo ¿Tienen SIEM o logging centralizado? ¿Qué fuentes envían logs y cuál es la retención?*

**RESPUESTA: Si se tiene SIEM o logging centralizado, los logs son enviados por Firewalls, switchs y servidores, con una retención de 60 días**

***OBSERVACIÓN 22.*** *Capacidad de detección y respuesta ¿Tienen SOC propio o tercerizado?*

**RESPUESTA: Si se tiene SOC tercerizado**

***OBSERVACIÓN 23.*** *¿Usan EDR/XDR o IDS/IPS?*

**RESPUESTA: Se usa EDR/XDR**

***OBSERVACIÓN 24*** *¿Hay un playbook de respuesta a incidentes documentado?*

**RESPUESTA: No existe Playbook documentado**

***OBSERVACIÓN 25*** *¿Qué tipo de cuentas/credenciales nos proveerán (admin local, cuenta de dominio con privilegios de lectura, acceso a consolas de gestión)?*

**RESPUESTA: Se proveerá cuentas solo lectura o de ser necesario cuentas mantenimiento**

***OBSERVACIÓN 26*** *¿Hay VPN o conexión dedicada para el equipo evaluador?*

**RESPUESTA: Hay Vpn dedicada fortigate**

***OBSERVACIÓN 27*** *¿Hay ventana de mantenimiento si alguna revisión requiere reinicios o genera riesgo de interrupción?*

**RESPUESTA: Hay Ventana de mantenimiento de ser necesario**

***OBSERVACIÓN 28*** *Se deben presentar 5 hojas de vida diferentes o una sola persona puede presentarte para más de un perfil.*

**RESPUESTA: Una sola persona no puede cumplir los 5 roles, cada rol debe ser diferenciado**

**PROPRONENTE:** YEAPDATA

***OBSERVACIÓN 1*****:** *¿La Corporación dispone de un inventario actualizado de activos tecnológicos (servidores, estaciones, dispositivos de red, activos cloud y aplicaciones) que será suministrado al contratista para contrastar los resultados del descubrimiento de activos solicitado?*

**RESPUESTA: La Corporación si dispone de inventario de activos actualizado y será suministrado al contratista**

**OBSERVACIÓN 2:** *¿Existe una estimación del número total de activos que conforman la superficie de ataque interna y externa objeto de evaluación?*

**RESPUESTA: Si existe una estimación del número total de activos que conforman la superficie de ataque objeto de evaluación**

**OBSERVACIÓN 3:** *¿La organización cuenta con una CMDB o herramienta de gestión de activos de software que permita validar software autorizado, no autorizado o fuera de soporte?*

**RESPUESTA: La organización si cuenta con una herramienta de gestión de activos que permita validar software autorizado, no autorizado**

**OBSERVACIÓN 4:** *¿La evaluación deberá contrastar las configuraciones encontradas contra algún estándar específico de hardening como CIS Benchmarks, Microsoft Security Baselines, DISA STIG o lineamientos del fabricante?*

**RESPUESTA: La evaluación si deberá contrastar las configuraciones** encontradas **contra algún estándar específico**

**OBSERVACIÓN 5:** *¿La revisión de hardening incluirá controladores de dominio, servidores de aplicaciones, bases de datos y dispositivos de red o únicamente sistemas operativos?*

**RESPUESTA La revisión de hardening debe incluir controladores de dominio, servidores de aplicaciones, bases de datos y dispositivos de red**

**OBSERVACIÓN 6:** *¿Existe un inventario actualizado de cuentas privilegiadas, cuentas de servicio y cuentas compartidas que será suministrado al contratista?*

**RESPUESTA: Si existe un inventario actualizado de cuentas privilegiadas, cuentas de servicio y cuentas compartidas que será suministrado al contratista**

**OBSERVACIÓN 7:** *¿La Corporación utiliza mecanismos MFA para accesos administrativos, VPN, aplicaciones críticas y servicios cloud que deban formar parte del alcance de validación?*

**RESPUESTA: La Corporación si utiliza mecanismos MFA que forman parte del alcance de la validación**

**OBSERVACIÓN 8:** *¿La entidad dispone actualmente de herramientas de gestión de vulnerabilidades y podrán ser utilizadas como insumo para la evaluación?*

**RESPUESTA: La entidad si dispone actualmente de herramientas de gestión de vulnerabilidades y podrán ser utilizadas como insumo**

**OBSERVACIÓN 9:** *¿Se espera únicamente la identificación de vulnerabilidades o también la validación controlada de explotación para confirmar criticidad e impacto real?*

**RESPUESTA: Se espera la identificación de vulnerabilidades y validación controlada**

**OBSERVACIÓN 10:** *¿La revisión de logs y monitoreo contempla únicamente la existencia de registros o también la evaluación de cobertura, retención, correlación y capacidades de detección?*

**RESPUESTA: La revisión de Logs y monitoreo también contempla evaluación de cobertura, retención, correlación y capacidades de detección**

**OBSERVACIÓN 11:** *¿Podría la entidad informar la cantidad aproximada de segmentos de red, VLANs y sedes que deberán ser analizados dentro de la evaluación de segmentación?*

