RESPUESTA A OBSERVACIONES AL PROYECTO DE PLIEGOS DEL PROCESO INFI S.A008-2025

El área de sistemas da respuesta a las observaciones presentadas frente al proyecto de pliegos del proceso **LP-005-2025,** que tiene por objeto: **"PRESTAR UN SERVICIO INTEGRAL DE MONITOREO, GESTIÓN, ANÁLISIS Y ACTUALIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE INFICALDAS DURANTE EL PERIODO 2026, COMPLEMENTADO CON ASESORÍA ESPECIALIZADA PARA FORTALECER Y ACTUALIZAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CONFORME A LA NORMA ISO/IEC 27001:2022 Y LOS LINEAMIENTOS REGULATORIOS DEL MINTIC, GARANTIZANDO LA CONTINUIDAD, MEJORA Y CUMPLIMIENTO NORMATIVO EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"** conforme a lo dispuesto en el Decreto 1082 de 2015, en los siguientes términos:

A. OCTAPUS.IO

1. Dentro del servicio de Ethical hacking por favor confirmar si se debe incluir retest de verificación del correcto cierre de las vulnerabilidades.

   RESPUESTA:

   Se deberá incluir el retest de verificación dentro del alcance del servicio de Ethical Hacking, con el fin de confirmar el correcto cierre de las vulnerabilidades identificadas.
   Esta actividad garantiza que las vulnerabilidades hayan sido gestionadas y mitigadas de manera efectiva, y proporciona mayor confianza sobre el estado de seguridad de los activos tecnológicos evaluados, asegurando el cumplimiento de las mejores prácticas internacionales en seguridad de la información y de los requerimientos técnicos y normativos definidos en el pliego de condiciones.

2. Dentro del servicio de Ethical Hacking. Por favor confirmar la cantidad de aplicaciones web que se deben evaluar.

   RESPUESTA:

   Dentro del servicio de Ethical Hacking, se deberán evaluar cuatro (4) aplicaciones web de INFICALDAS:

- IAS
- SIICO
- Workmanager
- Página web institucional

   Todas estas aplicaciones han sido adquiridas o contratadas a terceros, por lo que se consideran aplicaciones comerciales (COTS – *Commercial Off-The-Shelf*), y no corresponden a desarrollos internos o a la medida de la entidad.

3. Dentro del servicio de Ethical Hacking. Por favor confirmar la cantidad de infraestructura que se deben evaluar.

RESPUESTA:

Dentro del servicio de Ethical Hacking, la infraestructura de INFICALDAS que deberá ser evaluada incluye:

- 50 equipos de cómputo
- 9 servidores
- 1 firewall
- 2 equipos activos de red
- 4 puntos de acceso inalámbricos (Access Point)

Esta definición asegura que el alcance del servicio cubra todos los activos tecnológicos críticos de la entidad, conforme a las mejores prácticas de seguridad de la información y los requerimientos técnicos establecidos en el pliego de condiciones.

4. ¿Dentro del servicio de Ingeniería social, por favor confirmar si se debe hacer un phishing mensual para 50 usuarios?

RESPUESTA:

Dentro del servicio de Ingeniería Social, se deberá realizar una campaña mensual de phishing dirigida a los cincuenta (50) usuarios previamente identificados por INFICALDAS.

Esta actividad tiene como objetivo evaluar y fortalecer la concienciación y resiliencia de los usuarios frente a amenazas de ingeniería social, siempre dentro de los términos del servicio y de las necesidades operativas de la organización, garantizando la confidencialidad, integridad y disponibilidad de la información durante su ejecución.

5. Dentro del Servicio de Monitoreo SOC, pudieran informar dentro de los activos a monitorear cuentos EPS (Eventos por segundo) están generando.

RESPUESTA:

Dentro del Servicio de Monitoreo SOC, el volumen promedio diario de eventos de seguridad generado por la infraestructura tecnológica de INFICALDAS es de aproximadamente 250 eventos por día.

Este valor se considera como referencia para dimensionar el monitoreo, análisis y correlación de eventos dentro del SOC, asegurando la gestión efectiva de incidentes de seguridad y la respuesta oportuna ante alertas críticas, conforme a los requerimientos técnicos del pliego de condiciones.

6. Dentro del requerimiento de implementar el control de DLP, se deberá proporcionar tanto la solución como el servicio de ingeniería de implementación. O la solución DLP sería proveida por la entidad.

RESPUESTA:

De acuerdo con los requisitos establecidos, la solución DLP (Data Loss Prevention) será provista íntegramente por el contratista, quien además se encargará de prestar el servicio de ingeniería para su implementación. Esto implica que el contratista suministrará tanto el software o agente DLP necesario como los servicios técnicos asociados para su despliegue y configuración en todos los equipos de la entidad, garantizando una protección integral frente a la fuga de datos y facilitando la administración centralizada de las políticas de seguridad

7. Frente al requerimiento de DLP por favor informar que se va proteger, si son dispositivo o correos? Y cuantos de cada uno hay.

RESPUESTA:

De acuerdo con la información disponible, el control de DLP (Data Loss Prevention) está orientado a proteger los dispositivos de la entidad. Específicamente, se contempla la instalación del agente DLP en todos los equipos, sin distinción entre equipos críticos y no críticos, lo que garantiza una cobertura total frente a la fuga de datos. Esta medida permite monitorear, prevenir y gestionar los riesgos asociados al manejo de información sensible en todos los endpoints de la organización.
En cuanto a la cantidad de dispositivos, la infraestructura tecnológica de INFICALDAS está compuesta por:

- 50 equipos de cómputo
- 9 servidores
- 1 firewall
- 2 equipos activos de red
- 4 Access Poin

8. Frente al servicio de cumplimiento, cuando fue la última auditoría al SGSI y cuantos procesos corporativos tienen dentro del SGSI?.

RESPUESTA:

La última auditoría interna al Sistema de Gestión de Seguridad de la Información (SGSI) de INFICALDAS se realizó del 21 de noviembre al 15 de diciembre de 2025. El informe final fue presentado el 15 de diciembre de 2025

El alcance organizacional oficial de la auditoría incluyó principalmente el proceso de Prestación de Servicios Financieros. Sin embargo, para verificar la eficacia y coherencia de los controles del SGSI, se revisaron adicionalmente otros procesos institucionales que, aunque no forman parte explícita del alcance oficial, están directamente vinculados a la implementación y operación de controles del SGSI según la norma ISO/IEC 27001:2022.

