Hacia un marco holístico de Ciberseguridad para e-Gobiernos según Análisis Sistemático de Propuestas existentes*

Víctor Figueroa[1][0000−1111−2222−3333], Luis E. Sánchez[1][0000−1111−2222−3333], and Antonio Santos-Olmo[1][0000−1111−2222−3333]

Universidad de Castilla-La Mancha. Ciudad Real, España

Abstract. Para los organismos gubernamentales, gestionar la seguridad de la información significa un compromiso implícito que estos mantienen con la sociedad de la información. La sociedad supone que aquellos datos que son de su propiedad y que resultan de interés para el Estado, para que éste logre llevar a cabo el ejercicio de sus funciones, se gestionan de forma segura. Ahora bien, gestionar la seguridad de la información en este tipo de organismos supone un reto que difiere en gran medida a los que se presentan cuando nos encontramos en el contexto de una organización del sector privado. Se puede idealizar a un gobierno como una gran empresa compuesta por una serie de áreas´ de negocio representadas por sus organismos públicos, adonde cada uno de ellos captura información de los ciudadanos afín a sus intereses de negocio, la procesan, la comparten con sus pares, y ponen a disposición de la sociedad información que retroalimenta al ciclo de vida de sus procesos. En este contexto, la seguridad de toda ´esta información es tan robusta como lo es el más débil en toda la cadena de procesos. Convergen en este escenario diversos factores: diferentes servicios e infraestructuras tecnológicas con sus amenazas inherentes, diferentes marcos normativos aplicables, diferentes grados de madurez en materia de cultura de seguridad, etc., con lo cual, conocer el grado general de seguridad para un Gobierno es imposible si no se cuenta con un modelo de gestión de la seguridad de la información que alcance de forma transversal a todos los organismos que lo componen. En este trabajo, se propone, a partir de un análisis sistemático de las propuestas existentes, modelar un ecosistema seguro para los organismos de gobierno, que utilice como ejes transversales el cumplimiento normativo, la gestión de riesgos, y un marco de intercambio seguro de datos, que sea capaz de garantizar un nivel adecuado de la seguridad de la información de manera holística.

Keywords: Seguridad de la Información Pública · Ciberseguridad · e-Gobierno · Gestión de Riesgos · Cumplimiento Normativo · MARISMA · X-ROAD.

* GSyA Research Group, Universidad de Castilla-La Mancha. Ciudad Real, España

1 Introducción

Los gobiernos no han estado exentos de la transformación digital que vive la sociedad de la información durante las últimas décadas; en realidad, han sido, en gran medida, sus principales impulsores [1], dando paso al concepto de gobierno electrónico o e-Gobierno, que se refiere al uso de tecnologías de la información y la comunicación (TIC) para mejorar y simplificar los servicios gubernamentales y la relación entre los ciudadanos y el gobierno [2]. Ahora bien, no es nuevo que esta transformación digital ha sido pobremente acompañada con estrategias de seguridad de la información; abundan los antecedentes sobre incidentes de gravedad en los cuales se vieron afectados datos de ciudadanos, e incluso información sensible de los gobiernos [3]. En este sentido, tal como ha ocurrido con internet, la seguridad se ha ido construyendo a contramano de las implementaciones de tecnología [4], y dotar de seguridad a algo que no es seguro desde su concepción, representa un desafío continuo. En este marco, Estonia, el país más digitalizado del mundo [5] supone un factor diferencial. Este país, desarrolla e implementa un marco para intercambio seguro de datos conocido como X-TEE [6] desde el año 1.998, que le ha permitido sentar las bases de uno de los Gobiernos Electrónicos más avanzados. En el año 2.018, Estonia fundó junto a Islandia, Finlandia y otros países nórdicos, el Instituto Nórdico para Soluciones de Interoperabilidad [7], NIIS por sus siglas en inglés, con el objetivo de aunar esfuerzos y recursos tendientes a promover el uso del framework, bajo el principio código abierto, bautizándolo con el nombre de X-ROAD. Si bien la adopción de este framework supone la instauración de un ecosistema en el cual sus miembros pueden interoperar de forma segura, es conveniente, y las buenas prácticas de seguridad de la información así lo sugieren, someter a estas implementaciones a revisiones permanentes para garantizar que los servicios de seguridad se mantengan vigentes en el tiempo; en otras palabras, debe ser sometido a una gestión de riesgos. La gestión de riesgos es un proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización, para saber que decisión tomar ante una posible eventualidad [8]. En este sentido, una metodología emergente es la Metodología de Análisis de Riesgos Sistemáticos Basado en Patrones Asociativos, MARISMA [8], que permite analizar los riesgos de las organizaciones de forma dinámica y basado en patrones reutilizables y adaptables. En un contexto tan diverso como el de los Entes Gubernamentales, adonde cada actor tiene requerimientos de seguridad, requerimientos normativos y legales específicos de su dominio, MARISMA, a través de su enfoque basado en patrones, se transforma en una excelente herramienta para gestionar los riesgos y facilitar a la vez el cumplimiento normativo. Estas tres capacidades, intercambio seguro de datos, gestión de riesgos y cumplimiento normativo, unidas a los principales aportes que se pueden extraer de las propuestas existentes de estrategias de ciberseguridad para e-Gobiernos, permiten confiar en que la creación de un marco holístico es posible.

