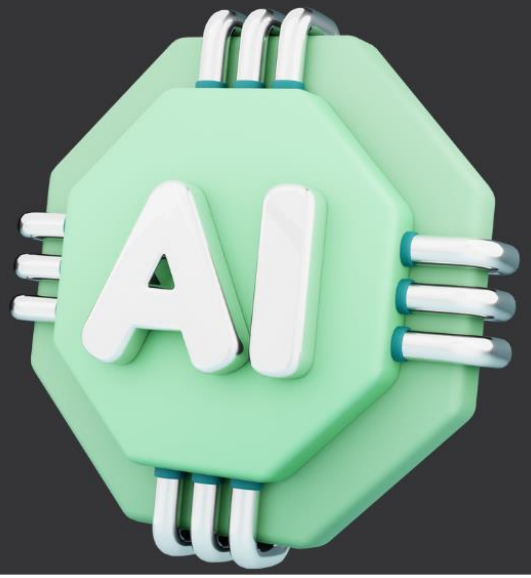
15ª Jornada de Auditoría del Sector Público

La ciberseguridad y la inteligencia artificial en el Sector Público



24 de abril de 2024 | 9:00 a 13:45h | Formato híbrido desde la Sede del CCJCC

Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

LA CIBERSEGURIDAD EN EL SECTOR PÚBLICO

PONENTES

Javier Burguera

Senior manager Risk Advisor-Cyber
en Deloitte

Vanessa González

Coordinadora del Equipo de
Auditoría Informática IGAE

En general: las personas son, cada vez, más dependientes de los sistemas informáticos en su día a día.

- **¿Cuáles son las debilidades de los sistemas informáticos? ¿están identificados?**

Las debilidades de los sistemas informáticos están constantemente en evolución debido a la aparición de nuevas vulnerabilidades y amenazas. Podemos agrupar las debilidades de los sistemas en:

- *Vulnerabilidades de software*
- *Falta de parches de seguridad*
- *Configuraciones inseguras*
- *Controles de acceso insuficientes.*
- *Falta de monitorización y detección de amenazas*

Una forma de identificar estas debilidades es mediante el Common Vulnerabilities and Exposures (CVE), un diccionario público de información de seguridad sobre vulnerabilidades de seguridad conocidas.

La falta de conciencia sobre las amenazas y las mejores prácticas de seguridad, así como la falta de capacitación del personal, aunque no son debilidades de los sistemas, son aprovechadas también por los atacantes para comprometer los sistemas. Es lo que se llama ataques de ingeniería social.

Javier Burguera

- **¿Cuáles son las amenazas y los riesgos? ¿se pueden mitigar? ¿Qué protecciones existen?**

Las amenazas y riesgos en ciberseguridad pueden ser complejos, pero algunas de las tendencias incluyen:

- *Amenazas persistentes avanzadas (APTs)*
- *Ransomware y extorsión*
- *Ataques a la cadena de suministro*
- *Desinformación y manipulación*

Para mitigar estas amenazas y riesgos, es fundamental adoptar un enfoque integral de ciberseguridad que abarque tanto la prevención como la detección y respuesta.

Algunas de las protecciones y medidas que pueden ayudar a mitigar estos riesgos incluyen:

- *Implementación de mejores prácticas de seguridad*
- *Capacitación y concientización de los empleados*
- *Desarrollo de capacidades de detección y respuesta*
- *Compartir información*

Las organizaciones deben mantenerse actualizadas sobre las últimas vulnerabilidades y amenazas, y tomar medidas proactivas para proteger sus sistemas contra posibles ataques.

Y es esencial que las organizaciones realicen evaluaciones regulares de seguridad para identificar y remediar estas debilidades en sus sistemas informáticos.

Javier Burguera

- Si los objetivos de la ciberseguridad o seguridad informática para la protección de las infraestructuras, la información y los usuarios, son la protección, la detección y la respuesta, **¿qué deben hacer, qué están haciendo, las organizaciones para asegurar estos objetivos?**

Para asegurar los objetivos de la ciberseguridad, las organizaciones deben realizar una evaluación de riesgos de sus activos de información que aborde las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Esto implica implementar medidas técnicas, políticas y procedimientos adecuados para proteger los sistemas y datos contra una variedad de amenazas.

