Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

ANEXO – HISTORIAL DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN RELEVANTES

Respuesta a– Formulario Póliza Cyber 2026

Alcance y manejo de la información. El presente anexo contiene un resumen ejecutivo de los eventos de seguridad relevantes conocidos y gestionados a nivel institucional durante el periodo consultado. Por razones de seguridad de la información, no se incorporan configuraciones, credenciales, direcciones IP, indicadores de compromiso, vulnerabilidades específicas ni procedimientos técnicos cuya divulgación pueda incrementar la exposición de los sistemas.

1. Objeto

Documentar, para efectos de la pregunta HIS-1 del formulario de suscripción de la póliza Cyber, los principales incidentes de seguridad de la información y ciberseguridad ocurridos durante los últimos tres (3) años y conocidos en el nivel central, indicando de forma ejecutiva su naturaleza, afectación, causa conocida o estado de investigación, impactos económicos cuando se encuentran cuantificados, notificaciones efectuadas, tiempos de detección y recuperación cuando existe información consolidada, y las principales medidas adoptadas para reducir la exposición futura.

2. Consideraciones sobre el alcance

- La Rama Judicial opera bajo un esquema amplio y descentralizado, con múltiples corporaciones, dependencias y Direcciones Seccionales; por ello, la información aquí consolidada corresponde a los eventos relevantes conocidos y gestionados en el nivel central.
- Cuando un dato no se encuentra consolidado, cuantificado o técnicamente confirmado, se indica expresamente como “no consolidado”, “por determinar” o “en investigación”, evitando estimaciones no soportadas.
- Este documento no sustituye los informes técnicos, forenses, contractuales o regulatorios existentes para cada caso, los cuales conservan su propio nivel de reserva y custodia.

3. Resumen ejecutivo de eventos relevantes

Periodo	Evento	Afectación general	Impacto económico	Estado / medidas principales
2023	Incidente de ransomware asociado a proveedor de nube privada (IFX Networks)	Indisponibilidad de múltiples servicios judiciales y afectación operativa sobre información y servicios alojados en la infraestructura contratada.	No se reportó pérdida financiera material directa en la declaración de 2025; sí se reconocieron costos operativos de recuperación y riesgos legales.	Gestión de recuperación, continuidad, coordinación con proveedor, fortalecimiento de controles y seguimiento institucional/regulatorio.

2025	Incidente de exfiltración de información	Afectación a la confidencialidad de determinada información y generación de riesgo legal potencial. Solicitaban el pagoda una suma de por no publicar la demás información	En la declaración de 2025 no se reportó pérdida económica material directa asociada.	Análisis, contención, evaluación de alcance, gestión de evidencias y fortalecimiento de capacidades de monitoreo y respuesta.
2026	Acceso y utilización no autorizada de recursos de nube asociados a un servicio institucional	Uso no autorizado de recursos tecnológicos y consumo de servicios de nube; investigación técnica y contractual en curso.	Consumo no autorizado de créditos en nube.	Bloqueo de la cuenta asociada, restablecimiento de credenciales, revocación de sesiones/tokens, rotación de claves, análisis forense, revisión de MFA y monitoreo reforzado.

4. Detalle ejecutivo por evento

4.1. Incidente de ransomware asociado a IFX Networks – 2023

Fecha / periodo	12 de septiembre de 2023.
Descripción del evento	El proveedor IFX Networks, encargado de servicios de nube privada donde se alojaba parte de la infraestructura tecnológica de la Rama Judicial, fue afectado por un incidente de ransomware que generó indisponibilidad de múltiples servicios judiciales.
Causa	Ataque de ransomware dirigido al proveedor tecnológico. El detalle técnico de la causa raíz y del vector de compromiso corresponde al análisis del proveedor y a las actuaciones adelantadas en el marco del incidente.
Afectación	Principalmente disponibilidad de servicios institucionales, con impactos operativos sobre plataformas judiciales y riesgos asociados a la integridad y protección de la información alojada en el servicio contratado.
Costos internos / a terceros	Por determinar.
Notificaciones / actuaciones	El evento dio lugar a actuaciones institucionales y regulatorias. Se tiene conocimiento de recomendaciones formales de la Superintendencia de Industria y Comercio orientadas al fortalecimiento de las medidas de protección de datos personales.
Tiempo de detección	No se dispone de un indicador consolidado institucional de tiempo medio de detección para este evento. La afectación fue conocida a partir de la indisponibilidad y comunicaciones asociadas al incidente del proveedor.
Tiempo de recuperación	La recuperación fue progresiva y dependió de los servicios afectados. No se presenta un único tiempo consolidado de recuperación aplicable a todas las plataformas.
Medidas de mitigación	Coordinación con el proveedor; actividades de recuperación y continuidad; fortalecimiento de capacidades de monitoreo y respuesta; revisión de medidas de

	seguridad aplicables a servicios de terceros; y seguimiento a recomendaciones de protección de datos y seguridad.

