

Una guía para

Garantizar la seguridad en las adquisiciones de tecnología electoral



Center for Internet Security



-
- Entidad sin fines de lucro.
 - Crowdsourcing.
 - Proteger a las organizaciones públicas y privadas.
 - Centro de análisis e intercambio de información de la infraestructura electoral.

Autores



Mike García

- Economista doctorado
- Experto en ciberseguridad
- National Strategy for Trusted Identities in Cyberspace (NIST)



John M. Gilligan

- Presidente y director ejecutivo de CIS
- Director de Información de la Fuerza Aérea y el Departamento de Energía
- Director Schafer Corporation



Aaron Wilson

- Director sénior de seguridad electoral en CIS
- Director de Enhanced Voting (empresa privada de votación)


Parte I: Introducción



Introducción

- La **comunidad electoral** identificaron una **dificultad** constante para obtener resultados de **seguridad** de calidad en adquisiciones.
- Destinada a **funcionarios electorales**, funcionarios de adquisiciones y *proveedores*.
- El **objetivo** es **mejorar la seguridad** de la **infraestructura electoral** proporcionando un conjunto de mejores prácticas de seguridad específicas para adquisiciones de IT.



A photograph of Donald Trump, wearing a dark blue suit and a red tie, speaking at a podium. He is holding a white rectangular sign in front of him with both hands. The sign has the words "ELECTORAL" and "FRAUD" printed in large, bold, black, sans-serif capital letters, one above the other. In the background, to the right, is a large American flag. To the left, a portion of a gold-framed picture is visible on the wall.

**ELECTORAL
FRAUD**

The background of the slide is a photograph of a modern, curved building with a metallic, reflective facade, possibly the Walt Disney Concert Hall. The entire image is overlaid with a semi-transparent blue filter. The text is positioned on the left side of the slide.

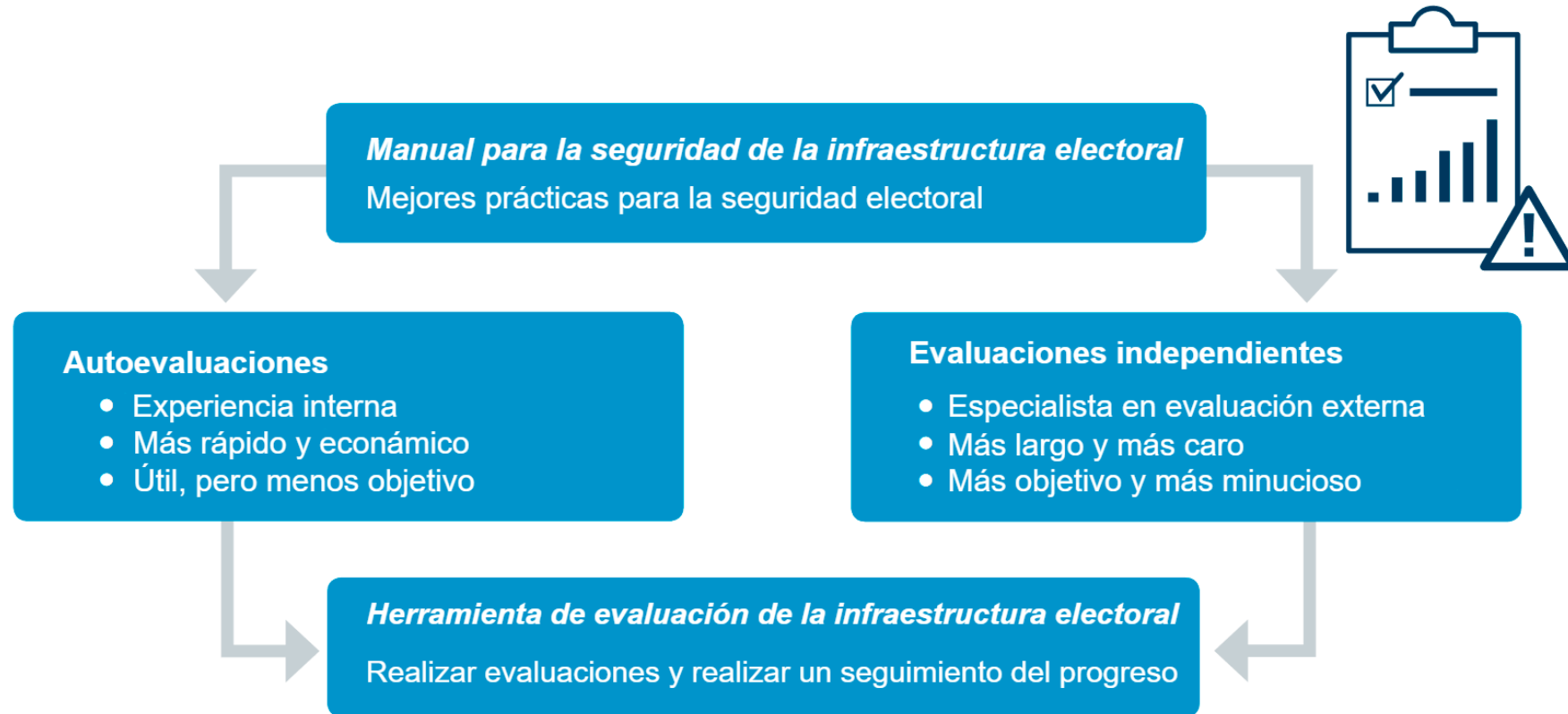
Parte II:

