Un nuevo ecosistema de ciberseguridad para la transformación digital

Miles de empresas de todo el mundo tienen ante sí el reto de la transformación digital. La llamada Industria 4.0 requiere la conjunción de las tecnologías de operación (OT) e Internet de las Cosas (IoT). Hay nuevos riesgos y ciberamenazas y, por ello, se requieren nuevas herramientas de gestión. AENOR ha elaborado un nuevo ecosistema que pretende ser el aliado de los Chief Information Officer (CIO) porque atiende a las nuevas necesidades de ciberseguridad y privacidad.

Boris Delgado
Gerente TIC

Carlos Manuel Fernández
Asesor estratégico TI AENOR

La evolución y el vertiginoso desarrollo que las Tecnologías de la Información y Comunicaciones (TIC) han experimentado en los últimos 10 años es de una magnitud incuestionable. La Industria 4.0, o cuarta revolución industrial como ya se denomina por muchos, tiene su base precisamente sobre este desarrollo puesto que es la suma de las tecnologías de operación (OT) e Internet de las Cosas (IoT). Y es que la transformación digital está marcando el presente y futuro de muchas organizaciones, industrias y de la sociedad en su conjunto.

La generalización y el uso extensivo de la conectividad móvil, redes sociales, Big Data, etc. ha supuesto un despliegue de las tecnologías conocidas como SMAC (*Social-Mobility-Analytics-Cloud*) que, junto con el desarrollo de la mencionada Industria 4.0, implica nuevos riesgos y amenazas. Por ello, es fundamental dotar de ciberseguridad a las nuevas tecnologías implicadas en la transformación digital.

La ciberseguridad se podría definir como la seguridad en un mundo digital-virtual para prevenir los ciberataques cuyo origen está en nuevas amenazas y riesgos ya sea en entornos de gestión empresarial (SMAC) o en entornos industriales (OT).

Teniendo en cuenta este escenario y considerando el actual desarrollo del marco legal y regulatorio nacional y europeo junto con las normas internacionales ISO, AENOR ha diseñado un "Ecosistema de Ciberseguridad y Privacidad". Éste ofrece soluciones a los nuevos riesgos y amenazas a los que se enfrentan las organizaciones públicas o privadas a la hora de afrontar su transformación digital; utilizando como herramientas para conseguirlo la implantación y posterior certificación de estos referenciales (ver figura 1).

El ecosistema desarrollado por AENOR para la ciberseguridad y la privacidad, completamente compatible e integrable con el Modelo de Gobierno y Gestión de las TIC de AENOR, abarca las siguientes siete esferas.

1. Seguridad de la información. La certificación según la Norma ISO/IEC 27001 de sistemas de gestión de seguridad de la información ya se considera como una *commodity* para las organizaciones. Esta certificación es la base del ecosistema, ya que implanta la Ciberseguridad/Seguridad orientada a los procesos y objetivos del negocio. Se basa en el análisis de Riesgos de TIC considerando la confidencialidad, integridad y disponibilidad de los sistemas de información, aplicando los controles de las ISO/IEC 27002 y fundamentándose en la mejora continua.

Además, esta certificación puede complementarse con la ISO/IEC 27032 que añade elementos específicos de la ciberseguridad. Y es que contempla riesgos y amenazas propias de ciberseguridad como ataques de ingeniería social, basados en baja concienciación y formación en seguridad de los usuarios; el acceso no autorizado a sistemas informáticos (*Hacking*); o software malicioso de secuestro y cifrado de información (*Ransomware*). Además, propone controles específicos relacionados con la seguridad en el desarrollo de software (*security-by-design*), la seguridad en las configuraciones de los servidores y la concienciación en el usuario final, teniendo en cuenta la prevención y gestión de incidentes de seguridad. Aquí es importante el apoyo de los CERT (Computer Emergency Response Team), organizaciones públicas y privadas que disponen de expertos en seguridad que identifican amenazas y vulnerabilidades. En España, dos de los principales CERT son CCN-Centro Criptológico Nacional y el INCIBE-Instituto de Ciberseguridad de España, certificado éste por AENOR en ISO 27001 y Esquema Nacional de Seguridad, ISO 9001.