El articulo queda organizado de la siguiente forma, en el apartado segundo se analizará el plan seguido; en el apartado tercero se expone el método de investigación de revisión sistemática de la literatura utilizado; en el apartado cuarto se muestran los resultados obtenidos; en el apartado quinto se analizan dichos resultados; en el apartado sexto se propone una potencial solución a las carencias detectadas; finalmente el último apartado se analizan las principales conclusiones obtenidas.

2 Plan de Revisión

En esta sección se formula la pregunta de investigación. Se enfoca sobre el área de interés de la obra y define tanto el problema a abordar como sus principales características.
Para ello, se establece el Alcance de la pregunta de investigación, siendo el resultado de esta revisión adquirir conocimientos sobre propuestas existentes para establecer una estrategia de ciberseguridad para e-Gobiernos. Posteriormente, se someten a análisis para descubrir qué aspectos comparten, en qué se diferencian, e identificar las oportunidades de mejora, complementándolas con los tres ejes transversales planteados: cumplimiento normativo, gestión de riesgos y el marco de intercambio seguro de datos. La pregunta de investigación definida para este trabajo es, por lo tanto, la siguiente:

¿Qué trabajos se han realizado para establecer estrategias de ciberseguridad para e-Gobiernos que pueda ser aplicable a Argentina?

Las palabras clave y los conceptos relacionados que se utilizaron para formular esta pregunta durante la ejecución de la revisión son las siguientes:

Seguridad de la Información: Ciberseguridad, políticas de seguridad de la información, estrategias de ciberseguridad para gobiernos.
e-Gobierno: gobierno electrónico, gobierno 4.0.
Gestión de Riesgos: metodologías de análisis de riesgos, marcos de análisis de riesgos, modelos de análisis de riesgos asociativos.
X-ROAD: marco de intercambio seguro de datos, intercambio de datos para e-gobiernos, interoperabilidad.

Las propuestas existentes sobre estrategias de ciberseguridad para e-Gobiernos se encuentran bajo análisis y revisión sistemática. El énfasis se coloca en las propuestas orientadas a e-Gobiernos. Las más importantes están siendo documentadas y son sometidas posteriormente a análisis y comparación. La población analizada comprende las publicaciones existentes en los repositorios de las fuentes de datos seleccionadas que están relacionadas con el objetivo de este trabajo.

3 Método de Revisión

El método de revisión se basa en el protocolo de investigación. En esta etapa, se definen: la estrategia de búsqueda, las fuentes que se están utilizando para identificar las propuestas primarias, las posibles restricciones, los criterios de inclusión y exclusión, los criterios para evaluar la calidad de las propuestas primarias y la forma en la que se extraen y sintetizan los datos de las propuestas.

3.1 Selección de fuentes

El objetivo de esta fase es establecer las fuentes utilizadas para buscar las propuestas existentes. Los criterios empleados para seleccionar las fuentes de búsqueda permiten consultar documentos en internet o en formato digital disponibles en la biblioteca de la Universidad de Castilla-La Mancha. Este repositorio contiene libros electrónicos y proporciona acceso a las siguientes bibliotecas digitales: ACM, IEEE, Elsevier, Springer, Taylor&Francis, a la Biblioteca línea Wiley, entre otras. También permite realizar búsquedas a través de motores con capacidades de consultas avanzadas y búsquedas por palabras clave, por editoriales, libros, revistas y congresos recomendados por expertos en la materia.
La búsqueda inicial de propuestas se realizó mediante motores de búsquedas existentes en la web, bases de datos electrónicas y también mediante búsquedas manuales como búsquedas en revistas, conferencias, libros, publicaciones específicas o publicaciones de investigación recomendadas por expertos en el campo.

