Imprenta Nacional de Colombia

MATRIZ DE RIESGOS

No.	Clase de Riesgo	Fuente del Riesgo	Tipo de Riesgo	Descripción del Riesgo *(Posibilidad de + Afectación Economica y/o Reputacional + Consecuencia + debido a + Causa raiz)*	Probabilidad	Impacto	Valoración	Categoría	¿A quién se le Asigna?	Control a Implementar *(Responsable + Acción + Periodicidad + Complemento)*	Tipo de Control	Impacto Después de Controles			
												Probabilidad	Impacto	Valoración	Categoría
1	Especifico	Externa	Operacional	Posibilidad de indisponibilidad parcial o total de la plataforma Sophos Central Email Advanced (SaaS), afectando la protección de los trescientos cincuenta (350) buzones de correo corporativo de Microsoft 365 de la Imprenta Nacional de Colombia, lo que podría comprometer la recepción, envío y análisis seguro de mensajes, exponiendo a la Entidad a amenazas informáticas y afectando la continuidad de las comunicaciones institucionales.	3 Posible (puede ocurrir en cualquier momento futuro.	5 Cualitativo: Perturba la ejecución del contrato de manera grave, imposibilitando la consecución del objeto contractual.	8	Riesgo Extremo	Contratista	Control a Implementar: Garantizar la disponibilidad permanente del servicio Sophos Central Email Advanced, verificando el estado de la suscripción, la integración con Microsoft 365, el funcionamiento de la plataforma SaaS, la actualización continua de los motores de protección y la atención oportuna de incidentes conforme a los Acuerdos de Nivel de Servicio (ANS).	Preventivo	2,25	0,00	6,91	Riesgo Alto
										Acción: Realizar monitoreo permanente de la plataforma, verificar la correcta protección de los buzones corporativos, validar el funcionamiento de la integración con Microsoft 365, efectuar seguimiento a incidentes reportados y controlar el cumplimiento de los tiempos establecidos en los ANS. Peridiocidad: Mensual y cada vez que se presente una indisponibilidad o incidente crítico sobre la plataforma. Complemento/Evidencia: - Reportes de disponibilidad del servicio. - Informes técnicos del contratista. - Tickets de soporte. - Reportes de monitoreo. - Evidencias de funcionamiento de Sophos Central. - Bitácoras de incidentes. - Actas de seguimiento. - Informes del supervisor.	Detectivo	1,91	0,00		
2	Especifico	Externa	Operacional	Posibilidad de incumplimiento de los tiempos de respuesta, diagnóstico, escalamiento y solución de incidentes establecidos en los Acuerdos de Nivel de Servicio (ANS), afectando la continuidad de la operación del servicio de seguridad del correo electrónico y la atención oportuna de eventos de ciberseguridad relacionados con Microsoft 365.	3 Posible (puede ocurrir en cualquier momento futuro.	4 Cualitativo: Obstruye la ejecución del contrato sustancialmente, pero aun asi, permite la consecución del objeto contractual.	7	Riesgo Alto	Contratista	Control a Implementar: Verificar permanentemente el cumplimiento de los Acuerdos de Nivel de Servicio (ANS), mediante el seguimiento a los tiempos de respuesta, atención, resolución y cierre de incidentes, validando igualmente el cumplimiento de los indicadores establecidos contractualmente.	Preventivo	2,25	0,00	5,91	Riesgo Medio
										Acción: Revisar mensualmente los informes de soporte, validar el cumplimiento de los tiempos de atención establecidos para incidentes de acuerdo con su nivel de criticidad, realizar seguimiento a los indicadores de desempeño y exigir la implementación de acciones correctivas cuando se evidencien incumplimientos. Periodicidad:Mensual. Complemento/Evidencia. - Reportes mensuales de ANS. - Indicadores de cumplimiento. - Tickets de soporte. - Informes técnicos. - Actas de seguimiento. - Informes del supervisor. - Planes de mejoramiento. - Reportes de escalamiento.	Detectivo	1,91	0,00		
3	Especifico	Externa	Tecnologico	Posibilidad de afectación a la disponibilidad, integridad y confidencialidad del servicio de correo electrónico institucional debido a configuraciones incorrectas, administración inadecuada o falta de ajuste de las políticas de seguridad de Sophos Central Email Advanced, incluyendo reglas de filtrado, protección contra phishing, malware, ransomware, Business Email Compromise (BEC), autenticación mediante SPF, DKIM y DMARC, listas de permitidos y bloqueados, políticas DLP, protección Time-of-Click y demás mecanismos de seguridad, permitiendo el ingreso de amenazas o el bloqueo indebido de comunicaciones legítimas.	3 Posible (puede ocurrir en cualquier momento futuro.	5 Cualitativo: Perturba la ejecución del contrato de manera grave, imposibilitando la consecución del objeto contractual.	8	Riesgo Extremo	Contratista	Control a Implementar: Garantizar que la administración de las políticas de seguridad del correo electrónico sea realizada por personal especializado, aplicando buenas prácticas de ciberseguridad, monitoreo continuo de amenazas, endurecimiento (Hardening) de la configuración, revisión periódica de reglas de seguridad, análisis de falsos positivos y falsos negativos, así como ajustes permanentes de acuerdo con el comportamiento del correo institucional y las amenazas emergentes.	Preventivo	2,25	0,00	6,75	Riesgo Alto