**RESPUESTA: La entidad si podrá informar la cantidad de segmentos de red y VLANs las sedes son 1**

**OBSERVACIÓN 12:** *¿La infraestructura objeto de análisis incluye ambientes cloud (AWS, Azure, GCP, OCI u otros) además de la infraestructura on-premise?*

**RESPUESTA: La infraestructura incluye Cloud en IFX**

**OBSERVACIÓN 13:** *¿Existen herramientas SIEM, XDR, EDR, NDR, SOAR o SOC actualmente operando que deban ser consideradas durante la evaluación de capacidades de detección y respuesta?*

**RESPUESTA: Si existen herramientas de las relacionadas que deben ser consideradas en la evaluación de detección y respuesta**

**OBSERVACIÓN 14:** *¿La evaluación deberá incluir análisis de cobertura frente a marcos MITRE ATT&CK y capacidades de detección de amenazas avanzadas?*

**RESPUESTA: La evaluación si debe incluir análisis de cobertura frente a marcos MITRE ATT&CK y capacidades de detección de amenazas avanzadas**

**OBSERVACIÓN 15:** *¿Existen terceros, proveedores o conexiones externas con acceso a la red corporativa que deban ser consideradas dentro del análisis de superficie de ataque y riesgo?*

**RESPUESTA: Si existen terceros, proveedores o conexiones externas con acceso a la red corporativa que deban ser consideradas dentro del análisis, Linalca y TSP**

**OBSERVACIÓN 16:** *¿Cuál es el número aproximado de aplicaciones web internas y externas que harán parte del alcance de la evaluación?*

**RESPUESTA: el número aproximado de aplicaciones web internas y externas 100**

**OBSERVACIÓN 17:** *¿Las aplicaciones incluidas en el alcance podrán ser objeto de pruebas manuales de seguridad alineadas con OWASP Top 10 o únicamente de revisión automatizada?*

**RESPUESTA: Las aplicaciones incluidas puedes ser objeto de pruebas manuares de seguridad alineadas con OWASP Top 10**

**OBSERVACIÓN 18:** *En caso de identificarse evidencia de compromiso activo durante la ejecución, ¿la Corporación dispone de procedimientos formales de respuesta a incidentes y escalamiento que deban seguirse?*

**RESPUESTA: La Corporación no dispone de procedimientos formales de respuesta a incidentes y escalamiento**

**OBSERVACIÓN 19***: ¿La Corporación autorizará pruebas de penetración controladas sobre activos internos y externos para validar la explotación efectiva de vulnerabilidades críticas identificadas?*

**RESPUESTA: La Corporación si autorizará pruebas de penetración controladas sobre activos internos y externos para validar la explotación efectiva de vulnerabilidades críticas identificadas**

**OBSERVACIÓN 20:** *Respecto a los sistemas legacy mencionados en el anexo técnico, ¿podría la*

*entidad informar la cantidad aproximada, criticidad y tecnologías involucradas para dimensionar adecuadamente el esfuerzo de evaluación y definición de controles compensatorios?*

**RESPUESTA: Frente a los sistemas legacy la entidad informar la cantidad aproximada, criticidad y tecnologías involucradas**

**OBSERVACIÓN 21:** *¿La entidad espera únicamente identificar activos no inventariados (Shadow IT) o también realizar análisis de riesgo, clasificación de criticidad y recomendaciones de tratamiento sobre dichos activos?*

**RESPUESTA: La entidad espera también realizar análisis de riesgo, clasificación de criticidad y recomendaciones de tratamiento sobre dichos activos**

**OBSERVACIÓN 22:** *¿Podría la entidad indicar el número de dominios, bosques (forests), relaciones de confianza (trusts) y controladores de dominio que harán parte de la evaluación de Active Directory*?

**RESPUESTA: La entidad si puede indicar estas cantidades**

**OBSERVACIÓN 23:** *Considerando la naturaleza hospitalaria de la organización, ¿la evaluación deberá incluir dispositivos biomédicos, equipos IoMT (Internet of Medical Things) y redes clínicas especializadas?*

**RESPUESTA HOSPITAL: La evaluación no incluye dispositivos biomédicos, equipos IoMT (Internet of Medical Things) y redes clínicas especializadas**

**OBSERVACIÓN 24:** *¿Existen ambientes clínicos, asistenciales o de misión crítica donde se encuentren restringidas las pruebas activas o intrusivas por requerimientos de continuidad operativa?*

**RESPUESTA: No existen ambientes restringidos para pruebas activas o intrusivas**

**OBSERVACIÓN 25***: ¿La entidad espera que los hallazgos sean mapeados a marcos de referencia como CIS Controls v8, NIST Cybersecurity Framework 2.0, MITRE ATT&CK e ISO 27001:2022 o únicamente a criterios técnicos de riesgo?*

**RESPUESTA: La entidad espera que los hallazgos sean mapeados a los marcos de referencia además de criterios técnicos de riesgo**

**OBSERVACIÓN 26:** *¿La Corporación cuenta con un inventario actualizado y clasificado de dispositivos IoMT, incluyendo fabricante, modelo, versión de firmware, sistema operativo embebido, criticidad clínica y ubicación física?*

