Estrategias de Gobernanza, Gestión de Riesgos y Cumplimiento a través de la Ciberseguridad en el Poder Judicial de la Provincia de Buenos Aires – Argentina

Tomás Cappelli [1[0009-0005-3878-7181]], Alejandra B. Lliteras [1,2[0000-0002-4148-1299]], Patricia Bazán [3[0000-0001-6720-345X]]
[1] UNLP Facultad de Informática, Centro LIFIA, Buenos Aires Argentina
[2]CICPBA, Buenos Aires Argentina
[3] UNLP Facultad de Informática, LINTI, Buenos Aires Argentina
{tcapelli, lliteras}@lifia.info.unlp.edu.ar
pbaz@info.unlp.edu.ar

Resumen. Este trabajo aborda las problemáticas vinculadas a la gobernanza de activos tecnológicos, la gestión de riesgos y el cumplimiento de normas y políticas en el ámbito de la Suprema Corte de Justicia de Buenos Aires (SCBA). Desde la experiencia del Área de Seguridad y Auditoría (SyA), se proponen acciones orientadas a la identificación y control de los activos a la adecuación operativa a los marcos normativos vigentes, tanto institucionales como nacionales e internacionales. Se destaca, como premisa central, la importancia de contar con un conocimiento preciso y actualizado de la infraestructura tecnológica, condición indispensable para ejercer una gobernanza efectiva, evaluar riesgos reales y aplicar de forma coherente las políticas de seguridad de la información. Asimismo, se detallan las acciones implementadas desde un enfoque integral de GRC (Gobernanza, Riesgo y Cumplimiento), orientadas a garantizar un nivel óptimo de ciberseguridad, fortaleciendo la trazabilidad, la capacidad de respuesta y el cumplimiento normativo en la infraestructura de la SCBA.

Palabras Clave: GRC (Gobierno, Riesgo y Cumplimiento), Ciberseguridad, Activos Tecnológicos, Gobernanza, Gestión de Riesgos, Seguridad y Auditoría.

1. Introducción

La Suprema Corte de Justicia de Buenos Aires (SCBA)[1] constituye el máximo órgano del Poder Judicial en dicha provincia, se encuentra organizado en veinte departamentos judiciales. Cada uno cuenta con una cabecera departamental y diversos juzgados de paz. Algunas localidades carecen de una cabecera departamental, pero cuentan con juzgados de paz; tal es el caso de San Carlos de Bolívar, perteneciente al departamento judicial de Azul.

SCBA dispone de la Subsecretaría de Tecnología Informática, cuya función principal consiste en "dirigir, coordinar y ejecutar los procesos asociados al desarrollo,

[1] www.scba.gov.ar

implementación y actualización de las tecnologías de información y comunicación en todo el ámbito de la Administración de Justicia"[2].

La infraestructura tecnológica de la SCBA está compuesta por un centro de datos propio, más de 19.000 puestos de trabajo, aproximadamente 1.000 servidores y más de 30 aplicaciones, algunas de las cuales son críticas.

En este marco, la ciberseguridad, como la práctica de proteger su información digital, dispositivos y activos[3], adquiere una relevancia esencial en el Poder Judicial de la Provincia de Buenos Aires, dada la creciente dependencia de los sistemas informáticos en la gestión de expedientes, las notificaciones electrónicas y el acceso remoto. La protección adecuada de estos sistemas garantiza no solo la continuidad operativa del servicio judicial, sino también la confidencialidad, integridad y disponibilidad de la información procesada. En este sentido, la aplicación de estrategias eficaces en seguridad informática resulta imprescindible para mitigar riesgos, prevenir ciberataques y fortalecer la infraestructura tecnológica de la Suprema Corte de Justicia.

2. Marco Conceptual y Contexto

En los últimos años, la creciente complejidad del entorno digital, sumada al incremento sostenido de amenazas cibernéticas, ha llevado a las organizaciones públicas a adoptar enfoques integrados de gestión que permitan alinear la seguridad informática con los objetivos institucionales, el control de riesgos y el cumplimiento normativo. En este contexto, el modelo GRC (*Governance, Risk Management and Compliance*) se presenta como un marco conceptual que articula de forma sistemática tres dimensiones esenciales para una gestión efectiva de la seguridad: la gobernanza de los activos, la evaluación y mitigación de riesgos, y la adecuación a marcos regulatorios internos y externos.