Procesos revisados dentro del SGSI:

- Prestación de Servicios Financieros (proceso principal dentro del alcance)
- Planeación y Gestión Institucional
- Administración de Recursos

- Gestión Jurídica
- Gestión de Talento Humano
- Gestión del Riesgo
- Control y Gestión

Estos procesos fueron evaluados por su vinculación directa con determinados controles del Anexo A de la ISO/IEC 27001:2022, aunque solo el primero forma parte del alcance oficial

9. Podrían incluir dentro de los códigos habilitantes UNSPsC el código: | 81 | 11 | 18 | 00 |

RESPUESTA:

Analizada la observación, esta se acoge, en atención a que el código UNSPSC 81111800 – Servicios de sistemas y administración de componentes de sistemas, guarda relación directa con el objeto contractual, el cual consiste en la prestación de un servicio integral de monitoreo, gestión, análisis y actualización de la seguridad de la información, así como en el fortalecimiento y actualización del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022 y los lineamientos regulatorios del MINTIC.

En efecto, las actividades propias del contrato implican la administración, operación, control y seguimiento de componentes de sistemas de información, gestión de accesos, monitoreo continuo, soporte a plataformas tecnológicas y análisis de incidentes de seguridad, las cuales se encuentran comprendidas dentro del alcance del citado código UNSPSC.

En consecuencia, se procederá a incluir el código UNSPSC 81111800 dentro de los códigos habilitantes del proceso, sin que ello implique modificación del objeto contractual ni ampliación de su alcance, manteniéndose incólumes las condiciones técnicas y jurídicas inicialmente establecidas.

10. Dentro de las certificaciones del equipo de trabajo, se debe contar con todas las certificaciones para el perfil Auditor de seguridad Informática, Perfil Auditor de Cumplimiento o se puede establecer que sean mínimo 2 de las listadas.

RESPUESTA:

Las certificaciones y especializaciones exigidas no podrán ser acreditadas en su totalidad por un solo profesional, por cuanto la correcta ejecución del contrato exige la conformación de un equipo de trabajo plural, multidisciplinario y técnicamente competente, en el cual las competencias y certificaciones se encuentren distribuidas entre los diferentes integrantes del equipo, garantizando así una cobertura integral de los conocimientos y responsabilidades requeridas.

11. Dentro del perfil de Auditor de seguridad Informática se pudiera agregar la certificación de: CPTE que homologa a la CEH.

RESPUESTA:

Ambas certificaciones son reconocidas internacionalmente y acreditan competencias equivalentes en pruebas de penetración y hacking ético, conforme a estándares globales de ciberseguridad, se acepta la observación

12. Dentro del perfil de Auditor de Cumplimiento se pudiera dejar la certificación Cybersecurity Nexus Certificate como Opcional ya que hace referencia a una certificación de un fabricante en especial y cierra la posibilidad de pluralidad de oferentes.

RESPUESTA:

Para el perfil de Auditor de Cumplimiento, se exigirá que el profesional cuente con al menos una certificación internacionalmente reconocida en auditoría, gestión o control de seguridad de la información. Se aceptarán, entre otras, certificaciones como CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), ISO/IEC 27001 Lead Auditor, CRISC (Certified in Risk and Information Systems Control), CISSP (Certified Information Systems Security Professional) o equivalentes. La certificación Cybersecurity Nexus Certificate (CSX) podrá ser presentada como una opción válida, pero no será de carácter obligatorio, con el fin de no restringir la pluralidad de oferentes y asegurar la participación de profesionales con diferentes acreditaciones reconocidas en el sector.

13. Podrían por favor compartir los formatos de anexos en formato editable Word.

RESPUESTA:

Los formatos de anexos solicitados estarán disponibles y se compartirán en formato editable Word, para su correcta diligencia por los proponentes.

14. Podrían por favor compartir todas las preguntas y respuestas de los otros oferentes para retroalimentarnos con las consultas y respuestas generadas.

INFICALDAS no comparte las preguntas ni respuestas de otros oferentes, dado que se trata de información de terceros sujeta a confidencialidad.

Para retroalimentación, los proponentes deberán basarse únicamente en la información oficial del pliego de condiciones, sus anexos y las aclaraciones o respuestas publicadas por la entidad.
Esta medida garantiza la equidad, transparencia y confidencialidad del proceso de selección.

B. KAVANTIC

1. Cybersecurity Nexus Certificate (NIST)

La exigencia del Cybersecurity Nexus Certificate (NIST) resulta técnicamente improcedente y jurídicamente restrictiva, toda vez que el National Institute of Standards and Technology (NIST) no emite certificaciones oficiales para personas, sino que desarrolla marcos de referencia y estándares técnicos de adopción voluntaria (NIST CSF, SP 800, entre otros). Exigir una certificación específica asociada a NIST, que no es expedida por dicha entidad ni exigida por norma legal o regulatoria, no constituye un criterio objetivo de idoneidad, y restringe injustificadamente la pluralidad de oferentes. El Consejo de Estado ha establecido que los requisitos habilitantes deben ser necesarios,

proporcionales y directamente relacionados con el objeto contractual, y no pueden convertirse en barreras artificiales de participación (Sección Tercera, Exp. 54001-23-31-000-2008-00005-01).

RESPUESTA:

Para el perfil de Auditor de Cumplimiento, se exigirá que el profesional cuente con al menos una certificación internacionalmente reconocida en auditoría, gestión o control de seguridad de la información. Se aceptarán, entre otras, las siguientes certificaciones:

- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- ISO/IEC 27001 Lead Auditor
- CRISC (Certified in Risk and Information Systems Control)
- CISSP (Certified Information Systems Security Professional)

La certificación Cybersecurity Nexus Certificate (CSX) podrá presentarse como una opción válida, pero no será obligatoria, con el fin de garantizar pluralidad de oferentes y asegurar la participación de profesionales con diferentes acreditaciones reconocidas en el sector.

2. Máster en Tecnologías Informáticas Avanzadas

La exigencia de un título de maestría resulta desproporcionada frente al objeto del contrato, el cual no contempla actividades de investigación académica, sino labores operativas, evaluativas y estratégicas en seguridad de la información, cumplimiento y gestión de riesgos.
El Consejo de Estado ha indicado que la exigencia de títulos académicos solo es válida cuando estos resultan estrictamente indispensables para el desarrollo del objeto contractual (Sección Tercera, Sentencia 3 de mayo de 2016).