- *Implementar medidas de redundancia y tolerancia a fallos en sus infraestructuras de TI, así como realizar copias de seguridad regulares y disponer de planes de continuidad del negocio para mitigar los efectos de posibles interrupciones.*
- *Asegurar la integridad de los datos mediante el uso de técnicas de cifrado, firmas digitales y controles de acceso adecuados.*
- *Asegurar la confidencialidad mediante el uso de cifrado, políticas de acceso basadas en roles y autenticación fuerte. Además, la implementación de soluciones de Data Loss Prevention (DLP) ayudan a detectar y bloquear fugas de información.*
- *Implementar controles de acceso robustos, como la autenticación multifactor y la gestión de identidades y accesos. También pueden utilizar tecnologías como las firmas y los certificados digitales para verificar la autenticidad de los datos y las comunicaciones.*
- *Implementar sistemas de registro y auditoría que registren las actividades de los usuarios y los cambios en los datos.*

Javier Burguera

- Los incidentes de seguridad (como ransomware, phishing, ingeniería social, fuga de información-shadow IT) **¿se prodigan por la rápida y constante adopción de las innovaciones tecnológicas?**

La rápida y constante adopción de innovaciones tecnológicas ha contribuido a la proliferación de incidentes de seguridad. A medida que las organizaciones adoptan nuevas tecnologías para mejorar la eficiencia, la productividad y la conectividad, también aumentan su superficie de ataque y su exposición a posibles vulnerabilidades y amenazas cibernéticas.

La seguridad no debe ser vista como un obstáculo para la adopción de tecnología, sino más bien como un habilitador al proteger activos críticos, fortalecer la confianza del cliente, facilitar la innovación segura y garantizar el cumplimiento normativo y legal.

- *Al garantizar la integridad, confidencialidad y disponibilidad de estos activos, la seguridad permite que las organizaciones operen de manera segura y continúen brindando servicios a sus clientes.*
- *Los consumidores esperan que las organizaciones protejan adecuadamente su información personal y financiera, y una violación de seguridad puede tener repercusiones graves en la reputación y la credibilidad de una organización.*
- *Al implementar controles de seguridad desde el principio del ciclo de vida del desarrollo de software, las organizaciones pueden reducir el riesgo de vulnerabilidades y mejorar la calidad y la seguridad de sus productos y servicios.*
- *Al cumplir con estas normativas, las organizaciones pueden evitar sanciones legales y financieras y mantener la confianza de los reguladores y las partes interesadas.*

Al integrar la seguridad en todos los procesos, las organizaciones pueden mitigar los riesgos y aprovechar al máximo las oportunidades que ofrecen las nuevas tecnologías.

Javier Burguera

Estamos interactuando constantemente con bancos, proveedores de bienes y servicios, con las AAPP; confiamos nuestra información y procesos en la “nube”; dependemos de un suministro constante de energía; …

- **¿Podemos confiar en sus sistemas informáticos? Nuestras operaciones habituales ¿están protegidas? Identificación, transacciones, pagos, cesión de datos, … ¿hay alternativas al corte de energía?**

Si bien ningún sistema es completamente infalible, existen medidas y regulaciones estrictas que buscan garantizar un nivel adecuado de protección de datos y seguridad cibernética en todos los sectores.

- *Las regulaciones de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea o leyes similares en otros países, imponen obligaciones a las organizaciones para proteger la privacidad y seguridad de la información personal de los individuos.*

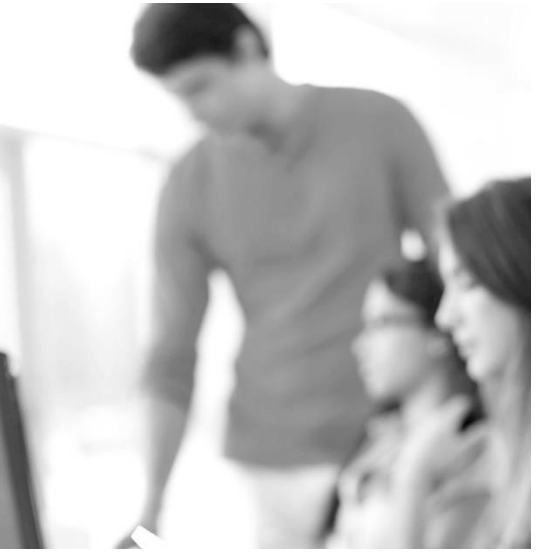
- *En el ámbito de la administración electrónica, existen regulaciones específicas como el ENS orientadas a garantizar un nivel adecuado de seguridad y confianza en los servicios digitales proporcionados por las administraciones públicas.*

Las organizaciones deben estar preparadas para gestionar y responder ante tales incidentes de manera efectiva, minimizando así su impacto en la seguridad y la continuidad del negocio.

En el sector público: la gestión (recaudación y gasto) de los recursos públicos es dependiente de los sistemas informáticos.

- **Las administraciones públicas, ¿tienen identificadas las debilidades, las amenazas y los riesgos de sus sistemas informáticos?**

INES (Informe del estado de la seguridad) es una solución desarrollada por el CCN (Centro criptológico nacional) para la gobernanza de la ciberseguridad, que permite evaluar regularmente el estado de la seguridad de los sistemas TIC de las entidades, organismos y organizaciones, además de su adecuación e implantación al Esquema Nacional de Seguridad (ENS) adaptándose a otros estándares o normas reguladoras en caso necesario.