Tal como lo establece el método MAGERIT v3 [1], el conocimiento de los riesgos constituye el punto de partida para desarrollar un modelo equilibrado de GRC, que permita garantizar que los sistemas tecnológicos se comporten de acuerdo con las expectativas. “El conocimiento de los riesgos permite calibrar la confianza en que los sistemas desempeñarán su función como la Dirección espera, habilitando un marco equilibrado de Gobierno, Gestión de Riesgos y Cumplimiento (GRC), tres áreas que deben estar integradas y alineadas para evitar conflictos, duplicación de actividades y zonas de nadie” [4].

En esta misma línea, la norma ISO/IEC 27001:2022[3] establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), y se encuentra estrechamente alineada con los principios del modelo GRC. Al incorporar procesos de identificación de riesgos, definición de responsabilidades, asignación de recursos desde la alta dirección y cumplimiento de requisitos legales y contractuales, esta norma refuerza la necesidad de estructurar la seguridad informática desde una perspectiva estratégica, normativa y operativa.

[2] https://www.scba.gov.ar/paginas.asp?id=39716

[3] https://url-shortener.me/YZR

En el ámbito del Poder Judicial de la Provincia de Buenos Aires, y más específicamente en la Suprema Corte de Justicia, la construcción de capacidades orientadas al GRC ha tenido como punto de partida la implementación de herramientas concretas de protección tecnológica. A partir del despliegue progresivo de soluciones como antivirus tradicionales y sistemas EDR (*Endpoint Detection and Response*) fue posible avanzar hacia una instancia superior de visibilidad, control y trazabilidad sobre los activos críticos de la infraestructura judicial.

En este proceso, se destaca una iniciativa clave que consolida la adopción práctica del modelo GRC. Se encuentra en curso el despliegue de una solución específica orientada a la gestión centralizada de gobierno, riesgos y cumplimiento, instalada inicialmente en servidores virtualizadores y delegaciones departamentales estratégicas. Esta herramienta permite recolectar información crítica de los activos (como ubicación, responsables asignados, servicios alojados, estado de protección y configuración) y construir representaciones dinámicas del mapa de servicios, posibilitando la automatización de alertas y tareas correctivas ante eventos detectados. Así, el componente tecnológico actúa como facilitador de la gobernanza y del monitoreo continuo, pilares fundamentales del modelo GRC.

El presente trabajo expone esta experiencia institucional, detallando cómo la incorporación de dichas herramientas no sólo permitió fortalecer la postura de ciberseguridad, sino también habilitar mecanismos operativos para ejercer gobernanza sobre los activos, gestionar riesgos emergentes de manera más eficiente y asegurar el cumplimiento de las normativas vigentes.

3. Situación Actual

Al inicio de la pandemia, la infraestructura tecnológica de la SCBA fue afectada por un incidente de seguridad, que implicó la introducción de software malicioso. Este evento, diseñado específicamente para aprovechar recursos computacionales, representó una seria amenaza para la estabilidad y seguridad de la información y tecnologías de la institución.

Tras la detección del incidente, se coordinó la acción conjunta de todas las áreas de tecnología para contener y mitigar la amenaza. Entre las medidas implementadas se destacan: 1) la identificación y aislamiento inmediato de los equipos comprometidos para prevenir la propagación del software malicioso, 2) la desactivación de procesos sospechosos en los sistemas afectados, y 3) la actualización y fortalecimiento de las medidas de seguridad existentes mediante la aplicación de parches de software y revisiones exhaustivas de configuración.

Una vez controlada la situación, se realizó un análisis exhaustivo con el objetivo de determinar el alcance del compromiso en la infraestructura, los activos afectados, la potencial persistencia del software malicioso en los sistemas y las vulnerabilidades explotadas para su ingreso.

Como resultado de dicha evaluación, se adoptó una medida de seguridad compleja pero altamente efectiva: la migración integral de la infraestructura hacia nuevas máquinas virtuales. Este incidente puso de manifiesto la importancia crítica de contar con protocolos robustos de detección y respuesta ante incidentes.

En este sentido, se implementaron nuevas estrategias preventivas de seguridad, tales como: 1) el incremento del monitoreo y análisis de la actividad en los activos informáticos, 2) el fortalecimiento de políticas de seguridad para minimizar la probabilidad de futuros compromisos, 3) el despliegue de herramientas avanzadas para la detección proactiva de amenazas, incluyendo soluciones de *Endpoint Detection and Response* (EDR), software antivirus basado en firmas, software especializado en seguridad y análisis de vulnerabilidades, y 4) el desarrollo y puesta en marcha de un Plan Integral de Seguridad de la Información.