Riesgo de seguridad en la adquisición de tecnología electoral

Riesgo de seguridad en la adquisición de tecnología electoral

- Evaluar el riesgo:

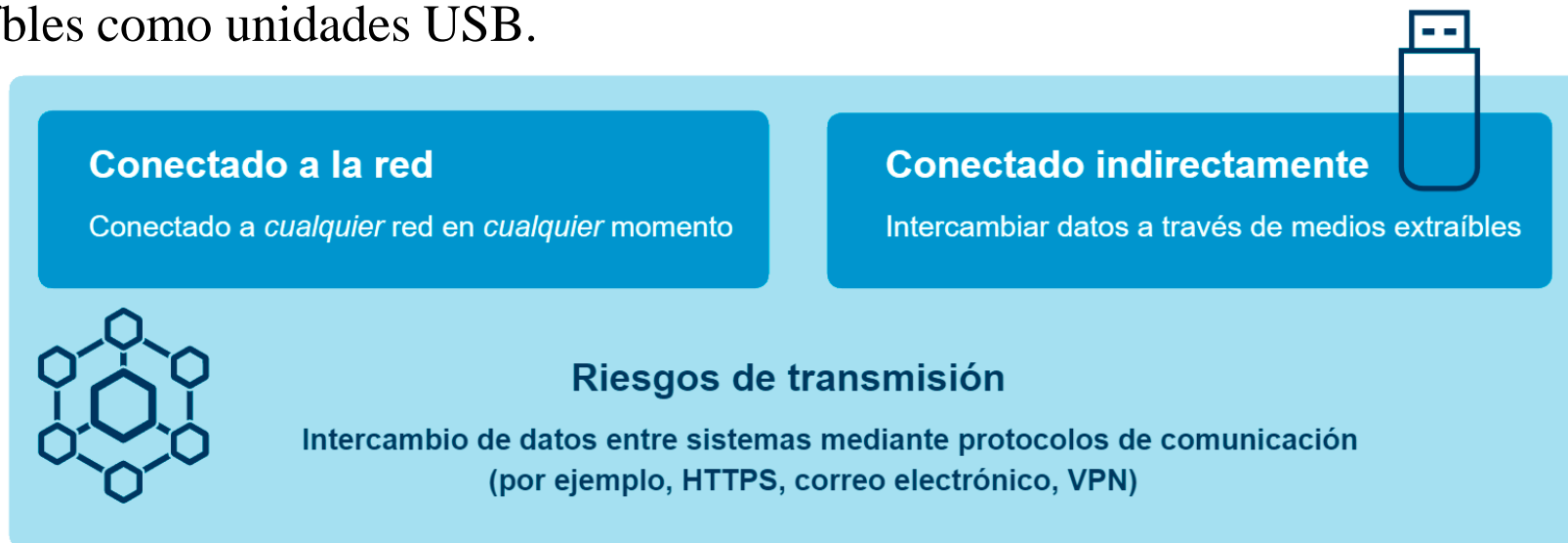
- **Autoevaluaciones:**
más rápidas y
menos costosas.
- **Evaluaciones independientes:**
suelen costar más y
demorar más,
completes.



Riesgo de seguridad en la adquisición de tecnología electoral

- **Riesgo organizacional:**

- CIS identificó que el nivel más alto de riesgo proviene de **sistemas que están conectados a la red**, (no solo a Internet).
- Los funcionarios electorales deben confirmar que las máquinas de votación no están conectadas a la red
- El intercambio de datos entre ellos, se produce indirectamente a través de medios extraíbles como unidades USB.



