Formato Riesgos de Estudios Previos Licitaciones Públicas

OBJETO:ADQUISICIÓN DE LICENCIAMIENTO POR SUSCRIPCIÓN (SAAS), IMPLEMENTACIÓN, TRANSFERENCIA DE CONOCIMIENTO Y SOPORTE TÉCNICO DE UNA SOLUCIÓN INTEGRAL DE PROTECCIÓN AVANZADA DE END POINTS PARA ESTACIONES DE TRABAJO Y SERVIDORES, INCLUYENDO CAPACIDADES EDR Y CONSOLA CENTRALIZADA DE ADMINISTRACIÓN Y MONITOREO PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA - CAR.

No	Clase	Fuente	Etapa	Tipo	Descripción (Que puede pasar y cómo puede ocurrir)	Consecuencia de la ocurrencia del evento	Probabilidad	Impacto	Valoración del Riesgo	Categoría	Sujeto Responsable	Tratamiento /Controles a ser implementados	Impacto después del tratamiento					Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y Revisión		
													Probabilidad	Impacto	3	Categoría	Afecta la ejecución del contrato?				Cómo se realiza el monitoreo?	Periodicidad	¿Cuando?
1	Específico	Externa	Ejecución	Riesgos Operacionales - corresponden a riesgos tecnológicos	Configuración inadecuada o funcionamiento parcial de las capacidades EDR/XDR contratadas.	Disminución de la capacidad de detección, análisis, contención y respuesta ante incidentes de seguridad informática.	(3) Posible	(3) Moderado	6	Riesgo medio	Contratista	Validación técnica de la configuración, ejecución de pruebas funcionales, revisión de políticas implementadas, verificación de cobertura y aprobación mediante actas de aceptación.	(1) raro	(2) Menor	3	Riesgo Bajo	Sí, si el tratamiento no es aplicado efectivamente.	Contratante	Una vez suscrita el acta de inicio	Terminado y liquidado el contrato	Informes de supervisión y validación técnica de la solución	Por periodos de pago	Cuando Aplique
2	Específico	Externa	Ejecución	Riesgos Operacionales - corresponden a riesgos tecnológicos	Fallas o dificultades en el despliegue de agentes e integración de la solución con la infraestructura tecnológica de la Entidad.	Equipos sin protección efectiva, retrasos en la implementación o cobertura incompleta de la solución.	(3)posible	(2) menor	5	Riesgo medio	Contratista	Validación previa de compatibilidad, pruebas piloto, despliegue controlado y seguimiento a la cobertura de los activos	(1) raro	(2) Menor	3	Riesgo Bajo	Sí, si el tratamiento no es aplicado efectivamente.	Contratante	Una vez suscrita el acta de inicio	Terminado y liquidado el contrato	Informe de gestión e informes de supervisión	Informes de implementación y seguimiento técnico	Cuando Aplique
3	General	Externa	Ejecución	Riesgo operacional	Incumplimiento en la entrega de las licencias.	No se logrará cumplir con lo planeado para la actual vigencia	(3)posible	(2) menor	5	Riesgo medio	Contratista	Verificación de la entrega de certificados de licenciamiento emitidos por el fabricante, validación del aprovisionamiento de las licencias en la consola o tenant institucional de la CAR, revisión de vigencias y conciliación de las cantidades contratadas frente a las efectivamente habilitadas.	(2) Improbable	(2) Menor	4	Riesgo Bajo	si el tratamiento aplicado es efectivo no se afecta la ejecución.	Contratante	Una vez suscrita el acta de inicio	Terminado y liquidado el contrato	Informe de supervisión	Bimensual	Cuando Aplique
4	Específico	Externa	Ejecución	Riesgos Operacionales - corresponden a riesgos tecnológicos	Licenciamiento no autorizado o proveedor sin acreditación oficial del fabricante para comercializar, implementar y soportar la solución ofertada.	Riesgos legales, limitaciones de soporte, afectación de garantías y posible incumplimiento contractual.	(2) Improbable	(3) moderado	5	Riesgo medio	Contratista	Verificación de certificaciones, cartas de autorización del fabricante y validación del licenciamiento suministrado a la Entidad.	(1) raro	(1) Insignificante	2	Riesgo Bajo	Sí, si el tratamiento no es aplicado efectivamente.	Contratante	una vez suscrita el acta de inicio	Terminado y liquidado el contrato	Revisión documental y validación de licencias	Una vez durante la implementación y cuando aplique	Cuando aplique