3.2 Selección de propuestas

Habiendo definido las fuentes, es necesario a posteriori, describir el proceso y los criterios empleados durante la ejecución de esta revisión para seleccionar y evaluar las propuestas existentes.
El primer paso en la selección de propuestas es adaptar la cadena de búsqueda al motor de búsqueda y ejecutar la consulta, limitar la búsqueda a artículos publicados en los últimos 10 años (2013-2023). Los criterios de inclusión y exclusión deben estar basados en la pregunta de investigación. El criterio de inclusión actúa sobre los resultados obtenidos al ejecutar la búsqueda en la fuente, por lo tanto, permite realizar una primera selección de trabajos considerados en el contexto de la revisión como candidatos a convertirse en propuestas para revisión. El principal criterio de inclusión es el análisis del título, palabras clave y resumen de cada trabajo. Esto hace posible ver como estas palabras están relacionadas y por qué se seleccionó el trabajo. Este criterio ubica y elimina la mayoría de los resultados obtenidos que no contribuyen a las estrategias de ciberseguridad para e-Gobiernos. El criterio de exclusión actúa sobre el subconjunto de trabajos obtenidos y hace posible la obtención del conjunto de trabajos de interés.

3.3 Ejecución de la selección

En este apartado, la búsqueda ha sido ejecutada en cada una de las fuentes seleccionadas para obtener una lista primaria de propuestas para evaluación posterior aplicando todos los criterios especificados. Los procedimientos de selección de propuestas se aplicaron sobre todos los resultados de las búsquedas. La ejecución de la consulta inicialmente arrojó un total de 9.824 resultados para el período 2013-2023, de los cuales 27 estudios corresponden exactamente a todos los criterios de inclusión y exclusión previamente definidos, y fueron eventualmente seleccionado.
Para estructurar los resultados del proceso de selección, los estudios fueron agrupados por iniciativa, distinguiendo cuatro categorías específicas y una categoría genérica que

incluye las propuestas restantes. A continuación, se brinda un breve detalle y mayor información se documenta en versiones extendidas del presente trabajo:

- Proceso: Conjunto de actividades planificadas en sucesivas fases con el fin de lograr un determinado objetivo.
- Framework: Estructura en capas, cuya función es para apoyar o guiar la construcción de un riesgo marco de gestión, que abarca un conjunto de funciones dentro del sistema, junto con las relaciones entre ellos.
- Maqueta: Artefacto específico que proporciona una representación de un sistema complejo para facilitar su comprensión.
- Metodología: Conjunto de procedimientos y técnicas que se aplican de forma ordenada y sistemática. manera en la resolución de un problema, en nuestro caso, con el fin de llevar a cabo una correcta gestión del riesgo gestión en una organización. ellos integran los conceptos de Proceso y Modelo.
- Otros: Propuestas que no encajaron del todo en las tipologías anteriores, pero que contienen conceptos relevantes para la investigación.

4 Recolección de Información

Se han recolectado 27 trabajos en la etapa anterior; como se muestra en la Figura 1, gran parte de los trabajos están relacionados con e-Gobierno y gestión de riesgos; en cuanto a X-ROAD, se han obtenido trabajos enfocados en la interoperabilidad de datos, y en relación a las estrategias de seguridad de la información, los trabajos recolectados abordan este dominio bajo el concepto de ciberseguridad.

Se pudieron identificar también otros conceptos que son transversales a estos dominios a partir del mapa de conexiones, el cual ilustra a estos dominios en grupos. El Clúster 1 agrega las publicaciones relacionadas con el dominio de “Gobierno Electrónico”, el Clúster 2 agrupa al dominio de “Gestión de Riesgos”, el Clúster 3 al de “Marcos de Trabajo”, y el Clúster 4 al dominio de “Interoperabilidad”. Cabe destacar que el tamaño de cada nodo varía según el número de citas de los trabajos que agrupa.