Riesgo de seguridad en la adquisición de tecnología electoral

- 3 clasificaciones para la aplicabilidad de los sistemas para cada mejor práctica:



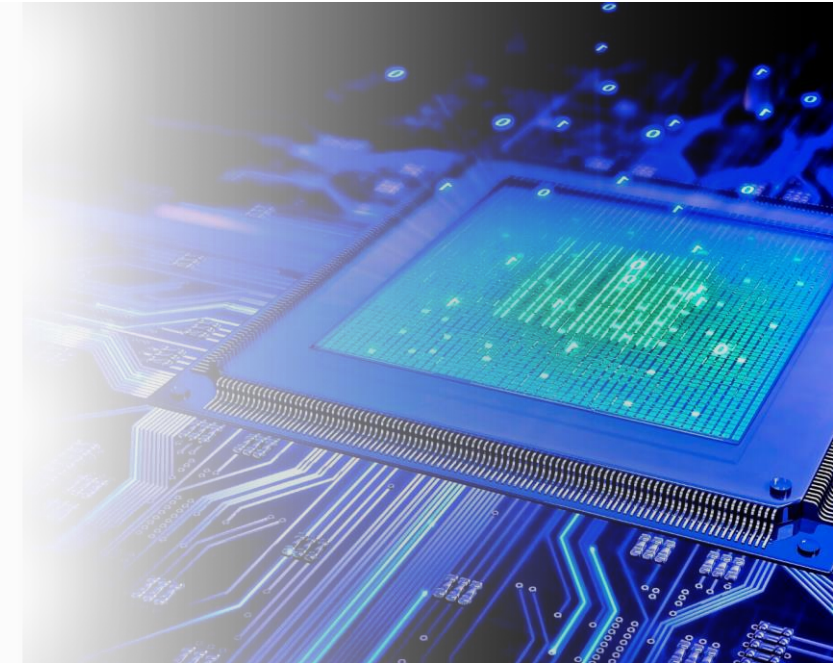
Parte III:

El proceso de adquisiciones



El proceso de adquisiciones

- **Protección de la información de seguridad confidencial:**
 - Muchos proveedores dudan en compartir información de seguridad que, si se divulga, podría beneficiar a los atacantes o competidores de la industria.
 - Las oficinas gubernamentales tienen la obligación de compartir información con el público.
 - Durante las adquisiciones, esta determinación debe dejarse clara a los posibles proponentes



El proceso de adquisiciones

- Comprensión de los tipos de adquisiciones comunes:



Contratos prenegociados

- Lo mejor para compras simples y de productos básicos.
- Por lo general, el más rápido y el más barato
- Flexibilidad limitada

El precio más bajo

- Mejor cuando los requisitos están bien definidos y se pueden lograr fácilmente
- Funciona bien cuando hay poca diferenciación entre los proponentes.

Mejor valor

- Ideal para sistemas complejos y aquellos con interdependencias
- Requerir justificación
- Por lo general, será mejor para sistemas electorales especializados.