										Acción: Realizar revisiones periódicas de las políticas de filtrado, validar la correcta configuración de SPF, DKIM, DMARC, DLP y demás mecanismos de protección, analizar eventos de seguridad detectados, ajustar oportunamente las configuraciones frente a nuevas amenazas y documentar todas las modificaciones realizadas sobre la plataforma. Periodicidad: Mensual y cada vez que se detecten nuevas amenazas, incidentes de seguridad o sea necesario modificar las políticas de protección. Complemento/Evidencia - Informes de Hardening. - Reportes de configuración. - Bitácoras de cambios. - Reportes de amenazas detectadas. - Registros de auditoría. - Informes técnicos. - Tickets de soporte. - Actas de seguimiento. - Evidencias de validación de políticas.	Correctivo	0,00	4,50		

4	Especifico	Externa	Tecnologico	Posibilidad de disminución en la capacidad de detección y prevención de amenazas debido a la no actualización oportuna de los motores antimalware, firmas de detección, modelos de inteligencia artificial, mecanismos antiphishing, protección contra Business Email Compromise (BEC), Time-of-Click Protection y demás capacidades de seguridad incorporadas por Sophos Central Email Advanced, exponiendo el correo institucional a nuevas amenazas cibernéticas.	3 Posible (puede ocurrir en cualquier momento futuro.	5 Cualitativo: Perturba la ejecución del contrato de manera grave, imposibilitando la consecución del objeto contractual.	**8**	Riesgo Extremo	Contratista	Control a implementar: Garantizar que la plataforma Sophos Central Email Advanced permanezca permanentemente actualizada con las últimas capacidades de protección suministradas por Sophos, verificando la correcta sincronización de motores de detección, firmas, inteligencia artificial y mecanismos de protección frente a amenazas emergentes.	Preventivo	2,25	0,00	6,75	Riesgo Alto
									Acción: Realizar seguimiento periódico al estado de actualización de la plataforma, validar la correcta incorporación de nuevas funcionalidades liberadas por Sophos, verificar el funcionamiento de los motores de protección y documentar cualquier incidente relacionado con retrasos o fallas en las actualizaciones. Periodicidad: Mensual y cada vez que Sophos publique nuevas capacidades de protección o actualizaciones relevantes. Complemento / Evidencia: - Reportes de actualización. - Informes técnicos. - Registros de Sophos Central. - Bitácoras de administración. - Evidencias de sincronización. - Informes del contratista. - Actas de seguimiento. - Informes del supervisor.	Correctivo	0,00	4,50		
5	Especifico	Externa	Tecnologico	Posibilidad de incremento en la materialización de incidentes de ciberseguridad sobre el correo electrónico institucional debido a una administración inadecuada de Sophos Central Email Advanced, deficiencias en el monitoreo continuo, ausencia de ajustes sobre las políticas de seguridad o respuesta tardía frente a amenazas emergentes, permitiendo el ingreso de campañas de phishing, malware, ransomware, Business Email Compromise (BEC), spoofing, ataques Zero-Day u otras amenazas dirigidas contra los usuarios de Microsoft 365.	3 Posible (puede ocurrir en cualquier momento futuro.	5 Cualitativo: Perturba la ejecución del contrato de manera grave, imposibilitando la consecución del objeto contractual.	**8**	Riesgo Extremo	Entidad	Control a implementar: Implementar un proceso permanente de monitoreo de eventos de seguridad, análisis de amenazas, ajuste continuo de políticas, endurecimiento (Hardening), gestión de falsos positivos y falsos negativos, revisión de indicadores de riesgo y aplicación de medidas preventivas conforme a las mejores prácticas de ciberseguridad y a las recomendaciones emitidas por Sophos.	Preventivo	2,25	0,00	6,91	Riesgo Alto
