## 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 Noviembre 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: 90%**

Para el plan de cierre de brechas de la vigencia 2025, se adelantaron las siguientes actividades en el marco del fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI):

- Se realizó el levantamiento y registro de activos de información de 39 procesos misionales y de apoyo de la entidad.
- Se emitió y socializó la Política de Etiquetado y Clasificación de la Información, alineada con los lineamientos del MinTIC y las buenas prácticas de seguridad digital.

- Se efectuó el levantamiento de riesgos de seguridad digital de 101 activos críticos del Ministerio, incluyendo activos tecnológicos, de información y servicios esenciales.
- Se implementó el bloqueo de WhatsApp Web para mitigar riesgos de fuga o exposición no autorizada de información institucional.
- Dentro del plan de mejora continua del MSPI, se realizó la modificación y actualización del Plan de Seguridad y Privacidad de la Información del MHCP, incorporando controles ajustados a las necesidades de la entidad y a las recomendaciones de auditoría.
- Estas acciones permiten avanzar en el fortalecimiento de la seguridad digital, la gestión de riesgos y la madurez del MSPI para la vigencia 2025.

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

**Avance: 90%**

- Como parte del fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), se llevó a cabo la identificación y caracterización de 4 riesgos de seguridad digital, los cuales fueron evaluados sobre los 101 activos críticos institucionales. Este ejercicio permitió determinar vulnerabilidades, impactos y controles requeridos para reducir el riesgo residual y orientar la toma de decisiones.

**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: 90 %**

- Se elaboró el proyecto de respuesta dirigido al Grupo de Transformación Digital, relacionado con el levantamiento de la infraestructura crítica del sector Hacienda, en el marco de las acciones de fortalecimiento de la seguridad digital y la identificación de activos esenciales para la continuidad de los servicios misionales.

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

**Avance: 90 %**

- 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: 90 %**

- En el marco del proceso de monitoreo y mejora continua del MSPI, se realizó el último análisis de vulnerabilidades sobre los activos críticos de la entidad, con el objetivo de identificar brechas de seguridad, evaluar el nivel de exposición tecnológica y priorizar las medidas de remediación.

  Este análisis permitirá fortalecer la postura de seguridad, reducir riesgos asociados a infraestructura misional y orientar las actividades del plan de mejora para la vigencia 2025.

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

**Avance: 90 %**

- Se realiza en el mes de Noviembre 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: 90 %**

- 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: 90 %**

- A través de la correlación de eventos de Qradar se procesaron 3,8 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 Noviembre 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: 90 %**

- En el marco de la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Hacienda y Crédito Público, se adelantó la revisión y actualización del procedimiento de atención de incidentes correspondiente al proceso Apo 1.3 – Gestión de la Seguridad de la Información, lo cual garantiza la eficacia en la identificación, análisis, contención y tratamiento oportuno de los incidentes de seguridad digital, fortaleciendo así la capacidad de respuesta ante eventos que puedan afectar la confidencialidad, integridad o disponibilidad de la información institucional.

**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: 90 %**

- Se dio la salida a producción de la Política de Etiquetado y Clasificación de la Información, documento que permitirá establecer reglas claras para la identificación, tratamiento y resguardo de la información institucional, conforme a su nivel de sensibilidad y criticidad. Esta política facilitará la aplicación coherente de controles de seguridad digital, reducirá el riesgo de fuga o manejo indebido de información y apoyará la toma de decisiones basada en el nivel de clasificación asignado.

**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: 90 %**

- Se realizó el informe forense del incidente de seguridad relacionado con la sospecha de actividad de tipo RAT (REMCOS), detectado el 25 de octubre 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: 90 %**

- 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: 90 %**

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

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: 90 %**

- Se brindó capacitación a los funcionarios del MHCP relacionada con la Política de Etiquetado y Clasificación de la Información, con el fin de fortalecer el adecuado manejo de los datos institucionales y promover la aplicación correcta de los niveles de clasificación definidos por la entidad.

**Productos del contrato**

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

Noviembre

Francisco Ariza Pastor
**Contratista**
C.C. 72.285.903

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: 2025.12.01 17:29:41 -05'00'

Diego Fernando Huertas Ortiz
**Director de Tecnología**
C.C. 79.783.903