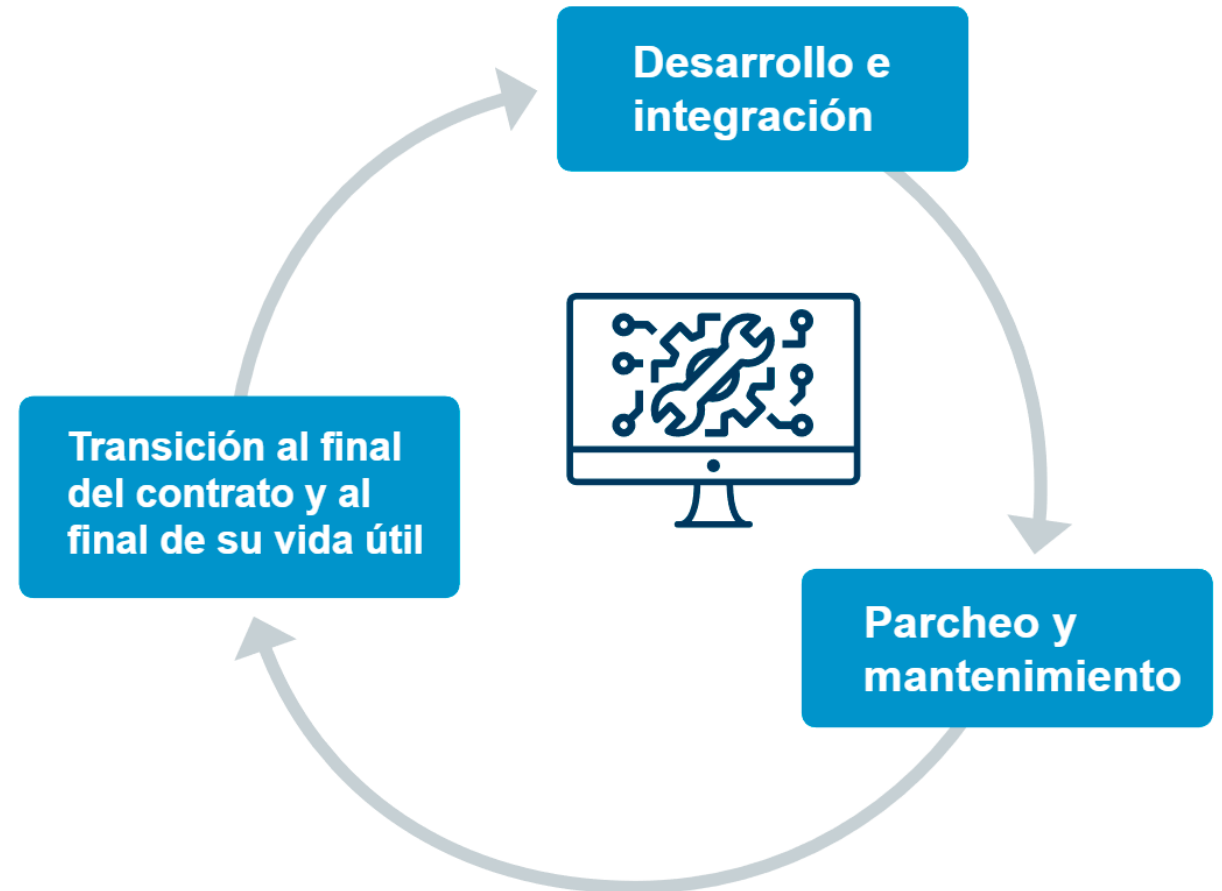
Parte IV:

Ciclo de vida de productos y servicios de IT



Ciclo de vida de productos y servicios de IT

- Protección de la información de seguridad confidencial.
- Al planificar una adquisición, se debe **pensar en este ciclo de vida completo** que comienza antes de la adquisición y termina mucho después.
- **Deficiencias en el diseño, implementación, integración o configuración puede generar vulnerabilidades** que pueden ser identificadas y explotadas por actores malintencionados.



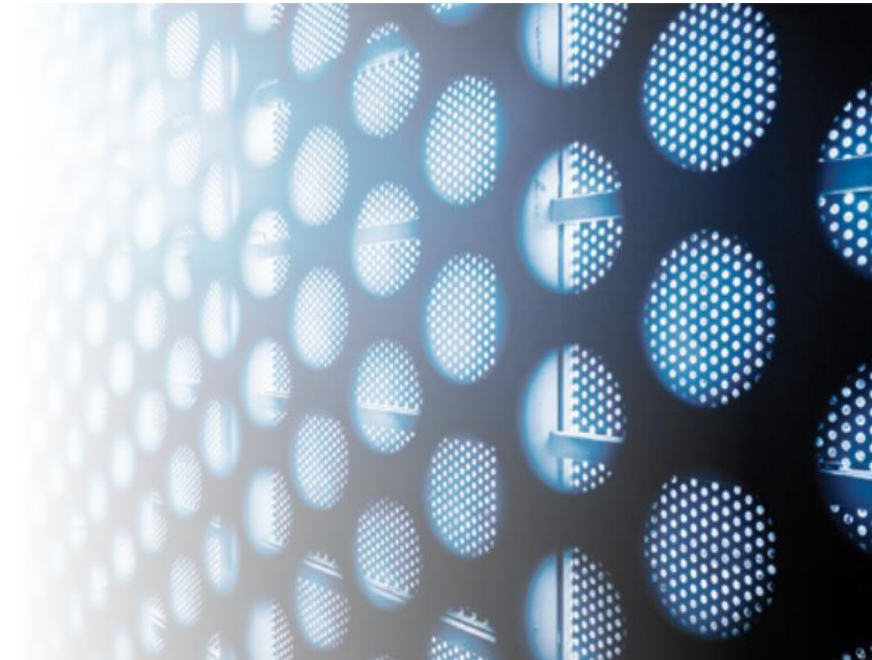
Parte V:

Ciberseguridad más allá de las adquisiciones



Ciberseguridad más allá de las adquisiciones

- La mayoría de los **funcionarios** electorales **no son expertos en ciberseguridad**.
- La mayoría de los estados han desarrollado **enfoques para ayudar a los funcionarios electorales** que no son competentes en la seguridad de la tecnología y la infraestructura electorales.
- El enfoque general de seguridad de IT debe **combinar prácticas de adquisición de calidad con seguridad operativa**.