RESPUESTA:

Un Máster en Tecnologías Informáticas Avanzadas aporta conocimientos especializados sobre tendencias y tecnologías emergentes, tales como inteligencia artificial, computación en la nube y análisis avanzado de amenazas. Estos conocimientos son esenciales para que la infraestructura tecnológica de la organización esté preparada para evolucionar y enfrentar nuevos desafíos de seguridad de manera efectiva.

Asimismo, un auditor o pentester con este nivel académico puede anticipar, identificar y mitigar riesgos complejos que superan los controles tradicionales, fortaleciendo la resiliencia y la seguridad de la información de la entidad.

3. Especialización en Auditoría de TI

Si bien la auditoría de TI es relevante, no constituye la única vía válida para evaluar la seguridad, eficiencia y cumplimiento de los sistemas de información, especialmente en contextos modernos donde la ciberseguridad incorpora inteligencia de amenazas, análisis ofensivo y gestión integral del riesgo digital. El Consejo de Estado ha sostenido que no es admisible exigir una formación específica cuando existen alternativas equivalentes que garantizan la idoneidad del contratista (Sección Tercera, Exp. 05001-23-31-000- 2012-00289-01). Solicitud: Eliminar la solicitud punctual de esas tres certificaciones o titulus y permitir la acreditación de competencias equivalentes mediante estudios y certificaciones profesionales tales como:

- Certified Ethical Hacker (CEH)
- Certificado en Ciberseguridad y Cibercrimilogia (CIC-I)
- Especializacion en seguridad informatica
- Certificado en Ciberseguridad
- Asesor Estratégico de Inteligencia y Contrainteligencia

RESPUESTA:

La especialización en auditoría de TI permite evaluar de manera sistemática la seguridad, eficiencia y cumplimiento de los sistemas de información. Un profesional especializado puede identificar vulnerabilidades, analizar riesgos y verificar que los controles implementados sean adecuados y eficaces para proteger los activos digitales, datos y sistemas de la organización.

Las auditorías de TI aseguran que la organización cumpla con normativas internacionales (ISO/IEC 27001, NIST, GDPR, entre otras) y adopte las mejores prácticas del sector. El incumplimiento puede generar sanciones legales y daños reputacionales, por lo que contar con expertos en auditoría es fundamental para mitigar estos riesgos.

Asimismo, la auditoría de TI es clave para anticipar amenazas cibernéticas, detectar vulnerabilidades antes de que sean explotadas y fortalecer la postura de seguridad de la organización. Permite implementar medidas correctivas y mejorar continuamente los procesos y controles de seguridad.

En este contexto, el auditor de TI desempeña un papel estratégico en la gestión de riesgos tecnológicos, identificando y evaluando amenazas que pueden afectar la operatividad, seguridad de los datos y cumplimiento normativo de la entidad.

4. El Proyecto de Pliego exige la implementación de herramientas de Análisis de Vulnerabilidades y Prevención de Pérdida de Datos (DLP), sin exigir que el proponente cuente con certificación oficial del fabricante.

Dichas herramientas corresponden a servicios críticos que impactan directamente la seguridad de la información, la continuidad del negocio y la responsabilidad legal de INFICALDAS S.A.
Los fabricantes establecen que la configuración avanzada, remediación automática, soporte especializado y escalamiento de incidentes solo pueden ser garantizados por partners certificados en niveles Gold, Platinum o equivalentes.

Solicitud de ajuste al Pliego: Se solicita a la entidad incluir la solicitud de certificacion del proponent como partner GOLD, PLATINUM o similar e naras de garantizar una adecuada ejecucion de la implementacion, mitigacion, correcciones, ajustes, soporte y gestion de las herramientas alineadas con el proposito de la entidad en ciberseguridad.

“El proponente deberá acreditar certificación vigente como Partner Gold, Platinum o nivel equivalente otorgado por el fabricante de la herramienta de Análisis de Vulnerabilidades y de la herramienta de Prevención de Pérdida de Datos (DLP) ofrecidas, o certificación equivalente que garantice soporte directo del fabricante, personal certificado y capacidad de implementación avanzada.”

RESPUESTA:

La norma ISO/IEC 27001:2022 establece la obligación de implementar controles eficaces para la gestión de vulnerabilidades y la protección de datos, lo que incluye el uso de herramientas especializadas como DLP (Prevención de Pérdida de Datos) y soluciones de análisis de vulnerabilidades. Esta norma exige que dichos controles sean realmente efectivos, estén alineados con los riesgos identificados en la organización y sean gestionados por personal debidamente competente.

Si bien la norma no impone de manera explícita la obligación de que el proveedor cuente con certificaciones Gold, Platinum o equivalentes otorgados por el fabricante de las herramientas, la exigencia de este tipo de acreditaciones puede considerarse una buena práctica. Esto se debe a que contar con partners certificados garantiza una adecuada configuración, soporte especializado y capacidad de remediación avanzada, aspectos fundamentales para la eficacia y continuidad de los controles implementados; exigir certificaciones de alto nivel puede elevar la calidad y seguridad de la implementación, pero debe justificarse adecuadamente y no convertirse en una barrera injustificada para la participación de proveedores idóneos. Los proponentes podrán presentar sus certificaciones, pero no será causa excluyente de quienes no la presenten.

C.

1. ¿INFICALDAS cuenta actualmente con una plataforma SIEM (Security Information and Event Management) implementada que deba utilizarse por el contratista, o este debe proveer, implementar y configurar una solución SIEM completamente nueva desde cero?

RESPUESTA:

INFICALDAS no cuenta actualmente con una plataforma SIEM implementada y operativa que deba ser utilizada por el contratista. En consecuencia, el contratista que resulte seleccionado deberá proveer, implementar y configurar una solución SIEM desde cero, conforme a los requerimientos técnicos, funcionales y normativos definidos en el pliego de condiciones, y en armonía con las mejores prácticas internacionales en seguridad de la información, tales como la ISO/IEC 27001:2022, así como los lineamientos y directrices emitidos por el MINTIC.

Lo anterior se entiende sin perjuicio de las demás obligaciones contractuales y dentro del alcance definido para el presente proceso.

2. ¿El servicio de SOC (Centro de Operaciones de Seguridad) 24x7x365 debe prestarse desde infraestructura propia de la contratista ubicada en sus instalaciones, o INFICALDAS cuenta con espacios físicos, puestos de trabajo y conectividad donde deba operar presencialmente el personal del SOC?