2. Ciberseguridad en *cloud* (seguridad y privacidad). Tomando como base el sistema de gestión de seguridad de la información que describe la ISO/IEC 27001 se pueden aplicar las extensiones de controles que propone para entornos *cloud* en cualquiera de sus modalidades (*IaaS-Infraestructure as a Service, PaaS-Platform as a Service SaaS-Software as a Service*), y obtener junto con la ISO 27001 un certificado de conformidad ISO/IEC 27017- ISO/IEC 27018 adicional.

El objetivo de la ISO/IEC 27017 *Code of practice for information security controls based-on ISO/IEC 27002 for Cloud Services* es la implementación de controles para organizaciones públicas o privadas que almacenan información en la nube. Basada en la ISO/IEC 27002, amplía con nuevos controles específicos (7 controles) y refuerza los ya existentes (37 controles) para las necesidades en seguridad de las organizaciones de la nube y sus usuarios finales.

Por su parte, la ISO/IEC 27018 *Code of Practice for Protection of Personally Identifiable Information (PII) in public clouds acting as PII processors* tiene por objetivo proteger la información de Identificación Personal (PII)-datos personales, almacenada o procesada en la nube pública. Orientada a los proveedores de la nube está alineada con los principios de privacidad de ISO/IEC 29100 y por tanto con el Reglamento General de Protección de Datos. Basada en la ISO/IEC 27002 amplía con nuevos controles específicos (25) y refuerza los ya existentes (16).

3. Esquema Nacional de Seguridad. El Real Decreto 3/2010 establece la política de seguridad en la utilización de medios electrónicos a través de principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Aplica a las administraciones públicas y a aquellas organizaciones privadas que proveen servicios o soluciones tecnológicas a las AA.PP.

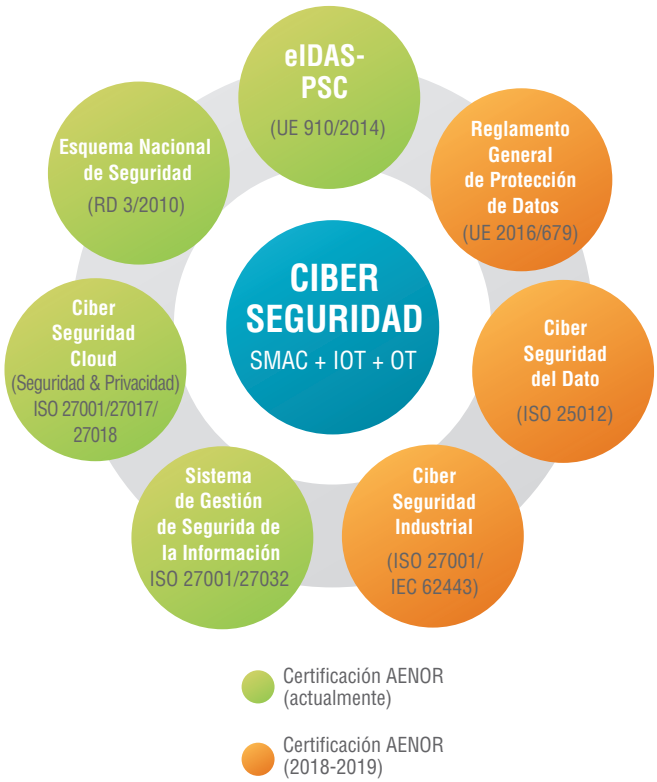
Así, las organizaciones que implantan el Esquema Nacional de Seguridad (ENS) deben implantar una serie de medidas (controles) de seguridad para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. AENOR, que tiene vigentes 26 certificados ENS, fue la primera entidad en ser acreditada por ENAC para esta certificación y actualmente es la única entidad acreditada para certificar ENS e ISO/IEC 27001.

4. Reglamento eIDAS-PSC (Prestadores de Servicios cualificados de Confianza) – UE 910/2014. El Reglamento de la UE 910/2014 relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior (eIDAS) tiene como objetivo establecer los criterios para los servicios de confianza. Igualmente, determina un marco jurídico para los servicios cualificados como firma electrónica, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web. AENOR es la primera entidad acreditada por ENAC para la certificación del Reglamento eIDAS en España.