4. Acciones sobre la Infraestructura

La gestión de la seguridad de la información en entornos complejos como el Poder Judicial requiere intervenciones concretas sobre la infraestructura tecnológica que garanticen la disponibilidad, integridad y confidencialidad de los servicios críticos. En el marco de un enfoque hacia la consolidación de capacidades institucionales en materia de gobernanza, gestión de riesgos y cumplimiento (GRC), la SCBA avanzó en el despliegue y adecuación de soluciones de protección para servidores y puestos de trabajo, así como en la implementación de herramientas para la administración centralizada y el monitoreo continuo de sus activos.

Esta sección describe las principales acciones realizadas sobre la infraestructura tecnológica, centradas en dos ejes técnicos: por un lado, el despliegue diferenciado de software de protección para servidores y estaciones de trabajo, y por otro, la incorporación de una herramienta especializada para la gestión integral de GRC. A su vez, se presenta una herramienta complementaria clave —el boletín técnico de seguridad— como mecanismo operativo de coordinación descentralizada, que facilita la toma de decisiones en territorio y mejora la trazabilidad de las acciones de respuesta frente a incidentes.

Las acciones aquí descritas complementan y profundizan las acciones presentadas en el trabajo previo Acciones y protocolos en ciberseguridad para el Poder Judicial de la Provincia de Buenos Aires – Argentina, el cual constituyó una primera aproximación sistemática a la formalización de prácticas y herramientas de ciberseguridad [2].

4.1. Despliegue de software de protección para servidores.

Tras un incidente de seguridad, se decidió implementar FortiEDR[4], una herramienta de detección y respuesta en *endpoints* (EDR) de Fortinet, para fortalecer la protección de los activos tecnológicos críticos. La elección se basó en sus capacidades de monitoreo en tiempo real, detección proactiva, respuesta automatizada y uso de *machine learning.* En línea con este enfoque, [5] propone una estructura avanzada para la detección de amenazas cibernéticas que aprovecha el aprendizaje automático como intervención tecnológica concreta para mejorar la ciberseguridad. La metodología incluye un preprocesamiento exhaustivo de datos, selección de características relevantes y la construcción y evaluación de modelos.

[4] https://www.fortinet.com/lat/products/endpoint-security/fortiedr

La instalación se realizó manualmente en cada servidor, permitiendo un control preciso del proceso. Inicialmente, el sistema se configuró en modo simulación para aprender el comportamiento habitual sin afectar la operatividad. Luego, se diseñó una metodología de agrupamiento de activos según su función, lo que permitió asignar reglas de seguridad específicas.

El análisis de más de 1.000 eventos detectados permitió clasificarlos como maliciosos o generar reglas de excepción para permitir procesos legítimos de forma controlada. Esta estrategia facilitó una transición segura al modo de protección activa, mejorando la eficacia del sistema mediante una adaptación progresiva a la realidad operativa.

El desarrollo metodológico descripto anteriormente ha permitido establecer un modelo de gobernanza tecnológica en la SCBA.

Este marco de gobernanza ha generado múltiples beneficios, destacándose especialmente en tres ámbitos principales:

Gobierno efectivo de activos y reglas: procedimiento detallado y riguroso aplicado para agrupar activos y generar reglas específicas de operación, facilitó una administración centralizada, transparente y eficiente de los recursos tecnológicos disponibles. Este enfoque favoreció la mejora en la visibilidad y trazabilidad del uso de cada activo informático, permitiendo una rápida identificación y gestión de los eventos críticos.

Reducción proactiva de riesgos: utilización de la solución en modo simulación inicialmente, seguida por la creación y aplicación precisa de reglas específicas, contribuyó significativamente a minimizar la exposición de la institución frente a amenazas y vulnerabilidades tecnológicas. La capacidad para identificar y neutralizar proactivamente eventos maliciosos, así como la definición granular de excepciones para procesos legítimos, permitió una reducción de los riesgos.

Control y cumplimiento normativo: gestión del entorno tecnológico, facilitada por esta estrategia, posibilita una adecuada supervisión del cumplimiento normativo. Mediante la implementación controlada de reglas específicas, se logró asegurar que los equipos operen en conformidad con las políticas internas establecidas, así como con estándares nacionales e internacionales en materia de seguridad informática.