RESPUESTA:

El servicio de SOC (Centro de Operaciones de Seguridad) 24x7x365 deberá ser prestado desde la infraestructura propia del contratista, ubicada en sus instalaciones. INFICALDAS no dispone actualmente de espacios físicos, puestos de trabajo ni conectividad destinados para la operación presencial del personal del SOC en sus sedes.

En consecuencia, el contratista que resulte seleccionado deberá garantizar la prestación integral del servicio desde su propia infraestructura, dando cumplimiento a los requisitos técnicos, de seguridad, confidencialidad y

disponibilidad establecidos en el pliego de condiciones, sin que ello implique obligaciones adicionales para la entidad.

3. ¿Cuál es el volumen promedio diario de eventos de seguridad que genera la infraestructura tecnológica de INFICALDAS expresado en EPS (Events Per Second) o eventos/día? ¿Cuál es la capacidad de almacenamiento requerida para logs históricos y cuál es el período mínimo de retención exigido por políticas internas o normativa aplicable?

   RESPUESTA:

Con base en la información disponible, el volumen promedio diario de eventos de seguridad generados por la infraestructura tecnológica de INFICALDAS es de aproximadamente 250 eventos por día.
La capacidad estimada de almacenamiento requerida es de 500 GB.
En cuanto a políticas específicas asociadas a la gestión y retención de eventos, actualmente no se cuenta con políticas definidas para este componente.

La información anterior se suministra con fines orientativos, sin que implique garantía sobre variaciones futuras ni modificación del alcance del proceso

4. Además de los 50 equipos de cómputo, 9 servidores, 1 firewall y 2 equipos activos de red mencionados en el pliego, ¿existen otros activos tecnológicos que deban ser monitoreados e incluidos en el alcance del servicio tales como: dispositivos móviles corporativos, equipos IoT, impresoras de red, sistemas de videovigilancia/cámaras IP, puntos de acceso inalámbricos WiFi, centrales telefónicas IP, UPS con gestión remota, u otros?

RESPUESTA:

Adicionalmente a los 50 equipos de cómputo, 9 servidores, 1 firewall y 2 equipos activos de red señalados en el pliego de condiciones, dentro del alcance del servicio se deberán incluir cuatro (4) puntos de acceso inalámbricos (*Access Point*).

5. ¿Los 50 equipos de cómputo y 9 servidores mencionados se encuentran todos ubicados físicamente en las oficinas principales de INFICALDAS en Manizales, o incluyen equipos en sucursales, sedes alternas, teletrabajadores o ubicaciones remotas?

   RESPUESTA:

Los servidores se encuentran actualmente ubicados en la oficina principal de INFICALDAS en Manizales; no obstante, la entidad se encuentra adelantando un proyecto de migración a la nube, dentro del cual el proponente deberá garantizar la continuidad del servicio de SOC sobre los entornos que sean migrados, conforme al alcance definido en el pliego de condiciones.
Por su parte, los equipos de cómputo se conectan a la infraestructura de la entidad a través de VPN, razón por la cual deberán ser monitoreados de manera permanente por el SOC, independientemente de su ubicación física, con el fin de garantizar la seguridad de la información y de los activos tecnológicos de INFICALDAS.

6. Respecto a la solución DLP (Data Loss Prevention) mencionada en el numeral
   7 de las especificaciones técnicas: ¿Todos los 50 endpoints requieren instalación de agente DLP, o

únicamente un subconjunto de equipos considerados críticos?

RESPUESTA:

La instalación del agente DLP deberá realizarse en la totalidad de los cincuenta (50) equipos de cómputo de INFICALDAS, sin distinción entre equipos críticos y no críticos.
Esta determinación obedece a la necesidad de garantizar una cobertura integral en la prevención de fuga de información, en concordancia con las mejores prácticas en seguridad de la información y los requisitos normativos aplicables. La implementación generalizada del agente DLP permite el monitoreo, prevención y gestión centralizada de los riesgos asociados al tratamiento de información sensible en todos los *endpoints*, evitando brechas derivadas de equipos no protegidos y facilitando el cumplimiento de los procesos de control, auditoría y verificación definidos por la entidad.

7. ¿Cuántas aplicaciones web posee INFICALDAS que deban ser objeto de evaluación mediante pruebas de Ethical Hacking? ¿Cuáles de estas aplicaciones son de desarrollo interno/a medida versus aplicaciones comerciales o COTS (Commercial Off-The-Shelf)?

RESPUESTA:

INFICALDAS cuenta actualmente con tres (3) aplicaciones web principales: IAS, SIICO y Workmanager, así como la página web institucional.
Todas las aplicaciones mencionadas han sido adquiridas y/o contratadas a terceros, por lo cual se consideran aplicaciones comerciales o COTS (*Commercial Off-The-Shelf*), y no corresponden a desarrollos internos o a la medida de la entidad.
En consecuencia, las pruebas de Ethical Hacking deberán realizarse sobre las cuatro (4) aplicaciones antes indicadas, conforme al alcance y condiciones técnicas establecidas en el pliego de condiciones.

8. ¿Las pruebas de Ethical Hacking y penetration testing pueden realizarse durante horario laboral normal (lunes a viernes 8:00-18:00), o deben ejecutarse obligatoriamente fuera del horario laboral, en fines de semana o en ventanas de mantenimiento específicas previamente programadas?

RESPUESTA:

Las pruebas de Ethical Hacking y *penetration testing* deberán ser debidamente planificadas y coordinadas, con el propósito de minimizar cualquier impacto en la operación y en la disponibilidad de los servicios de INFICALDAS.
De manera preferente, dichas pruebas deberán ejecutarse fuera del horario laboral normal, en fines de semana o durante ventanas de mantenimiento previamente programadas, especialmente cuando se trate de sistemas críticos o exista riesgo de afectación a los usuarios finales.

No obstante, cuando el nivel de riesgo operativo sea bajo, y siempre que se cuente con la autorización expresa de la entidad y la coordinación previa con las áreas técnicas y de negocio, las pruebas podrán realizarse en horario laboral, preferiblemente sobre sistemas no críticos o entornos de prueba.

En todos los casos, el contratista deberá informar oportunamente, documentar la ejecución de las pruebas y dar cumplimiento a los lineamientos de seguridad de la información y de cumplimiento normativo definidos por la entidad, sin afectar la continuidad del servicio.

9. ¿El alcance del servicio de Ethical Hacking contempla únicamente aplicaciones web tradicionales (acceso por navegador), o también debe incluir la evaluación de: APIs REST/SOAP, servicios web, aplicaciones móviles Android/iOS, servicios de microservicios, u otras arquitecturas?