5. Reglamento General de Protección de Datos (RGPD) - UE 2016/679. El Reglamento General de Protección de Datos (RGPD) UE 2016/679, de obligado cumplimiento a partir del próximo mes de mayo, establece un nuevo marco jurídico sobre la protección de los datos personales y sobre la libre circulación de los mismos. Su objetivo es ofrecer más control a los ciudadanos sobre su información personal en el entorno SMAC y la transformación digital, como ya citamos anteriormente.

Figura 1

Ecosistema de Ciberseguridad y Privacidad – AENOR



El Reglamento incluye varios aspectos que se tratan de forma similar en normas/estándares anteriores como la ISO 27001 o el ENS. Es el caso de la evaluación del impacto sobre la protección de datos (EIPD), es decir el análisis y la valoración de riesgos centrados en los datos personales, para establecer medidas (controles) que mitiguen los riesgos identificados. También incluye la notificación de incidentes de seguridad en los datos personales, ante la pérdida o acceso no autorizados a datos personales. Ésta se deberá documentar y notificar a la autoridad competente en un plazo limitado de tiempo.

6. Ciberseguridad del Dato. El dato, junto con las personas, es el activo principal en las organizaciones. Y para que un conjunto de datos (bases de datos, Big Data, Data Lake, u otros almacenes de datos) cumpla con las características relacionadas con la ciberseguridad, según las características de ISO/IEC 25012, es necesario que un laboratorio acreditado por ▶▶

EXPERIENCIAS

Un único entorno de gestión

Rafael Hernández
Responsable de Seguridad de Sistemas de Información
CEPSA

El Sistema de Gestión de Servicios y Seguridad de la Información de Cepsa, diseñado, implantado y evolucionado en los últimos diez años, nos ha permitido aplicar estándares de calidad y seguridad que son referencia en todo el mundo. Las certificaciones según las Normas ISO/IEC 20000 e ISO/IEC 27001 de AENOR, nos han permitido dar una respuesta ágil y adecuada a las necesidades de la organización, ante un entorno en cambio constante. También han ayudado a mejorar la eficiencia de los procesos de negocio, aportando soluciones tecnológicas adecuadas, con un mayor control de los costes. Asegurando la transparencia y el control en la gestión de los servicios, manteniendo los estándares de calidad adecuados tanto a las necesidades de los clientes como de los negocios, junto con una adaptación eficaz y ágil a una cultura colaborativa y de mejora continua.

Contar con un Sistema de Gestión de Seguridad de la Información nos garantiza que se cumplen unos niveles de seguridad adecuados y que, en el caso de que se produzcan incidentes o situaciones en las que la seguridad se pueda ver comprometida, éstas serán gestionadas de la manera más adecuada.

