## CONTENIDO DEL INFORME



## 1. CONDICIONES DEL CONTRATO

| | |
|---|---|
| Número de Contrato: | 3.122-2025 |
| Nombre del Contratista: | **Francisco José Ariza Pastor** |
| Periodo informe: | 01 al 30 de Septiembre de 2025 |
| Supervisor: | **Diego Fernando Huertas Ortiz** |
| Área perteneciente: | Dirección de Tecnología |

## 2. OBJETO DEL CONTRATO

Prestar los servicios profesionales para asesorar a la Dirección de Tecnología en la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI), de acuerdo con la política de Gobierno Digital y Seguridad Digital, así como validar y verificar los planes de mitigación y remediación de riesgos y la implementación de controles tecnológicos.

## 3. OBLIGACIONES DEL CONTRATO, ACTIVIDADES EJECUTADAS Y PRODUCTOS ENTREGADOS

Las obligaciones adquiridas son las siguientes:

**1. Realizar el seguimiento al plan de cierre de brechas generado a partir de los resultados de la actualización del autodiagnóstico del modelo de seguridad y privacidad de la información del MHCP.**

**Avance: 89%**

- Se realizó la revisión de las brechas identificadas en los distintos dominios del FURAG, lo que permitirá establecer planes de mejora orientados al fortalecimiento de la gestión institucional, optimizar los niveles de cumplimiento y avanzar en la consolidación de las capacidades de la entidad en materia de seguridad digital y gobierno de la información.

**2. Realizar el seguimiento al Plan de Tratamiento de Riesgos y Privacidad de la Información para el MHCP.**

**Avance: 89%**

- Durante el mes de septiembre, se llevaron a cabo capacitaciones en seguridad de la información dirigidas a los lideres de procesos relacionada con los riegos de seguridad digital.

**3. Proyectar las respuestas a los requerimientos relacionados con el estado de implementación del Modelo seguridad y privacidad de la información MSPI del MHCP y de la Política de Seguridad Digital.**

**Avance: 89 %**

- Se emitió respuesta a la propuesta comercial presentada por la compañía INTERNEXA, relacionada con la oferta de una solución de Centro de Operaciones de Seguridad (SOC) para la entidad.
- Se atendió la solicitud contenida en el memorando SIED-20/2025/TIPOCDI, mediante el cual se requería la entrega del backup correspondiente al periodo comprendido entre el 1 de enero y el 31 de octubre de 2019 de una funcionaria.

**4. Apoyar la implementación del procedimiento de gestión de activos de información en coordinación con las demás áreas de la Entidad competentes.**

**Avance: 89 %**

- Se culminó de manera satisfactoria el levantamiento de los activos de información correspondientes a los 43 procesos de la entidad, con el objetivo de identificar y mitigar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información crítica del Ministerio de Hacienda y Crédito Público (MHCP).

**5. Participar en la actualización del Sistema de Gestión de la Seguridad de la Información – SGSI para el proceso de gestión de TIC, en lo referente a análisis de riesgos, vulnerabilidades y controles, bajo la norma ISO 27001:2022 o las actualizaciones que se realicen a la misma.**

**Avance: 89 %**

- Se llevó a cabo la revisión del MSPI y, para la presente vigencia, se tiene previsto realizar la modificación al Manual de Seguridad y Privacidad de la entidad, la implementación del proceso de etiquetado de la información y la emisión de la Resolución de adopción del MSPI.

**6. Apoyar la realización de los Comités de Seguridad que sean indicados por el Supervisor del Contrato.**

**Avance: 89 %**

- Se realiza en el mes de septiembre dos (2) reunión con el Director de Tecnología donde se presenta los avances y mejoras al MSPI y las iniciativas de Seguridad y Privacidad de la Información para la vigencia 2025.
- Se asiste al comité operativo y seguridad de SIIF Nación.

**7. Realizar la elaboración y actualización de las estrategias de análisis de seguridad periódicos para sistemas de procesos misionales críticos, incluyendo aquellas condiciones de seguridad que deben cumplir los futuros contratista que ejecuten proyectos o presten servicios al Ministerio con Componentes tecnológicos**.

**Avance: 89 %**

- Para la vigencia 2025 se han realizado cuatro (4) pruebas de vulnerabilidades sobre activos críticos de la Entidad y dos (2) pruebas de penetración sobre portales web institucionales, las cuales arrojaron vulnerabilidades de tipo medio. Lo anterior indica la necesidad de implementar planes de remediación oportunos y efectivos, reforzar los controles de seguridad existentes y mantener un monitoreo continuo que permita reducir los riesgos asociados a la explotación de dichas vulnerabilidades.