4.2. Despliegue de software de protección para puestos de trabajo

En el marco de la estrategia de seguridad de la SCBA, se implementó un enfoque diferenciado: FortiEDR para proteger servidores críticos y ESET[5] para los más de 19.000 puestos de trabajo. La elección de ESET se basó en su facilidad de instalación, despliegue masivo y gestión centralizada, esenciales por la amplia distribución geográfica del sistema judicial.

[5] https://www.eset.com/ar

Una funcionalidad clave fue la integración con Active Directory[6], lo que permitió organizar y gestionar los equipos según su estructura organizacional, facilitando la aplicación de políticas de seguridad específicas para cada unidad.

Se definieron grupos estáticos (por pertenencia organizacional) y grupos dinámicos (por condiciones técnicas, como versión obsoleta del sistema operativo). Además, se asignaron perfiles con permisos restringidos para prevenir acciones no autorizadas en otras jurisdicciones.

Para equipos técnicos y críticos, se habilitó un entorno de *sandboxing* local, que permite ejecutar archivos sospechosos en un entorno aislado. Esto mejora la detección de amenazas difíciles de clasificar, evaluando tanto sus características estáticas como su comportamiento dinámico, y permite decidir si bloquear o permitir su ejecución.

4.3. Despliegue de software para GRC

Durante el segundo semestre del año 2025, y en el marco de una estrategia de mejora continua en materia de gobernanza, gestión de riesgos y cumplimiento (GRC), la Suprema Corte de Justicia de la Provincia de Buenos Aires procedió a la adquisición de 1.000 licencias de la herramienta especializada Asset Management [7], desarrollada por la empresa InvGate, e inició su implementación progresiva. Esta solución tecnológica representa un componente clave para mejorar la visibilidad, el control y la trazabilidad de los activos tecnológicos distribuidos en todo el ecosistema institucional.

Dado que el despliegue del agente requería su instalación en servidores críticos (algunos de los cuales alojaban máquinas virtuales vinculadas a servicios esenciales), se optó por iniciar el proceso mediante una instalación manual controlada. Esta fase piloto permitió realizar pruebas exhaustivas sin comprometer la estabilidad de los servicios, validando la compatibilidad operativa del software con los diferentes entornos productivos. Una vez confirmada su estabilidad, se extendió el despliegue manual a todos los equipos virtualizadores del centro de datos principal y de algunas Delegaciones de Tecnología Informática seleccionadas.

La herramienta introdujo funcionalidades significativas para la gestión integral de activos. Entre las más relevantes se destaca la recolección periódica, cada 15 minutos, de información técnica detallada de cada dispositivo, incluyendo: dirección IP, hipervisor asociado (en el caso de máquinas virtuales), historial de usuarios autenticados, capacidad de memoria RAM y disco, sistema operativo instalado, servidor de actualizaciones, estado del firewall, estado del antivirus y, en el caso de servidores específicos, las bases de datos alojadas.

Además de esta visibilidad técnica, la herramienta permite enriquecer cada activo con información adicional relevante desde una perspectiva de gobernanza. Por ejemplo, es posible asignar a cada activo un responsable formal, una ubicación física o lógica, y etiquetas funcionales tales como “base de datos”, “web server”, “hipervisor” o “punto

[6] https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[7] https://invgate.com/es/asset-management

de distribución". Esta clasificación mejora significativamente las capacidades de filtrado, búsqueda y gestión diferenciada por parte del personal técnico.

Uno de los aportes estratégicos más importantes de esta herramienta es la posibilidad de construir un mapa de servicios en tiempo real que permite visualizar la interdependencia entre equipos y servicios, detectando en vivo si un nodo se encuentra fuera de línea y evaluando su impacto sobre los servicios que aloja. Este enfoque habilitó, además, la automatización de tareas ante eventos específicos. En la Fig. 1 se puede visualizar cómo se compone de forma parcial el servicio de Subastas Electrónicas. Por ejemplo, si un activo crítico de este servicio presenta una falla, se puede programar el envío automático de una notificación por correo electrónico al responsable asignado, facilitando la respuesta inmediata.