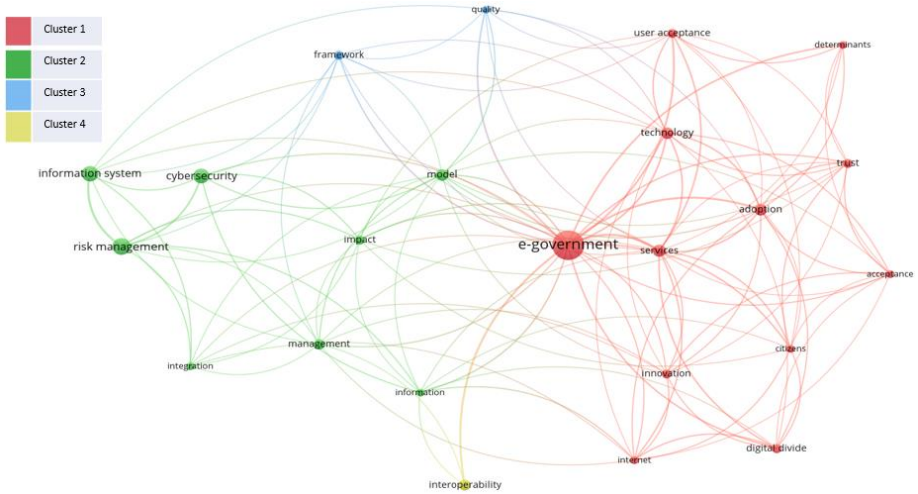

Fig. 1 – Conexiones entre dominios de los trabajos revisados.

Por otra parte, en la Figura 2, se representa a los países en los cuales han sido publicados cada uno de los trabajos revisados; al igual que en la Figura 1, el tamaño de los nodos representa la cantidad de citas que agrupan, y en color se representan los años de publicación.

Fig. 2 – Citas por país de origen y años de publicación de los trabajos revisados.

5 Análisis de Resultados

A partir de los gráficos anteriores y de la revisión sistemática en proceso, se han identificado una serie de carencias entre las que destacamos, por ser las más importantes, de manera resumida, las siguientes:

- Carencia de estrategias de e-Gobierno con enfoque basado en Gestión de Riesgos: Las estrategias de e-Gobierno enuncian un conjunto de medidas extraídas principalmente de normas estándares, pasando por alto la oportunidad de establecer una estrategia sostenible basada en Gestión de los Riegos tecnológicos.
- Carencia de criterios de seguridad de la información bien definidos para los de marcos de Interoperabilidad: En las estrategias de e-Gobierno, la Interoperabilidad es considerada una piedra angular de la transformación digital, sin embargo, no se establecen criterios sólidos para dotar a los procesos interoperables de una capa seguridad robusta.
- Bajo nivel de producción de trabajos que aborden las preguntas de búsqueda, en los países iberoamericanos: La escasez desarrollos en países iberoamericanos dificultan evaluar los progresos a partir de legislaciones comparativas.

6 Propuesta de marco holístico

El marco propuesto en este documento se desarrolló para abordar los desafíos identificados durante la revisión sistemática de la literatura en las secciones anteriores. En resumen, una estrategia de ciberseguridad integral para e-Gobiernos sigue sin consensuarse.

El Marco propuesto, pretende garantizar la seguridad de los datos durante el intercambio de información entre los organismos de Gobierno, asegurando su confidencialidad, integridad y disponibilidad a partir de una arquitectura sólida y madura, complementada por una metodología de gestión de riesgos para sistemas de información, que facilite el cumplimiento normativo y la ejecución dinámica de análisis de riesgos, que bajo los criterios de mejora continua, permita elevar de manera progresiva el grado de cumplimiento de las medidas de seguridad contempladas en los marcos normativos.