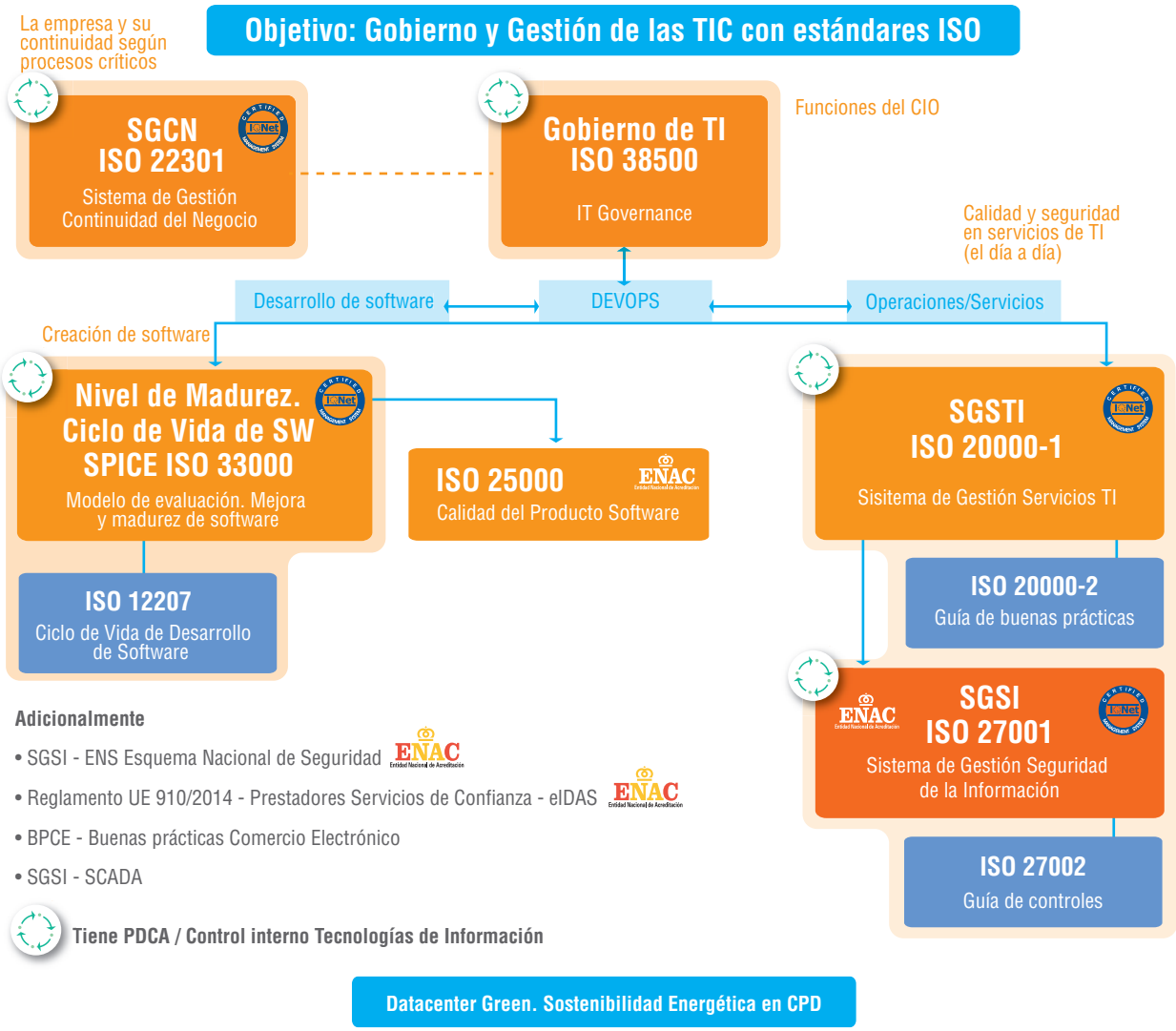
La adopción de estas normas nos ha permitido gestionar adecuadamente la información generada por los procesos de negocio; conocer y poder dar respuestas orientadas al cumplimiento de requisitos legales; cumplir con las exigencias de seguridad expresados por clientes, y tomar conciencia del valor de los activos de información.

La aparición de nuevos riesgos y ciberamenazas nos hicieron dar una vuelta de tuerca a nuestro SGSI, integrando ambas normas bajo un único entorno de gestión, y aplicando estos controles que la norma nos da a los nuevos riesgos de la ciberseguridad vinculados a la prestación de servicios tecnológicos.

Los análisis de riesgos y la definición de indicadores, que sean entendidos por los negocios, dan visibilidad a estas acciones y contribuyen a valorar aspectos que hasta el momento pasaban desapercibidos. Es el mecanismo natural de entendimiento con los responsables de riesgos de la organización y con nuestra Dirección.

Figura 2

Modelo Dinámico de Gobierno y Gestión de las TIC con ISO - AENOR



ENAC (como puede ser AQCLAB, laboratorio *partner* de AENOR) las evalúe, para posteriormente poder certificar la Calidad de los Datos.