RESPUESTA:

El alcance del servicio de Ethical Hacking deberá incluir la evaluación de todas las arquitecturas y componentes relevantes que formen parte de los activos tecnológicos de INFICALDAS, comprendiendo, pero no limitado a:

- Aplicaciones web tradicionales (acceso por navegador).
- APIs REST/SOAP y servicios web.
- Aplicaciones móviles (Android/iOS).
- Servicios de microservicios y otras arquitecturas o plataformas críticas utilizadas por la entidad.

Lo anterior se entiende sin perjuicio de la inclusión de otros componentes tecnológicos que la entidad determine como relevantes, con el fin de garantizar una cobertura integral de seguridad sobre los activos de información.

10. ¿Cuántos empleados, contratistas y colaboradores tiene actualmente INFICALDAS en total? ¿Cuántos de ellos tienen cuenta de correo electrónico corporativo y deben ser incluidos en las campañas mensuales de phishing simulado y pruebas de ingeniería social?

RESPUESTA:

INFICALDAS cuenta aproximadamente con ciento diez (110) personas que disponen de cuenta de correo electrónico corporativo, incluyendo empleados, contratistas y colaboradores.
Todas estas personas deberán ser incluidas obligatoriamente en las campañas mensuales de phishing simulado y en las pruebas de ingeniería social, con el fin de garantizar la efectividad de las acciones de sensibilización y fortalecimiento de la seguridad de la información en la entidad.

11. Respecto a las 6 actividades de sensibilización y capacitación en seguridad de la información mencionadas en el Anexo "E. Sensibilización y Capacitación": ¿Se trata de 6 sesiones distintas dirigidas al mismo grupo de 50 participantes (una sesión por tema, 50 personas capacitadas en total), o son 6 grupos diferentes de 50 personas cada uno totalizando 300 personas capacitadas?

RESPUESTA:

Las seis (6) actividades de sensibilización y capacitación en seguridad de la información, mencionadas en el Anexo *"E. Sensibilización y Capacitación"*, estarán dirigidas al mismo grupo de hasta cincuenta (50) participantes, con cada sesión abordando un tema diferente.
En consecuencia, el total de participantes capacitados será de hasta 50 personas, sin generar obligación de multiplicar el número de grupos por sesión.

12. ¿Las 6 actividades de capacitación y sensibilización deben impartirse obligatoriamente de manera 100% presencial en instalaciones de INFICALDAS en Manizales, o se acepta modalidad virtual sincrónica (videoconferencia) o modalidad híbrida? En caso de requerir presencialidad, ¿INFICALDAS dispone de auditorio o sala de capacitaciones con capacidad y equipamiento audiovisual necesario?

RESPUESTA:

Las 6 actividades de capacitación y sensibilización no deben impartirse obligatoriamente de manera 100% presencial; pueden ser presenciales, virtuales o una combinación de ambas modalidades, según lo determine INFICALDAS.

13. ¿Cuál es el tiempo máximo (SLA) establecido por INFICALDAS para la remediación de vulnerabilidades una vez identificadas en los análisis mensuales, diferenciado por nivel de criticidad? Es decir: vulnerabilidades críticas (_____horas/días), altas (__ días), medias (__ días), bajas (__ días). Esta información nos permite dimensionar el equipo de respuesta y establecer compromisos contractuales realistas.

RESPUESTA:

INFICALDAS establece que los servicios de monitoreo de seguridad (*SIEM* y *SOC*) deberán operar de manera continua, las 24 horas del día, los 7 días de la semana, durante todo el año, cubriendo servidores, archivos y firewalls críticos de la entidad.

El proveedor deberá gestionar incidentes de seguridad mediante actividades técnicas de detección, análisis y mitigación aplicadas a los activos críticos, asegurando una respuesta rápida y efectiva ante amenazas.
El sistema SIEM deberá generar alertas automatizadas basadas en reglas predefinidas y ser capaz de adaptarse a nuevas amenazas, facilitando la mitigación en tiempo real de vulnerabilidades y riesgos detectados.

Se aclara que el contrato no establece tiempos máximos fijos de remediación por nivel de criticidad, por lo que la priorización y el dimensionamiento del equipo se deberá realizar conforme a buenas prácticas de seguridad de la información y criterios de riesgo definidos por la entidad, sin que ello implique ampliación del alcance contractual.

14. El análisis mensual de vulnerabilidades mencionado en el pliego: ¿Debe consistir únicamente en escaneo automatizado mediante herramientas especializadas (Nessus, Qualys, OpenVAS, etc.), o también debe incluir análisis manual por parte de profesionales, validación técnica de hallazgos, confirmación de falsos positivos, y pruebas de concepto (PoC) de vulnerabilidades críticas?

RESPUESTA:

El análisis mensual de vulnerabilidades deberá incluir una combinación de escaneo automatizado y análisis manual, ejecutado por profesionales calificados.
Dicho análisis deberá contemplar, entre otros aspectos:

- Validación técnica de los hallazgos identificados por las herramientas automatizadas.
- Confirmación de falsos positivos, asegurando la precisión de los resultados.
- Pruebas de concepto (PoC) para las vulnerabilidades críticas, cuando sea necesario, con el fin de evaluar su impacto real sobre los activos de la entidad.

Esta metodología garantiza una gestión integral y robusta de vulnerabilidades, alineada con las mejores prácticas internacionales en seguridad de la información y los requerimientos técnicos y normativos establecidos en el pliego de condiciones.

15. ¿Existe un proceso documentado de gestión de excepciones para vulnerabilidades que no puedan

remediarse en el tiempo estipulado debido a dependencias operativas, restricciones del fabricante, falta de parches disponibles, o incompatibilidades tecnológicas? ¿Quién aprueba formalmente estas excepciones (Comité de Seguridad, Gerencia de TI, ¿Auditoría)? Esta aclaración es crítica para delimitar responsabilidades contractuales.

RESPUESTA:

Sí, INFICALDAS cuenta con un proceso documentado de gestión de excepciones para vulnerabilidades que no puedan ser remediadas dentro del plazo estipulado, debido a dependencias operativas, restricciones del fabricante, falta de parches disponibles o incompatibilidades tecnológicas.
El proceso contempla las siguientes etapas:

- Identificación de la vulnerabilidad y condiciones que impiden su remediación.
- Justificación técnica y análisis de riesgo asociado.
- Solicitud formal de excepción ante los órganos responsables.
- Revisión y aprobación por parte del Comité de Seguridad.
- Seguimiento periódico de las excepciones aprobadas y registro documental completo de todas las actuaciones.