5	Específico	Externa	Ejecución	Riesgos Operacionales - corresponden a riesgos tecnológicos	Instalación de software antivirus no autorizado o no licenciado	Vulnerabilidad del sistema por uso de herramientas no certificadas	(3)posible	(2) menor	5	Riesgo medio	Contratista	Validación de licencias, revisión técnica del software instalado y control centralizado de instalaciones desde servidores administrados	(1) raro	(1) Insignificante	2	Riesgo Bajo	No, si el tratamiento es aplicado efectivamente	Contratante	una vez suscrita el acta de inicio	Terminado y liquidado el contrato	Informe de supervisión	Inmediatamente	Cuando aplique
6	Específico	Externa	Ejecución	Riesgos Operacionales - corresponden a riesgos tecnológicos	Incumplimiento de los niveles de servicio (SLA) establecidos para la disponibilidad de la plataforma, soporte técnico, atención de incidentes y tiempos de respuesta acordados contractualmente.	Afectación de la operación de la solución, retrasos en la atención de incidentes y disminución de la capacidad de monitoreo y administración de la plataforma.	(3)posible	(2) menor	5	Riesgo medio	Contratista	Seguimiento periódico de indicadores de SLA, revisión de reportes de disponibilidad y verificación del cumplimiento de tiempos de respuesta y solución.	(1) raro	(1) Insignificante	2	Riesgo Bajo	Sí, si el tratamiento no es aplicado de manera efectiva.	Contratante	una vez suscrita el acta de inicio	Terminado y liquidado el contrato	Informe de supervisión	Por periodos de pagos	Cuando aplique
7	Específico	Externa	Ejecución	Riesgos Operacionales - corresponden a riesgos tecnológicos	Retrasos en las actividades de instalación, configuración, puesta en operación y transferencia de conocimiento de la solución contratada.	Incumplimiento del cronograma contractual y retraso en la entrada en operación de los mecanismos de protección requeridos por la entidad.	(3)posible	(2) menor	5	Riesgo medio	Contratista	Seguimiento al plan de trabajo, verificación de hitos contractuales y realización de reuniones de seguimiento para identificar desviaciones y establecer acciones correctivas.	(1) raro	(1) Insignificante	2	Riesgo Bajo	Sí, si el tratamiento no es aplicado de manera efectiva.	Contratante	una vez suscrita el acta de inicio	Terminado y liquidado el contrato	Informe de supervisión y seguimiento al cronograma	Por periodos de pagos	Cuando aplique
8	Específico	Externa	Ejecución	Riesgos Operacionales - corresponden a riesgos tecnológicos	Retrasos en las actividades de instalación, configuración, puesta en operación y transferencia de conocimiento de la solución contratada.	Inconsistencias entre el inventario institucional de activos tecnológicos y los equipos efectivamente protegidos y monitoreados por la solución EDR/XDR.	(3)posible	(2) menor	5	Riesgo medio	Contratista	Conciliación periódica entre inventario institucional, consola EDR/XDR y reportes de cobertura entregados por el contratista.	(1) raro	(1) Insignificante	2	Riesgo Bajo	Sí, si el tratamiento no es aplicado efectivamente.	Contratante	una vez suscrita el acta de inicio	Terminado y liquidado el contrato	Revisión de reportes de cobertura y activos protegidos	Por periodos de pagos	Cuando aplique

Tabla Complementaria – Riesgos de Seguridad de la Información (No Hace parte de la Matriz Contractual)

"La siguiente tabla corresponde al análisis de riesgos de seguridad de la información exigido por ISO/IEC 27001:2022, y hace parte del SGSI institucional. Esta tabla no sustituye ni modifica la matriz de riesgos contractual del proceso, y se integra al SGSI como evidencia del tratamiento de riesgos asociados al servicio o bien adquirido."

No	Activo asociado al contrato	Riesgo de Seguridad de la Información	CIA afectado (Confidencialidad, Integridad, Disponibilidad)	Probabilidad	Impacto	Nivel (Probabilidad X Impacto)	Controles existentes	Controles requeridos	Responsable
1	Información institucional intercambiada con el contratista	**Divulgación, acceso o uso no autorizado de información institucional durante la ejecución del contrato**	**C (Confidencialidad)**	**4. Probable**	**4. Mayor**	**16**	Cláusulas de confidencialidad contractual, políticas institucionales de seguridad de la información, acuerdos de confidencialidad (NDA)	Definición de roles y responsabilidades sobre el manejo de información, control de accesos, capacitación en seguridad de la información, seguimiento contractual	Supervisor del contrato / Contratista
2	Información y datos institucionales gestionados o procesados por el contratista	**Alteración, modificación no autorizada o pérdida de integridad de la información institucional durante la prestación del servicio**	**I (Integridad)**	**3. Posible**	**3. Moderado**	**9**	Procedimientos operativos, validaciones funcionales, controles de cambios, registros de actividades	Trazabilidad de cambios, segregación de funciones, controles de versionamiento, auditoría y revisión periódica de la información	Supervisor del contrato / Contratista
3	Servicios e información institucional soportados por el contrato	**Indisponibilidad de la información o de los servicios asociados al contrato que afecte la continuidad operativa de la entidad**	**D (Disponibilidad)**	**4. Probable**	**4. Mayor**	**16**	Acuerdos de nivel de servicio (ANS), seguimiento contractual, soporte técnico definido	Planes de contingencia y continuidad, respaldos de información, tiempos de respuesta definidos, pruebas periódicas	Supervisor del contrato / Contratista
4	Consola centralizada de administración y monitoreo de la solución EDR/XDR	**Acceso no autorizado o uso indebido de credenciales con privilegios administrativos sobre la plataforma durante la ejecución del contrato.**	**C (Confidencialidad) – I (Integridad)**	**3. Posible**	**4. Mayor**	**12**	Políticas institucionales de seguridad de la información, gestión de usuarios y control de acceso.	Autenticación multifactor (MFA), gestión de privilegios basada en roles, revisión periódica de accesos, registros de auditoría y control de cuentas privilegiadas.	Supervisor del contrato / Contratista
5	Plataforma SaaS de administración, monitoreo y gestión de eventos de seguridad	**Indisponibilidad de la consola SaaS que impida la administración, monitoreo o consulta de eventos de seguridad durante la ejecución del contrato.**	**D (Disponibilidad)**	**3. Posible**	**4. Mayor**	**12**	Acuerdos de nivel de servicio (SLA), soporte técnico especializado y monitoreo de disponibilidad.	Procedimientos de continuidad del servicio, monitoreo permanente, escalamiento oportuno de incidentes, mecanismos de contingencia y seguimiento al cumplimiento de SLA.	Supervisor del contrato / Contratista

Responsables:

NELSON JOSÉ OROZCO SALGADO
JEFE OFICINA DE OFICINA DE GOBERNANZA DIGITAL Y ANALITICA DE DATOS - OGDAD

Revisó: Jeison Jair González Vargas – Profesional Especializado DGEN.