**RESPUESTA: La Corporación no cuenta con inventario actualizado y clasificado con las especificaciones relacionadas en la pregunta**

**OBSERVACIÓN 27:** *¿Se dispone actualmente de mecanismos para identificar dispositivos IoMT no autorizados o activos biomédicos conectados fuera del inventario institucional (Shadow IoMT)?*

**RESPUESTA: Actualmente si se dispone de mecanismos para identificar dispositivos IoMT no autorizados o activos biomédicos conectados fuera del inventario institucional (Shadow IoMT)**

**OBSERVACIÓN 28:** *¿La evaluación deberá incluir la identificación de vulnerabilidades conocidas (CVE), alertas de fabricantes y exposición a amenazas activas asociadas a los dispositivos IoMT presentes en la organización?*

**RESPUESTA: La evaluación si debe incluir la identificación de vulnerabilidades conocidas (CVE), alertas de fabricantes y exposición a amenazas activas asociadas a los dispositivos IoMT presentes en la organización**

**OBSERVACIÓN 29:** *¿Se espera que el contratista realice análisis de exposición de dispositivos IoMT frente a campañas de ransomware hospitalario, amenazas persistentes avanzadas (APT) y amenazas específicas dirigidas al sector salud?*

**RESPUESTA: Si se espera que el contratista realice exposición de dispositivos IoMT frente a campañas de ransomware hospitalario, amenazas persistentes avanzadas (APT) y amenazas específicas dirigidas al sector salud**

**OBSERVACIÓN 30:** *¿La evaluación incluirá la identificación de dispositivos biomédicos con acceso directo o indirecto a Internet y la valoración de los riesgos asociados a dicha exposición?*

**RESPUESTA: La evaluación si incluirá la identificación de dispositivos biomédicos con acceso directo o indirecto a Internet y la valoración de los riesgos asociados a dicha exposición**

**OBSERVACIÓN 31:** *¿Se requiere evaluar la exposición de protocolos médicos especializados tales como DICOM, HL7, FHIR y demás protocolos clínicos presentes en la infraestructura?*

**RESPUESTA: No se requiere evaluar la exposición de protocolos médicos especializados**

**OBSERVACIÓN 32:** *¿La evaluación deberá contemplar el análisis de movimiento lateral potencial desde dispositivos IoMT hacia sistemas críticos como HIS, PACS, RIS, LIS, Active Directory y bases de datos institucionales?*

**RESPUESTA: La evaluación si debe contemplar el análisis de movimiento lateral potencial desde dispositivos IoMT hacia sistemas críticos**

**OBSERVACIÓN 33:** *¿La Corporación dispone actualmente de capacidades de monitoreo de amenazas sobre dispositivos IoMT, tales como NAC, SIEM, NDR, XDR o plataformas especializadas para entornos biomédicos?*

**RESPUESTA: La Corporación no dispone actualmente de capacidades de monitoreo de amenazas**

**OBSERVACIÓN 34:** *¿Se espera que el contratista realice ejercicios de Cyber Threat Intelligence para identificar indicadores de compromiso (IoC), tácticas, técnicas y procedimientos (TTP) asociados a amenazas activas dirigidas al sector salud y aplicables a los activos IoMT identificados?*

**RESPUESTA: Si se espera que el contratista realice ejercicios asociados a amenazas activas dirigidas al sector salud**

**OBSERVACIÓN 35:** *¿La entidad espera recibir una matriz de priorización de riesgos IoMT que correlacione criticidad clínica, exposición a amenazas, vulnerabilidades identificadas e impacto potencial sobre la continuidad de la atención médica?*

**RESPUESTA: La entidad si espera recibir una matriz de priorización de riesgos IoMT que correlacione criticidad clínica, exposición a amenazas, vulnerabilidades identificadas e impacto potencial sobre la continuidad de la atención médica.**

**OBSERVACIÓN 36:** *¿Se espera que el contratista identifique y correlacione información proveniente de fuentes OSINT, Dark Web, Breach Data, inteligencia de amenazas del sector salud y reportes de fabricantes biomédicos para determinar exposición, credenciales comprometidas o riesgos asociados a activos IoMT de la Corporación?*

**RESPUESTA: Si se espera que el contratista identifique y correlacione información proveniente de fuentes OSINT, Dark Web, Breach Data, inteligencia de amenazas del sector salud y reportes de fabricantes biomédicos para determinar exposición, credenciales comprometidas o riesgos asociados a activos IoMT de la Corporación**

**OBSERVACIÓN 37:** *¿Con el fin de dimensionar adecuadamente el alcance, esfuerzo técnico, recursos especializados y riesgos asociados al proyecto, se solicita a la entidad suministrar información agregada sobre cantidad de servidores, estaciones de trabajo, dispositivos de red, aplicaciones, dominios de Active Directory, activos IoMT y sedes que harán parte del alcance de la evaluación?*

**RESPUESTA: servidores 30, estaciones de trabajo 850, dispositivos de red 200, aplicaciones 50, dominios de Active Directory 1, activos IoMT 2 fw fortigate y sedes 1**