En la Figura 3, la metodología de gestión de riesgos y cumplimiento normativo MARISMA establece tres procesos bien definidos: el proceso 1 refiere a la Generación de Patrones de Riesgos que vinculan un estándar normativo con los componentes del análisis de riesgos; el proceso dos que inicia con la selección de un patrón de riesgo, siguiendo con el inventario de activos, el checklist de cumplimiento, el cálculo de los riesgos y obtención de un Plan de Mantenimiento; y un tercer proceso dedicado al Mantenimiento Dinámico del Riesgo, que permite actualizar los cálculos de riesgos a partir de cualquier cambio mínimo en el contexto.
Cada organismo de gobierno cuenta con una instancia propia de MARISMA que le permite gestionar sus riesgos de forma eficiente y dinámica.
A la vez, los organismos interactúan entre sí, intercambiando información a través de una instancia de X-ROAD; para ello, cuentan con un componente local conocido como Servidor de Seguridad, que hace de pasarela de seguridad entre los sistemas de información internos y los demás Servidores de Seguridad de la Red. Este componente permite el transito de datos hacia uno y otro extremo bajo un esquema de autenticación basado en Certificados Digitales de Servidor y Certificados de Firma de mensajes; además, el acceso a cualquier servicio de datos provisto por el sistema de información interno debe ser previamente definido en la pasarela.
Esta instancia de X-ROAD es coordinada por un Servidor Central que establece y distribuye las políticas de seguridad a los Servidores de Seguridad que forman parte de su instancia. Las Políticas de seguridad se basan principalmente en determinar quiénes brindan de servicios de seguridad, tales como la Autoridad de Certificación que emite los Certificados de Autenticación de Servidor y Certificados de Firmas de mensajes, además del servicio de validación de certificados OCSP y el Servicio de Autoridad de Tiempo. El objetivo de los Servicios de Seguridad es garantizar la integridad, confidencialidad y el no repudio de las transacciones.

Fig. 3 – Marco holístico propuesto de ciberseguridad para e-Gobiernos

Teniendo en cuenta que existe además una capa complementaria de protección de ciberseguridad compuesta por los dispositivos de seguridad propios de un esquema de defensa en profundidad, se establece con este marco un ecosistema tecnológico con características robustas de seguridad.

7 Conclusiones

Dentro de las limitaciones de extensión del trabajo, se ha buscado mostrar las bases tanto de los resultados iniciales de investigación como de la arquitectura del framework.
Se ha realizado una revisión sistemática de la literatura existente, y se ha podido identificar un conjunto de carencias que dan paso a la construcción de un nuevo framework que resuelva las carencias existentes. En el presente artículo se ha mostrado la base sobre la que está desarrollando dicho framework.
El trabajo futuro consistirá en el desarrollo de todas las etapas del framework y su validación sobre el contexto del gobierno regional de la provincia de Neuquen.

Agradecimientos

Este trabajo ha sido Desarrollo bajo el auspicio de los proyectos AETHER-UCLM (PID2020-112540RBC42) financiado por MCIN/AEI/10.13039/501100011033, y ALBA-UCLM (TED2021-130355B-C31, id.4809130355-130355-28-521) financiado por el Ministerio de Ciencia e Innovación.
Un prototipo basado en la propuesta presentada se implementa en la Administración Pública del Gobierno de la Provincia del Neuquén, República Argentina, desde donde se extraen experiencias fundamentales para el desarrollo de éste trabajo.

Referencias

1. Alrubaiq, Abdullah and Alharbi, Talal: Developing a Cybersecurity Framework for e-Government Project in the Kingdom of Saudi Arabia. Journal of Cybersecurity and Privacy, 302-318 (2021)
2. Hamza Ahmad Qureshi and Yaamina Salman and Sidra Irfan and Nasira Jabeen: A systematic review of e-Government Evaluation. Department of Economics, University of the Punjab, pp. 355–390. (2017).
3. Artiles, Néstor Ganuza: Situación de la Ciberseguridad en el ámbito internacional y en la OTAN. Cuadernos de estrategia.165-214. Instituto Español de Estudios Estratégicos (2011).
4. Abbate, Janet: Internet: su evolución y sus desafíos. Journal Fronteras del conocimiento (2008).
5. Bekerman, Uriel and Cresta, Guido Damián: Sociedades digitales: e-Estonia (Digital Societies: e-Estonia). Diario DPI Suplemento Derecho y Tecnologías. 55-05 (2020).
6. Adeodato, Rodrigo and Pournouri, Sina: Secure implementation of e-governance: A case study about Estonia. Journal Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. 397-429. Springer (2020).
7. Robles, Gregorio and Gamalielsson, Jonas and Lundell, Bjó: Setting up government 3.0 solutions based on open source software: the case of X-road. Electronic Government: 18th IFIP WG 8.5 International Conference, EGOV 2019, San Benedetto Del Tronto, Italy. 69-81. Springer (2019).
8. Santos Olmo Parra, Antonio and Sanchez Crespo, Luis Enrique and Alvarez, Esther and Huerta, Monica and Fernandez Medina Paton, Eduardo: Methodology for Dynamic Analysis and Risk Management on ISO27001. IEEE Latin America Transactions. 2897-2911 (2016).