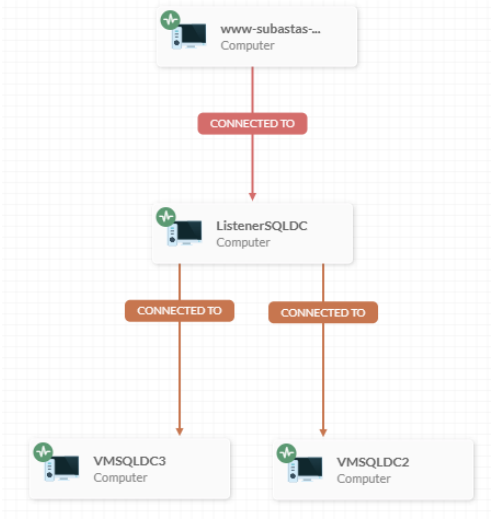

Fig. 1. Diagrama parcial del servicio de subastas electrónicas [*Elaboración Propia*].

El sistema permite auditar el estado de los activos en relación con el cumplimiento normativo y operativo. Esto incluye la detección de actualizaciones pendientes, reinicios necesarios, análisis del software instalado (con posibilidad de bloqueo o desinstalación remota).

Al día de la fecha se ha optimizado el proceso de despliegue del agente mediante la integración con las infraestructuras de gestión centralizada ya existentes. Específicamente, se ha configurado una directiva de grupo que permite la instalación automática del agente en todos los puestos de trabajo que se incorporan al dominio.

Esta medida garantiza que todo nuevo equipo que se integre al dominio cuente desde el inicio con la solución de GRC implementada, sin necesidad de intervención manual.

Adicionalmente, se ha integrado este proceso con el sistema de gestión de configuración *Microsoft System Center Configuration Manager* (SCCM)[8], a través del cual se diseñó y automatizó una tarea específica que permite ejecutar el instalador del

[8] https://learn.microsoft.com/es-es/intune/configmgr/core/understand/introduction

agente en los equipos objetivo previamente seleccionados. Esta funcionalidad resulta particularmente útil para realizar implementaciones dirigidas, ya sea por área, por tipo de dispositivo o por el criterio deseado.

4.4. Boletín semanal de seguridad

Ante el incremento sostenido en el volumen de información generada por los sistemas de protección y detección de amenazas desplegados en la Suprema Corte de Justicia de la Provincia de Buenos Aires, y considerando la disponibilidad limitada de recursos humanos especializados en seguridad informática en las Delegaciones de Tecnología Informática (DTI) distribuidas en el territorio provincial, se identificó la necesidad de implementar un mecanismo de comunicación eficiente y de ejecución de acciones concretas.

Este mecanismo se materializó en la creación de un boletín técnico de seguridad, cuyo propósito principal es canalizar información precisa, oportuna y accionable hacia los técnicos de las DTI, permitiéndoles enfocar sus esfuerzos exclusivamente en los eventos relevantes que afectan a sus jurisdicciones. La premisa fundamental del boletín es reducir la complejidad inherente a la gestión de incidentes de seguridad, evitando la sobrecarga de información y facilitando la toma de decisiones informadas a nivel local.

Para asegurar su eficacia operativa, se establecieron criterios claros sobre el tipo de información que sería incluida en cada emisión del boletín. El boletín contempla tres ejes temáticos prioritarios: 1- Amenazas detectadas en las consolas de seguridad: se reportan eventos relevantes capturados por los sistemas de protección (EDR y antivirus), incluyendo actividades sospechosas, procesos maliciosos, etc., 2- Estado de protección de los dispositivos: se identifican y notifican aquellos equipos que se encuentran en estado de vulnerabilidad, ya sea por estar desactualizados, fuera de línea, o sin conexión a las consolas de seguridad correspondientes. Esta información permite priorizar acciones correctivas de mantenimiento o remediación, y 3-Detección de software no autorizado y alertas críticas: se incluye la detección de programas instalados que violan las políticas institucionales, así como cualquier otro evento clasificado como crítico, como intentos de escalamiento de privilegios, accesos anómalos o cambios no autorizados en configuraciones sensibles.

En términos de Gobernanza, Riesgo y Cumplimiento (GRC), estos boletines adquieren un valor estratégico al permitir la integración entre la gestión operativa de la seguridad informática y el cumplimiento normativo. Su emisión periódica garantiza no solo una respuesta técnica efectiva, sino también una supervisión constante de los riesgos tecnológicos, promoviendo la toma de decisiones alineada a las políticas institucionales. Esto convierte al boletín en una herramienta clave para sostener un sistema de gestión de seguridad de la información coherente, transparente y orientado a resultados medibles.