Estas características que se deben evaluar son:

- **Conformidad:** grado en el que los datos cumplen estándares, convenciones o reglas similares relativas a la calidad en un contexto específico de uso.
- **Confidencialidad:** grado en el que los datos tienen atributos que aseguran que sólo pueden ser accedidos por usuarios autorizados en un contexto específico de uso.
- **Trazabilidad:** grado en el que los datos proporcionan registros de acceso a datos y sobre los cambios realizados en los datos, en un contexto específico de uso.
- **Disponibilidad:** grado en el que los datos pueden ser recuperados por usuarios o aplicaciones autorizadas, en un contexto específico de uso.
- **Recuperabilidad:** grado en el que los datos pueden tienen atributos que permiten un nivel de calidad, incluso en caso de fallos, en un contexto específico de uso.

7. Ciberseguridad Industrial. Los ciberataques a los sistemas industriales (centrales térmicas, fábricas de automóviles/textiles/alimentarias, laboratorios químicos/farmacéuticos, etc.) y concretamente a sus sistemas de control y supervisión de procesos (SCADA, por sus siglas en inglés), constituyen hoy día una amenaza real.

Tradicionalmente el control de los procesos industriales (OT) se realizaba mediante sistemas propietarios y aislados de los sistemas de información empresarial (TIC). Sin embargo en el momento actual ambos mundos comparten tecnologías de información, introduciendo numerosas amenazas, vulnerabilidades y riesgos de los sistemas de TIC a los sistemas OT.

En este escenario y tomando como base el sistema de gestión de seguridad de la información descrito en la

ISO/IEC 27001, y de acuerdo al análisis de riesgos sobre los procesos industriales, se aplican controles propios para estos entornos industriales como son la familia de normas ISA 99 o IEC 62443.

Modelo de Gobierno de las TIC y Ecosistema de Ciberseguridad & Privacidad

El Ecosistema de Ciberseguridad y Privacidad nace después de más de 10 años de implantación del Modelo de Gobierno y Gestión de las TIC de AENOR. Éste surgió como una solución pragmática para los CIO ante los riesgos para las áreas de Desarrollo y Operaciones de un Centro de Proceso de Datos (CPD), ya sea en modo *on-premise* (interno) o en *outsourcing* (externalizado). (ver figura 2)

Se diseñó como un modelo *bottom-up* (de abajo arriba) utilizando los estándares con sistema de gestión orientados a TIC basados en el ciclo de mejora continua (PDCA, por sus siglas en inglés). Éstos son:

- ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información (seguridad de la Información orientada a objetivos de negocio)
- ISO/IEC 20000–1–Sistema de Gestión de Servicios de TI (calidad y seguridad en los servicios de TI)
- SPICE-ISO 33000/12207 – Modelo de Madurez para los procesos de Ingeniería del Software (Calidad en el Desarrollo del Software)
- ISO 25000 – Requisitos y Evaluación de Calidad de Productos de Software (Calidad en el Producto Software)
- ISO 22301 – Sistema de Gestión de Continuidad de Negocio. (Continuidad y Resiliencia en los procesos y servicios críticos de la organización)

Y en la cumbre del Modelo se encuentra el estándar ISO 38500 - Buen Gobierno de TI, que se basa en la correcta implantación de los estándares anteriores y donde el CIO toma decisiones alineando el plan estratégico de TIC al plan estratégico de la organización, considerando los riesgos de TIC de la organización, IT Compliance y la Ciberseguridad.

Además, se incorporaron a esta legislación nacional certificable, el RD 3/2010 Esquema Nacional de Seguridad –de obligado cumplimiento para las AA.PP y proveedores privados para las AA.PP– o Reglamentos Europeos como es el UE 910/2014 Reglamento para los Prestadores de Servicios Cualificados de Confianza, de obligado cumplimiento para aquellas organizaciones que presten servicios cualificados de Firma Electrónica, Sello de Tiempo, etc.

El ecosistema de AENOR de Ciberseguridad y Privacidad descrito tiene como principio de diseño la certificación individual de cada sistema (esfera) y la posible integración de los diferentes sistemas (como un *pack* o *bundle* de certificaciones), aportando una solución única a múltiples necesidades de Ciberseguridad y Privacidad para las organizaciones.

Actualmente, AENOR tiene vigentes más de 600 certificados según las normas incluidas en el Modelo de Gobierno de las TIC. ◗