									Acción: Realizar monitoreo continuo de las amenazas detectadas, revisar periódicamente los reportes de seguridad, analizar campañas de phishing y demás eventos relevantes, efectuar ajustes oportunos sobre las políticas de protección y documentar las acciones implementadas para reducir la exposición al riesgo. Periodicidad: Mensual y cada vez que se detecten amenazas críticas o campañas dirigidas contra la Entidad. Complemento / Evidencia: - Reportes de amenazas. - Dashboard de Sophos Central. - Informes de Hardening. - Registros de incidentes. - Bitácoras de administración. - Informes técnicos. - Actas de seguimiento. - Evidencias de ajustes realizados.	Detectivo	1,91	0,00		
6	Especifico	Externa	Operacional	Posibilidad de incremento en los tiempos de atención, errores durante la administración de Sophos Central Email Advanced, configuraciones inadecuadas, respuesta deficiente frente a incidentes de seguridad o afectación en la protección del correo institucional, debido a que el personal asignado por el contratista no cuente con la experiencia, conocimientos o certificaciones requeridas para administrar plataformas Sophos y soluciones avanzadas de seguridad para Microsoft 365.	2 Improbable (puede ocurrir ocasionalmente).	4 Cualitativo: Obstruye la ejecución del contrato sustancialmente, pero aun asi, permite la consecución del objeto contractual.	**6**	Riesgo Alto	Contratista	Control a Implementar: Verificar que el personal asignado por el contratista cuente con experiencia comprobable y certificaciones vigentes en tecnologías Sophos Central, seguridad del correo electrónico, Microsoft 365 y administración de plataformas de ciberseguridad, garantizando que cualquier reemplazo mantenga o supere las competencias inicialmente acreditadas.	Preventivo	1,50	0,00	5,28	Riesgo Medio
									Acción: Revisar las hojas de vida, certificaciones técnicas, experiencia específica y perfiles profesionales del personal asignado, verificando además que cualquier cambio de recurso humano durante la ejecución contractual sea informado y aprobado por la supervisión del contrato. Periodicidad: Al inicio de la ejecución contractual y cada vez que se presente reemplazo o incorporación de personal técnico. Complemento/Evidencia: - Hojas de vida. - Certificaciones Sophos. - Certificaciones Microsoft. - Certificaciones laborales. - Actas de aprobación del personal. - Registro de cambios de personal. - Informes de supervisión. - Evidencias de capacitación.	Detectivo	1,28	0,00		
7	Especifico	Externa	Tecnologico	Posibilidad de afectación en la disponibilidad, funcionalidad o nivel de protección del servicio de correo electrónico institucional debido a errores durante la ejecución de actividades de hardening, modificación de políticas de seguridad, ajuste de reglas de filtrado, administración delegada o cambios realizados sobre Sophos Central Email Advanced, permitiendo el ingreso de amenazas o afectando la entrega normal de mensajes legítimos.	2 Improbable (puede ocurrir ocasionalmente).	5 Economico: Impacto sobre el valor del contrato en mas del 30%.	**7**	Riesgo Alto	Entidad	Control a Implementar: Garantizar que toda modificación sobre la plataforma Sophos Central Email Advanced sea ejecutada por personal especializado, siguiendo procedimientos documentados de administración de cambios, análisis de impacto, validación previa, ejecución controlada, plan de reversa y pruebas posteriores antes de implementar modificaciones en producción..	Detectivo	1,70	0,00	6,45	Riesgo Alto
									Acción: Verificar que toda modificación de políticas de seguridad cuente con solicitud formal, análisis técnico, aprobación cuando corresponda, documentación de los cambios realizados y validación posterior del correcto funcionamiento de la plataforma. Periodicidad: Cada vez que se realicen cambios de configuración, hardening o administración de políticas sobre la plataforma. Complemento/Evidencia: - Solicitudes de cambio. - Actas de aprobación. - Bitácoras de administración. - Informes técnicos. - Evidencias de pruebas. - Registro de cambios. - Actas de cierre. - Informes del supervisor.	Detectivo	1,45	0,00		

8	Especifico	Externa	Tecnologico	Posibilidad de afectación en la protección del correo electrónico institucional debido a fallas en la integración mediante API entre Sophos Central Email Advanced y Microsoft 365, ocasionando interrupciones en el análisis de mensajes, pérdida de visibilidad sobre eventos de seguridad, errores en la aplicación de políticas o disminución de la capacidad de detección y respuesta frente a amenazas.	3 Posible (puede ocurrir en cualquier momento futuro.	5 Cualitativo: Perturba la ejecución del contrato de manera grave, imposibilitando la consecución del objeto contractual.	**8**	Riesgo Extremo	Contratista	Control a Implementar: Verificar permanentemente el correcto funcionamiento de la integración entre Sophos Central y Microsoft 365, realizando monitoreo continuo del estado de la conexión mediante API, validando la sincronización de los buzones protegidos y corrigiendo oportunamente cualquier falla detectada.	Preventivo	2,25	0,00	6,91	Riesgo Alto