Lo anterior permite delimitar responsabilidades contractuales, asegurando que las excepciones sean gestionadas de manera formal, controlada y alineada con las políticas de seguridad de la información de la entidad.

16. ¿Cuáles son los tiempos máximos de respuesta esperados por parte del SOC (Security Operations Center) ante alertas de seguridad generadas por el SIEM, diferenciados por nivel de severidad? Ejemplo: alertas críticas (___minutos), altas (___horas), medias (___horas), bajas (___días).

RESPUESTA:

INFICALDAS establece que los servicios de monitoreo de seguridad (SIEM y SOC) deberán operar de manera continua, las 24 horas del día, los 7 días de la semana, durante todo el año, cubriendo servidores, archivos y firewalls críticos de la entidad.
El proveedor deberá gestionar incidentes de seguridad mediante actividades de detección, análisis y mitigación aplicadas a los activos críticos, asegurando una respuesta rápida y efectiva ante amenazas. El sistema SIEM deberá generar alertas basadas en reglas predefinidas, adaptándose a nuevas amenazas y facilitando la mitigación en tiempo real.
Los tiempos máximos de respuesta recomendados, según nivel de severidad de la alerta, son los siguientes:

- Alertas críticas: Respuesta inmediata, idealmente en menos de 30 minutos.
- Alertas altas: Respuesta en menos de 2 horas.
- Alertas medias: Respuesta en menos de 8 horas.
- Alertas bajas: Respuesta en menos de 24 horas, dependiendo del impacto y la criticidad.

Estos tiempos son orientativos y podrán ajustarse de acuerdo con las políticas internas y los acuerdos de nivel de servicio (SLA) definidos por INFICALDAS, garantizando prioridad absoluta en la atención de alertas críticas y la gestión eficiente de todos los incidentes de seguridad.

17. El servicio de monitoreo y correlación de eventos SIEM: ¿Debe operar de manera 100% ininterrumpida 24x7x365 sin excepciones (disponibilidad 99.9% o superior), o se aceptan ventanas de mantenimiento programadas previamente acordadas? En caso de aceptar mantenimientos, ¿cuál es la frecuencia y duración máxima permitida?

RESPUESTA:

El servicio de monitoreo y correlación de eventos SIEM deberá operar de manera ininterrumpida 24x7x365, garantizando una disponibilidad mínima del 99,9%.

No obstante, se aceptan ventanas de mantenimiento programadas, siempre que:

1. Sean previas y formalmente acordadas con INFICALDAS.
2. Sean mínimas y notificadas oportunamente a la entidad.
3. Su frecuencia y duración máxima se definan en el Acuerdo de Nivel de Servicio (SLA), recomendando que no superen de 2 a 4 horas mensuales y se ejecuten en horarios de bajo impacto operativo para la entidad.

Lo anterior permite garantizar la continuidad operativa del servicio sin afectar la seguridad de la información ni los compromisos contractuales establecidos.

18. ¿El contrato establece penalizaciones o multas económicas por incumplimiento de SLAs (tiempos de respuesta, disponibilidad del servicio, entrega tardía de informes mensuales/trimestrales)?

RESPUESTA:

El contrato no establece penalizaciones o multas específicas por incumplimiento de SLAs (tiempos de respuesta, disponibilidad del servicio, entrega de informes, etc.).

Sin embargo, el cumplimiento del contrato está respaldado mediante la constitución de una garantía única a favor de INFICALDAS, que podrá consistir en póliza de seguro expedida por una compañía legalmente establecida en Colombia o garantía bancaria otorgada por un banco local, con los siguientes amparos:

- Cumplimiento, incluyendo amparo de posibles multas y cláusula penal pecuniaria: 20% del valor del contrato, vigente por el plazo de ejecución más cuatro (4) meses.
- Calidad del servicio: 20% del valor del contrato, vigente por el plazo de ejecución más cuatro (4) meses.
- Pago de salarios, prestaciones e indemnizaciones laborales: 20% del valor del contrato, vigente por el plazo de ejecución más tres (3) años.

19. ¿INFICALDAS cuenta actualmente con certificación vigente en la norma ISO/IEC 27001:2022 (o versión anterior 2013 en proceso de transición), o el Sistema de Gestión de Seguridad de la Información debe implementarse, documentarse, madurar y certificarse por primera vez durante la vigencia 2026? Favor indicar estado actual de certificación y fecha de última auditoría de certificación o seguimiento.

RESPUESTA:

INFICALDAS no cuenta actualmente con certificación vigente en la norma ISO/IEC 27001:2022 ni en su versión anterior 2013.

La última auditoría interna del Sistema de Gestión de Seguridad de la Información (SGSI) se realizó del 21 de noviembre al 15 de diciembre de 2025, y el informe final fue presentado el 15 de diciembre de 2025.

En consecuencia, el SGSI deberá implementarse, documentarse, madurar y certificarse por primera vez durante la vigencia 2026, conforme a los requerimientos de la norma y los procedimientos establecidos por INFICALDAS para la obtención de la certificación.

20. ¿Cuáles fueron los hallazgos, no conformidades, observaciones u oportunidades de mejora principales identificados en la última auditoría interna de seguridad de la información, auditoría de certificación ISO 27001, o inspección realizada por la Superintendencia Financiera de Colombia, que deban ser atendidos prioritariamente por el contratista durante la vigencia 2026? Favor proporcionar informe ejecutivo de auditoría (puede ser con información sensible omitida).

RESPUESTA:

Principales Hallazgos, No Conformidades y Oportunidades de Mejora La última auditoría interna al Sistema de Gestión de Seguridad de la Información (SGSI) de INFICALDAS se realizó **del 21 de noviembre al 15 de diciembre de 2025**.

1. Contexto, Alcance y Partes Interesadas (Cláusulas 4.1 a 4.3)

- Si bien existen definiciones documentadas, se identifican vacíos en la integración del cambio climático, justificación de exclusiones de controles y descripción de interfaces con proveedores externos.

2. Liderazgo, Roles y Política (Cláusulas 5.1 a 5.3)

- El compromiso de la alta dirección es evidente, pero hay debilidades en la designación formal de responsables del SGSI y en la comunicación externa de la política.