4.2. Incidente de exfiltración de información – 2025

Fecha / periodo	2025.
Descripción del evento	Se registró un incidente de seguridad asociado a exfiltración de información, declarado en la autoevaluación de ciberseguridad de diciembre de 2025.
Causa	Se comprometieron credenciales de una VPN. Los detalles técnicos se encuentran en los registros e informes específicos del incidente.
Afectación	Afectación a la confidencialidad de determinada información, con impactos operativos y riesgo legal potencial.
Costos internos / a terceros	No se reportó en la declaración de 2025 una pérdida económica material directa asociada al evento.
Notificaciones / actuaciones	Se adelantaron las actuaciones y comunicaciones que resultaron aplicables de acuerdo con el alcance del incidente y denuncia. La información detallada sobre destinatarios y comunicaciones se conserva en los soportes del caso.
Tiempo de detección	Un día
Tiempo de recuperación	No se dispone de un tiempo único consolidado. La gestión comprendió análisis, contención, evaluación de alcance y acciones de recuperación y seguimiento.
Medidas de mitigación	Fortalecimiento del monitoreo, análisis de evidencias, contención, revisión de accesos y controles de seguridad, y seguimiento técnico de los activos y servicios involucrados.

4.3. Acceso y utilización no autorizada de recursos de nube – 2026

Fecha / periodo	2026. Se identificó una ventana de actividad no autorizada
Descripción del evento	Se identificó acceso y utilización no autorizada de recursos de nube mediante una cuenta técnica asociada a un proveedor
Causa	La investigación identificó el uso de una cuenta asociada al proveedor - investigación en curso.
Afectación	Uso no autorizado de recursos de nube,.
Costos internos / a terceros	Se identificó un consumo no autorizado en revision
Notificaciones / actuaciones	El caso fue escalado y trabajado con los equipos internos.
Tiempo de detección	En invetigación
Tiempo de recuperación / contención	Las medidas de contención sobre la cuenta y credenciales fueron ejecutadas una vez identificado el riesgo
Medidas de mitigación	Bloqueo de la cuenta involucrada; restablecimiento de contraseña; revocación de sesiones y tokens; rotación de claves del aplicativo; revisión de accesos, delegaciones y actividad asociada; análisis forense en curso.

5. Medidas institucionales de fortalecimiento

Como resultado de la gestión de incidentes y del proceso de fortalecimiento continuo de ciberseguridad, la Rama Judicial ha venido reforzando, entre otras, las siguientes capacidades:

- Monitoreo y correlación de eventos de seguridad mediante plataformas SIEM, EDR/XDR y servicios especializados de monitoreo y respuesta.
- Fortalecimiento de autenticación multifactor, controles de identidad y revisión de cuentas privilegiadas y de terceros.
- Gestión de vulnerabilidades, análisis de exposición externa y aplicación de controles compensatorios cuando la remediación inmediata no es técnicamente viable.
- Revisión de accesos de proveedores y fortalecimiento de requisitos de seguridad, confidencialidad y trazabilidad en servicios tecnológicos contratados.
- Mejora de procedimientos de gestión de incidentes, preservación de evidencias, análisis forense y coordinación con fabricantes y proveedores especializados.
- Actividades de sensibilización y capacitación en seguridad de la información, phishing, protección de credenciales e identidad digital.

6. Declaración sobre información no incluida

La información presentada corresponde a un resumen ejecutivo preparado para fines de suscripción de seguro. Los soportes técnicos y administrativos de cada incidente se conservan en los expedientes, registros, informes y sistemas institucionales correspondientes. Cualquier solicitud adicional de información técnica deberá evaluarse bajo criterios de necesidad de conocimiento, confidencialidad, protección de datos personales y seguridad de la información.