**8. Participar en la definición de soluciones requeridas para remediar vulnerabilidades y mitigar riesgos reportados en los análisis de seguridad, para el Ministerio.**

**Avance: 89 %**

- A través de la correlación de eventos de Qradar se procesaron 4,1 millones de eventos correspondiente a 42 activos críticos, de los cuales se desprenden 99 casos de usos parametrizados en la herramienta de monitoreo perimetral, evidenciando que el alertamiento de seguridad que más recurrente para el mes de Septiembre fue el de intento de intrusión, seguido con obtención de información y contenido dañino.

**9. Efectuar la revisión, actualización y elaboración de nuevos procedimientos y/o modificación de los existentes, de auditoría, trazabilidad y seguimiento que puedan ser aplicados y/o implementados en los servicios tecnológicos y en los sistemas de información de la entidad.**

**Avance: 89 %**

- Actualmente, las etiquetas de información se habilitaron en ambiente de prueba dentro de la suite de Office, lo que permitirá realizar validaciones y ajustes antes de su implementación en producción. Esta fase busca garantizar que las etiquetas contribuyan de manera efectiva a la clasificación, protección y trazabilidad de la información sensible de la entidad, fortaleciendo la postura de seguridad digital y el cumplimiento de los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información.

**10. Proponer procesos o procedimientos que aseguren la integridad, disponibilidad y confidencialidad de los datos utilizados en los sistemas de información de la entidad, así como procedimientos para trazabilidad, auditoría de transacciones o acciones para el registro de eventos de creación, actualización, modificación o borrado de información.**

**Avance: 89 %**

- Se efectuó el bloqueo del acceso a WhatsApp Web en los equipos conectados al dominio del MHCP, con el fin de fortalecer la seguridad digital de la entidad, reducir los riesgos asociados a la fuga de información y mitigar posibles vectores de ataque derivados del uso de aplicaciones de mensajería no autorizadas en el entorno corporativo.

**11. Brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos**

**Avance: 89 %**

- Se atendió un incidente de seguridad relacionado con la sospecha de actividad de tipo RAT (REMCOS), detectado el 25 de septiembre de 2025. El hallazgo incluyó la identificación de un ejecutable sospechoso generado mediante MSI, la caída de múltiples DLL en la ruta C:\ProgramData\Comsync\, así como la presencia de un ejecutable temporal que intentaba establecer comunicación con el dominio coldalt.coldalt.com, comportamiento asociado a la táctica TA0011 – Command and Control (C2) del marco MITRE ATT&CK.

**12. Participar en la realización de las actividades necesarias para identificar los componentes de Infraestructura Crítica Cibernética, de acuerdo con los lineamientos que, para tal fin, establezcan las instancias del Estado.**

**Avance: 89 %**

- Se participó en reunión del sector Hacienda, convocada por el COLCERT orientado a la identificación de la infraestructura crítica del país, con el propósito de conocer lineamientos estratégicos, amenazas emergentes y buenas prácticas para la protección de activos esenciales a nivel nacional.

**13. Mantener estricta reserva y confidencialidad sobre la información y datos que conozca por causa o con ocasión de la ejecución del contrato.**

**Avance: 89 %**

- Se garantizó la reserva de la información en el marco de las actividades realizadas para el mes Septiembre.

**14. Realizar la transferencia de conocimiento de las actividades del contrato a los funcionarios del MHCP y las personas que indique el supervisor del contrato, entregando el soporte documental que corresponda en cada caso.**

**Avance: 89 %**

- Durante el mes de Septiembre, se llevaron a cabo cinco (5) jornadas de capacitación en seguridad de la información, dirigidas a los líderes de proceso, con el objetivo de socializar la metodología para el levantamiento de los riesgos de seguridad digital, en el marco del fortalecimiento del Modelo de Seguridad y Privacidad de la Información de la entidad.

**Productos del contrato**
Los productos y entregables del contrato se relacionan en el siguiente Link:

Septiembre

Francisco Ariza Pastor
**Contratista**
C.C. 72.285.893

En mi calidad de supervisor del contrato me permito avalar el contenido del informe y el avance en la ejecución del mismo de acuerdo a lo descrito.

El contrato no presenta a la fecha dificultades en su ejecución, ni situaciones exógenas que afecten el normal desarrollo del mismo.

**FIRMA SUPERVISOR**

HUERTAS ORTIZ DIEGO FERNANDO
Firmado digitalmente por HUERTAS ORTIZ DIEGO FERNANDO
Fecha: 2025.10.01 14:48:45 -05'00'

Diego Fernando Huertas Ortiz
**Director de Tecnología**
C.C. 79.783.893