5. Conclusiones y Trabajos Futuros

A partir del análisis y las acciones detalladas en este trabajo, queda en evidencia que uno de los principios fundamentales para una gestión efectiva de la ciberseguridad es

el conocimiento profundo y actualizado de la infraestructura tecnológica que se busca proteger. Resulta ineludible identificar con precisión qué activos existen, cuál es su estado actual y cómo se interrelacionan dentro del ecosistema institucional, a fin de definir con claridad qué acciones deben tomarse y qué políticas deben aplicarse para cada caso particular. En otras palabras, no se puede proteger lo que no se conoce.

Este conocimiento no solo constituye la base para una toma de decisiones informadas, sino también para garantizar un modelo de gobierno de activos tecnológicos, asociado al análisis de riesgos y al cumplimiento normativo, tanto a nivel institucional como en función de los estándares nacionales e internacionales aplicables.

Asimismo, es prioritario destacar la necesidad de adaptar y reutilizar las herramientas ya disponibles, maximizando su aprovechamiento mediante configuraciones adecuadas, integración entre sistemas y desarrollo de soluciones complementarias. La consolidación de un enfoque GRC no requiere necesariamente de licencias comerciales: puede lograrse también mediante el uso eficiente de software libre o desarrollos propios, alineados con los objetivos estratégicos de la organización. De esta manera, se promueve no solo la eficiencia y la sostenibilidad técnica, sino también la autonomía operativa y la soberanía tecnológica en el ámbito público.

5.1 Trabajos Futuros

En el marco de la consolidación de un modelo institucional basado en los principios de Gobernanza, Gestión de Riesgos y Cumplimiento (GRC), se identifican líneas de acción futuras que resultan estratégicas para profundizar en materia de seguridad de la información. Estas iniciativas no sólo responden a necesidades operativas, sino que constituyen pilares fundamentales para asegurar una correcta gestión de los activos.

Se proyecta la elaboración e implementación de una normativa institucional de uso aceptable de los activos, que permita establecer con claridad los límites, responsabilidades y buenas prácticas en torno al uso de computadoras, recursos de red, dispositivos móviles, internet y correo electrónico. Esta normativa no solo contribuirá a la optimización del uso de los activos, sino que también permitirá tener mecanismos de control del cumplimiento de las políticas vigentes y reducirá significativamente los riesgos derivados de un uso inadecuado, negligente o no autorizado de los activos informáticos.

Es necesario un protocolo de respuesta ante amenazas de seguridad informática, que defina, de forma secuencial y con criterios de responsabilidad compartida, las acciones que deben ejecutar los actores intervinientes para contener, reportar y remediar un incidente, reduciendo el tiempo de exposición y el impacto sobre la infraestructura.

Por último, es necesario avanzar con el desarrollo de una política de continuidad operacional y de recuperación ante desastres. Dicha política deberá contemplar de forma estructurada los procedimientos, responsables y activos involucrados, a fin de garantizar la restauración de los servicios críticos ante incidentes de seguridad que comprometan la operatividad servicios críticos ante eventos de seguridad.

Cabe aclarar que, la ejecución de estos proyectos no requiere necesariamente la adquisición de herramientas comerciales o propietarias, sino que también puede realizarse a través del empleo de software libre, cuya disponibilidad y calidad son

ampliamente reconocidas, o bien, mediante el desarrollo de soluciones propias dentro del organismo.

Referencias

1. MAGERIT 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (2012). https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
2. Cappelli T., Lliteras A., & Bazán, P. (2025). Acciones y protocolos en ciberseguridad para el Poder Judicial de la Provincia de Buenos Aires - Argentina. In Simposio de Informática en el Estado (SIE 2025) - JAIIO 54 (Universidad de Buenos Aires, 4 al 7 de agosto de 2025). *En prensa.*
3. International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. https://www.iso.org/standard/27001
4. Centro Criptológico Nacional. (2012). *MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método* (v3). Madrid: Ministerio de Hacienda y Administraciones Públicas. NIPO: 630-12-171-8
5. Shah, S. B. (2025). Machine learning for cyber threat detection and prevention in critical infrastructure. Journal of Global Research in Electronics and Communication, 2(2), 1–7. https://doi.org/10.5281/zenodo.14955016