3. Gestión de Riesgos (Cláusulas 6.1 a 6.3 y 8.2 a 8.3)

- Existe una metodología aplicada, pero se detectan debilidades en la trazabilidad documental, aprobación formal del plan de tratamiento y aceptación del riesgo residual.

4. Recursos, Competencias y Conciencia (Cláusulas 7.1 a 7.3)

- Los roles están definidos, pero falta integración homogénea de competencias SGSI y evaluación formal de la comprensión de consecuencias del incumplimiento.

5. Operación y Control (Cláusula 8)

- La gestión de cambios está documentada, pero hay baja apropiación por parte de los líderes de proceso y limitada integración del SGSI en la operación diaria.

6. Evaluación del Desempeño y Mejora (Cláusulas 9 y 10)

- Existen indicadores y auditoría interna, pero no hay un ciclo formal y documentado de mejora continua del SGSI.

7. Proceso de Servicios Financieros

- Se identifican debilidades en la integración explícita del SGSI en la caracterización del proceso, planificación de gestión de incidentes, gestión de accesos, inventario de activos y apropiación de procedimientos operativos documentados.

Recomendaciones Estratégicas Prioritarias para 2026

1. **Consolidar el contexto, alcance y partes interesadas** en un documento integral, incluyendo interfaces con proveedores y requisitos de la Enmienda AMD 1.
2. **Designar formalmente al responsable del SGSI** y definir mecanismos claros de reporte a la Alta Dirección.
3. **Formalizar y aprobar el Plan de Tratamiento de Riesgos**, asegurando la aceptación explícita de riesgos residuales y trazabilidad documental.
4. **Integrar el SGSI en la operación de procesos misionales y de apoyo**, especialmente en Servicios Financieros.
5. **Fortalecer la gestión de competencias y la toma de conciencia** en seguridad de la información, con formación diferenciada y evaluaciones formales.
6. **Asegurar la implementación efectiva de controles**, verificando su aplicación y eficacia en la operación diaria.
7. **Estandarizar y documentar el ciclo de mejora continua** del SGSI, integrando resultados de indicadores, auditorías, incidentes y planes de acción.
8. **Reforzar la integración del SGSI con la gestión del riesgo institucional**, asegurando trazabilidad y alineación con la gobernanza corporativa.

21. Respecto al Reporte F408 trimestral a la Superintendencia Financiera de Colombia sobre indicadores de Seguridad de la Información y Ciberseguridad:

¿INFICALDAS ya reporta actualmente el F408 de manera regular o será la primera vez que lo presentará en 2026? ¿Existe una plantilla, formato o lineamiento específico definido por la SFC o por INFICALDAS para la elaboración de este reporte? Favor compartir formato si está disponible.

RESPUESTA:

INFICALDAS ha venido reportando regularmente el Formulario F408 a la Superintendencia Financiera de Colombia (SFC) durante varios años, por lo que no se trata de la primera presentación en 2026.
Existe un formato y lineamientos específicos previamente definidos por la SFC, que INFICALDAS ha venido utilizando para la elaboración del reporte. Dicho formato se adjuntará al proceso para conocimiento de los proponentes y para garantizar que la información requerida sea reportada de manera consistente y conforme a los criterios regulatorios.

22. ¿INFICALDAS cuenta actualmente con una solución de DLP (Data Loss Prevention) implementada, licenciada y en operación que deba ser administrada, gestionada y optimizada por el contratista, o este debe proveer, adquirir licencias, implementar, configurar y poner en operación una solución DLP completamente nueva desde cero?

RESPUESTA:

INFICALDAS no cuenta actualmente con una solución DLP implementada operativa que deba ser utilizada por el contratista. En consecuencia, el contratista que resulte seleccionado deberá proveer, implementar y configurar una solución DLP desde cero, conforme a los requerimientos técnicos, funcionales y normativos definidos en el pliego de condiciones, y en armonía con las mejores prácticas internacionales en seguridad de la información, tales como la ISO/IEC 27001:2022, así como los lineamientos y directrices emitidos por el MINTIC.

23. ¿El alcance de la solución DLP debe cubrir únicamente protección en endpoints (estaciones de trabajo y portátiles), o también debe incluir: protección de correo electrónico (gateway), monitoreo de tráfico de red, control de almacenamiento en servicios cloud (OneDrive, Google Drive, Dropbox), ¿y gestión de dispositivos móviles corporativos? Favor especificar alcance completo y cantidad de licencias por módulo.

RESPUESTA:

De acuerdo con la información disponible, el control de DLP (Data Loss Prevention)
está orientado a proteger los dispositivos de la entidad. Específicamente, se contempla la instalación del agente DLP en todos los equipos, sin distinción entre equipos críticos y no críticos, lo que garantiza una cobertura total frente a la fuga de datos. Esta medida permite monitorear, prevenir y gestionar los riesgos asociados al manejo de información sensible en todos los endpoints de la organización.

En cuanto a la cantidad de dispositivos, la infraestructura tecnológica de INFICALDAS está compuesta por:

- 50 equipos de cómputo
- 9 servidores
- 1 firewall
- 2 equipos activos de red
- 4 Access Poin

- INFICALDAS cuenta aproximadamente con ciento diez (110) personas que disponen de cuenta de correo electrónico corporativo

24, ¿Qué versión de Microsoft Active Directory utiliza actualmente INFICALDAS (Windows Server 2012 R2, 2016, 2019, 2022)? ¿Cuántos dominios tiene configurados? ¿Cuántos controladores de dominio (Domain Controllers) están en operación y en qué ubicaciones físicas? ¿Existe bosque de dominio multi-dominio o dominio único? Esta información es crítica para dimensionar las actividades de auditoría y fortalecimiento de políticas de seguridad.

RESPUESTA:

Windows Server 2022, un dominio, un controlador ubicado en las instalaciones de la entidad, una maquina virtual sobre Vmware.

25. ¿INFICALDAS utiliza actualmente soluciones de autenticación multifactor (MFA/2FA) tales como Microsoft Azure MFA, Duo Security, Google Authenticator, tokens físicos, u otras? ¿Para qué sistemas y usuarios es obligatorio el uso de MFA (acceso remoto VPN, administradores, usuarios privilegiados, todos los usuarios)? Favor detallar implementación actual y cobertura.

RESPUESTA:

INFICALDAS utiliza actualmente soluciones de autenticación multifactor (MFA/2FA) para fortalecer la seguridad de sus sistemas críticos, con la siguiente implementación y cobertura:

- Duo Security: utilizado para el acceso remoto VPN de los funcionarios.
- Microsoft Authenticator: implementado para el acceso a correo corporativo (Office 365).
- FortiToken: requerido para el acceso a dispositivos de seguridad de red, específicamente FortiGate.