									Acción: Realizar verificaciones periódicas del estado de la integración, revisar alertas generadas por Sophos Central, validar la protección efectiva de los buzones institucionales y documentar las acciones implementadas para corregir incidentes relacionados con la conectividad o sincronización. Periodicidad: Mensual y cada vez que se presenten incidentes relacionados con la integración entre ambas plataformas. Complemento/Evidencia: - Reportes de integración. - Dashboard de Sophos Central. - Registros de sincronización. - Informes técnicos. - Tickets de soporte. - Reportes de monitoreo. - Actas de seguimiento. - Informes del supervisor.	Detectivo	1,91	0,00		
9	Especifico	Externa	Tecnologico	Posibilidad de pérdida, alteración, eliminación o modificación no autorizada de las configuraciones de seguridad, políticas de protección, listas de remitentes permitidos o bloqueados, excepciones, registros de auditoría, configuraciones de autenticación y demás parámetros administrativos de Sophos Central Email Advanced, afectando la capacidad de protección del correo institucional y dificultando las labores de auditoría e investigación de incidentes.	2 Improbable (puede ocurrir ocasionalmente).	5 Cualitativo: Perturba la ejecución del contrato de manera grave, imposibilitando la consecución del objeto contractual.	**7**	Riesgo Alto	Entidad	Control a Implementar: Implementar controles para proteger las configuraciones administrativas de la plataforma, incluyendo gestión segura de privilegios, respaldo periódico de configuraciones críticas, control de cambios, revisión de auditorías y monitoreo permanente de actividades administrativas realizadas sobre Sophos Central.	Preventivo	1,50	0,00	6,13	Riesgo Alto
									Acción: Verificar periódicamente la integridad de las políticas configuradas, revisar los registros de auditoría, validar las copias de respaldo de configuraciones críticas, controlar los privilegios administrativos y documentar cualquier modificación realizada sobre la plataforma. Periodicidad: Trimestral y cada vez que se realicen modificaciones administrativas relevantes. Complemento/Evidencia: - Reportes de auditoría. - Registros administrativos. - Evidencias de respaldo. - Informes técnicos. - Bitácoras de cambios. - Actas de revisión. - Informes del supervisor. - Evidencias de validación.	Preventivo	1,13	0,00		
10	Especifico	Externa	Operacional	Posibilidad de indisponibilidad parcial o total del servicio SaaS de Sophos Central Email Advanced o de la conectividad necesaria para su integración con Microsoft 365, ocasionando la suspensión temporal de las funciones de análisis, detección y protección del correo electrónico institucional frente a amenazas avanzadas, afectando la continuidad del servicio de seguridad del correo electrónico.	3 Posible (puede ocurrir en cualquier momento futuro.	5 Cualitativo: Perturba la ejecución del contrato de manera grave, imposibilitando la consecución del objeto contractual.	**8**	Riesgo Extremo	Entidad	Control a Implementar: Posibilidad de indisponibilidad parcial o total del servicio SaaS de Sophos Central Email Advanced o de la conectividad necesaria para su integración con Microsoft 365, ocasionando la suspensión temporal de las funciones de análisis, detección y protección del correo electrónico institucional frente a amenazas avanzadas, afectando la continuidad del servicio de seguridad del correo electrónico.	Preventivo	2,25	0,00	6,91	Riesgo Alto
									Acción: Verificar periódicamente la disponibilidad del servicio SaaS, revisar los paneles de estado de Sophos Central, validar el funcionamiento de la integración con Microsoft 365, realizar seguimiento a incidentes de disponibilidad y documentar las acciones implementadas hasta el restablecimiento completo del servicio. Periodicidad: Mensual y cada vez que se presente una indisponibilidad del servicio o incidente de conectividad. Complemento/Evidencia: - Reportes de disponibilidad. - Paneles de estado del servicio. - Informes técnicos. - Tickets de soporte. - Reportes de monitoreo. - Actas de seguimiento. - Informes del supervisor. - Evidencias de restablecimiento del servicio.	Detectivo	1,91	0,00		
11												0,00	0,00	0,00	
												0,00	0,00		
12												0,00	0,00	0,00	
												0,00	0,00		