Parte VI:

Prácticas de ciberseguridad en las adquisiciones de IT

Prácticas de ciberseguridad en las adquisiciones de IT

- **Conjunto de mejores prácticas** en sus adquisiciones para mejorar los resultados de seguridad.
- Las mejores prácticas están **destinadas a generar respuestas de proveedores potenciales** que puedan ayudar a los funcionarios electorales a tomar decisiones informadas.
- Para cada una de las mejores prácticas, se **clasifican en categorías**.



Práctica:

Descripción

Aplicabilidad del sistema:

El tipo de sistemas a los que se aplica la recomendación:

- Todos
- Operacionales
- Críticos

Tipo de IT:

El tipo de IT al que se aplica la recomendación:

- Hardware
 - Software
 - Servicios
 - Crítico
-

Idioma sugerido:

Este es el idioma recomendado que puede incluir en sus documentos de adquisición. La mayoría de las veces tendrá la forma de una pregunta para una RFI o RFP, pero también podría enumerar qué buscar en otros aspectos de la adquisición o qué incluir en un contrato.

Bueno:

Una descripción de una buena respuesta a la recomendación o lenguaje para incluir en un documento de adquisición.

Malo:

Una descripción de una respuesta deficiente a la recomendación o lenguaje para incluir en un documento de adquisición.

Consejos:

Detalles adicionales que podrían contribuir a una adquisición más exitosa.

Referencias y enlaces:

Recursos o sitios web que pueden resultar útiles.

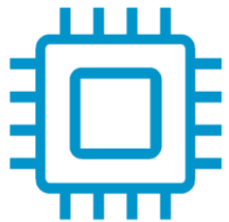
Prácticas de ciberseguridad en las adquisiciones de IT



- **Personas:** Garantizar que las personas tengan la experiencia y los conocimientos adecuados en ciberseguridad.



- **Procesos:** Asegurarse de que el proponente tenga los enfoques correctos para lograr los resultados que afirma.



- **Tecnología:** garantizar que el proponente pueda ofrecer soluciones de IT que satisfagan las necesidades de seguridad de su organización.

Mejores prácticas: Personas (9)

- Cualificaciones y experiencia de las personas propuestas para trabajar.
- Desempeño pasado demostrado realizando el trabajo propuesto.
- Políticas de personal del proponente con respecto a los estándares de contratación.
- Ubicación del proponente donde se realizará el trabajo.
- Procedimientos de formación para el proponente.
- Políticas y prácticas del proponente para el personal de los subcontratistas.

Mejores prácticas: Procesos (15)

- El proceso regular del proponente para identificar y remediar los riesgos cibernéticos, con un enfoque particular en los componentes y la información que son críticos para el éxito de la misión y una mayor atención a estos elementos.
- Plan de transición para la finalización del contrato.
- Acuerdo del proponente para implementar un conjunto específico de controles de seguridad.
- La voluntad del proponente de adherirse a las prácticas de seguridad establecidas de su organización.
- Plan de seguridad para obra propuesta. Proporcionar el plan de seguridad para implementar los requisitos y controles de seguridad para el producto o servicio.
- Certificaciones de procesos en toda la empresa y adherencia demostrada a los procesos documentados del proponente.

Mejores prácticas: Tecnología (9)

- Controles sobre los datos y el acceso.
- Opciones de seguridad en la nube.
- Uso de estándares abiertos y enfoques comunes en software y formatos de datos comunes.
- Arquitectura de seguridad para la solución propuesta o requerida.
- Aproximación a la criptografía y la gestión de claves para la seguridad de los datos.
- Propiedad de software y otros activos.
- Protección avanzada de *endpoints* en sistemas centrales.

Referencias

- https://en.wikipedia.org/wiki/Center_for_Internet_Security
- <https://www.cisecurity.org/blog/election-technology-procurements-guide/>
- <https://www.cisecurity.org/elections-resources/>
- <https://www.kuppingercole.com/events/eic2015/speakers/1309>
- <https://www.nist.gov/blogs/i-think-therefore-iam/authors/mike-garcia>
- <https://www.cisecurity.org/about-us/leadership/john-m-gilligan/>
- <https://www.linkedin.com/in/wilsoaa>
- <https://www.rsaconference.com/experts/aaron-wilson>
- <https://www.cisecurity.org/press-release/cis-launches-election-technology-procurement-guide/>



Fin

Presentación basada en:
Election Technology Procurements Guide (2019)