El uso de MFA es obligatorio para los sistemas críticos mencionados y para los usuarios que acceden a ellos, garantizando así protección de la infraestructura y de la información sensible de la entidad, conforme a las mejores prácticas de seguridad de la información.

26. ¿INFICALDAS cuenta con Planes de Continuidad del Negocio (BCP - Business Continuity Plan) y Planes de Recuperación ante Desastres (DRP - Disaster Recovery Plan) formalmente documentados, aprobados por la Alta Dirección, y probados mediante simulacros, o estos planes deben elaborarse completamente

RESPUESTA:

INFICALDAS cuenta actualmente con un Plan de Recuperación ante Desastres (DRP) implementado con su proveedor de servicios. La última prueba/simulacro del DRP se realizó el 28 de noviembre de 2025.

En consecuencia, no será necesario elaborar un DRP desde cero durante la vigencia 2026, aunque cualquier actualización o ajuste requerido por cambios en la infraestructura tecnológica o por nuevas políticas de seguridad

deberá ser incorporado conforme a las buenas prácticas de continuidad del negocio y recuperación ante desastres, garantizando la aprobación de la Alta Dirección y la ejecución de pruebas periódicas.

27. ¿Cuáles son los valores de RPO (Recovery Point Objective - pérdida máxima de datos aceptable) y RTO (Recovery Time Objective - tiempo máximo de recuperación aceptable) establecidos por INFICALDAS para cada uno de sus sistemas críticos de información (ERP, Gestión Documental, Active Directory, File Server, bases de datos)?

RESPUESTA:

Los valores de RPO (Recovery Point Objective) y RTO (Recovery Time Objective) para los sistemas críticos de INFICALDAS se determinan considerando tanto las pruebas de restauración realizadas como la configuración de backups y replicación de datos hacia la nube y el datacenter alterno del proveedor.

- Pruebas de restauración: se ha verificado que el RTO y RPO para los sistemas críticos (ERP, Gestión Documental, Active Directory, File Server y bases de datos) son aproximadamente 6 segundos, reflejando la capacidad de recuperación de la infraestructura actual.

- Backups y replicación: el proveedor deberá configurar las tareas de backup y traslado de datos a la nube, así como la replicación de máquinas virtuales al datacenter alterno. El RPO final estará determinado por la frecuencia de estos backups y réplicas, dado que el contrato no establece un intervalo específico de pérdida máxima de datos aceptable.

Esta configuración garantiza la continuidad operativa y la recuperación eficiente de los sistemas críticos de la entidad, asegurando la resiliencia ante incidentes y alineándose con las mejores prácticas de gestión de continuidad de negocio.

28. Cómo está estructurado el esquema de pagos durante la vigencia del contrato: mensual, bimestral, trimestral, ¿o asociado a entregables específicos? ¿Está contemplado algún porcentaje de anticipo que permita al contratista realizar las inversiones iniciales en licenciamiento de software especializado (SIEM, DLP, plataformas de capacitación)?

RESPUESTA:

El contrato no contempla pagos anticipados para el contratista.

La forma de pago será mediante pagos parciales asociados a cada entrega o cumplimiento de obligaciones, de acuerdo con lo siguiente:

1. Autorización del supervisor que certifique el cumplimiento de las condiciones técnicas y de calidad de los bienes o servicios recibidos.
2. Presentación de la factura correspondiente, cumpliendo con los requisitos exigidos por la ley.
3. Constancia de cumplimiento de obligaciones con el sistema integral de seguridad, dejando claro que INFICALDAS adquiere obligaciones únicamente con el adjudicatario del proceso, y no efectuará pagos a terceros.

De esta manera, los pagos se realizarán tras la verificación y aceptación de los entregables, garantizando el cumplimiento técnico, de calidad y normativo, sin que exista obligación de anticipar recursos para inversiones iniciales en licenciamiento u otras plataformas.

29. El presupuesto oficial establecido en el pliego de condiciones por valor de DOSCIENTOS VEINTINUEVE MILLONES SETECIENTOS SETENTA Y DOS MIL QUINIENTOS PESOS M/CTE ($229.772.500) "INCLUIDO IVA, Y TODOS LOS IMPUESTOS A QUE HUBIESE LUGAR": ¿Este valor incluye las estampillas departamentales obligatorias (Pro-Desarrollo 1%, Pro-Universidad 2%, Pro- Adulto mayor 3%, Pro-Hospital 1%, Pro-Cultura 1%, totalizando 8%), o estas estampillas se descuentan del valor bruto del contrato?

RESPUESTA

El valor estimado del contrato se fija en DOSCIENTOS VEINTINUEVE MILLONES SETECIENTOS SETENTA Y DOS MIL QUINIENTOS PESOS M/CTE ($229.772.500), incluido el IVA (si aplica), todos los impuestos, contribuciones, estampillas y la totalidad de los costos directos e indirectos que correspondan.

En consecuencia, el presupuesto oficial ya contempla las estampillas departamentales obligatorias (Pro-Desarrollo 1%, Pro-Universidad 2%, Pro-Adulto Mayor 3%, Pro-Hospital 1%, Pro-Cultura 1%, totalizando 8%) y no se descontarán adicionalmente del valor bruto del contrato.

30. ¿Existe actualmente un contratista, proveedor o consultor prestando servicios similares o parciales de seguridad de la información, gestión de SGSI, o monitoreo de seguridad para INFICALDAS? En caso afirmativo: ¿Se requiere un período de empalme y transferencia de conocimiento entre el contratista saliente y el entrante? ¿Cuál es la fecha límite para el inicio de operación completa del servicio? ¿Existe documentación técnica, configuraciones, o entregables del contratista actual que deban ser transferidos al nuevo contratista?

RESPUESTA:

Actualmente, existe un proveedor encargado de la prestación del servicio. No se requiere empalme ni transferencia de conocimiento, dado que cada proveedor opera de manera autónoma en el uso de sus herramientas y en la prestación del servicio.
No existen documentos ni entregables que deban ser transferidos; la información necesaria para la operación será suministrada directamente por la entidad.
La fecha límite para el inicio de operación por parte del nuevo proveedor será de 2 días contados a partir de la adjudicación y entrega de la información necesaria.

Manizales, 29 de diciembre de 2025.

JOHN JAIRO GIRALDO VILLA
Profesional Especializado Sistemas