- **¿En quién (institución) recae la responsabilidad de los sistemas informáticos de las AAPP?**

De acuerdo al artículo 11 del ENS se marca la diferenciación de responsabilidades de conflictos.

1. *En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.*
2. *La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.*
3. *La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución.*

- **¿De quién (institución) depende la protección de los sistemas informáticos de las AAPP?**

En primer lugar, del propio organismo. De forma adicional el CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Vanessa González

- **¿DICAT son también objeto de las administraciones públicas?**

El ENS establece categorías de seguridad de los sistemas de información.

> *1. La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:*
>
> *a) Alcanzar sus objetivos.*
>
> *b) Proteger los activos a su cargo.*
>
> *c) Garantizar la conformidad con el ordenamiento jurídico.*
>
> *2. A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad:*
>
> *a) Confidencialidad [C].*
> *b) Integridad [I].*
> *c) Trazabilidad [T].*
> *d) Autenticidad [A].*
> *e) Disponibilidad [D].*

- ***¿Qué pueden hacer, qué hacen las AAPP para alcanzar estos objetivos?***

Un primer paso sería adaptar sus sistemas al ENS incidiendo de forma particular en las medidas técnicas específicas para cada sistema.

Vanessa González

El Esquema Nacional de Seguridad (RD 311/2022, de 3 de mayo, por el que se regula el ENS) es una normativa que tiene por objetivo establecer la política de seguridad en la utilización de medios electrónicos relacionados con la administración pública, y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

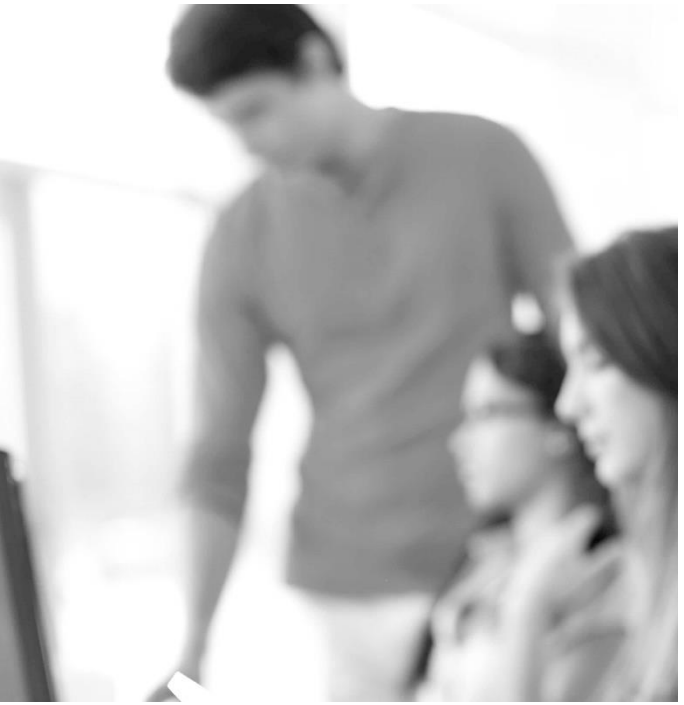
- **¿A quién afecta? y ¿cuál es su ámbito de aplicación?**

  - *Es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.*
  - *Será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.*
  - *También se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.*

- **¿Cuáles son los elementos principales del ENS?**

  - *Los principios básicos a considerar en las decisiones en materia de seguridad*
  - *Los requisitos mínimos que permitan una protección adecuada de la información*
  - *El mecanismo para lograr el cumplimiento de los principios básicos y de los requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger*
  - *El uso de infraestructuras y servicios comunes*
  - *Los perfiles de cumplimiento específicos*
  - *El informe de estado de la seguridad*
  - *La auditoría de la seguridad*
  - *La respuesta ante incidentes de seguridad*
  - *El uso de productos certificados*
  - *La conformidad*
  - *La formación y la concienciación*
  - *Las guías de seguridad*
  - *Las instrucciones técnicas de seguridad .*

Vanessa González



- **¿Qué aplicación tiene la categorización de los sistemas de información?**

Asignar una de las categorías (BAJA/MEDIA/ALTA), de forma que para cada control se apliquen las medidas específicas para ese nivel.

- **El cumplimiento del ENS ¿Qué supone? ¿garantiza el DICAT?**

Cada control del ENS afecta a una o varias dimensiones de seguridad con lo que el cumplimiento del control garantiza que estén cubiertas las dimensiones de seguridad afectadas.

El RD 311/2022, establece como un elemento principal la auditoría de seguridad que verifique el cumplimiento del ENS,

- **¿Corresponde a la IGAE? ¿Cómo afecta el ENS a las funciones de control interno y la auditoría pública de la IGAE?**

Naturalmente, no corresponde a la IGAE garantizar el cumplimiento del ENS en el resto de las organizaciones.
No obstante, sí se incluye el cumplimiento del ENS en aquellas auditorías cubiertas por el Equipo de Auditoría informática.