Alcance e implicaciones de la transformación digital

Ciberseguridad

Abril **2019**

DOCUMENTOS **CÍRCULO**

CÍRCULO DE EMPRESARIOS
ideas para crecer

Grupo de Trabajo de Transformación Digital

Desde el Círculo de Empresarios estamos elaborando una serie de documentos que faciliten el entendimiento e implicaciones de la transformación digital (TD), dirigidos fundamentalmente a las empresas, con un contenido didáctico y práctico, contando con respaldo académico/experto.

El presente documento centra su contenido en el impacto de la TD en la gestión de la ciberseguridad, aspecto cada vez más importante al estar las empresas necesariamente más expuestas tecnológicamente.

En la primera parte, se pretende describir brevemente el contexto actual de la ciberseguridad en las empresas, la gestión de las vulnerabilidades, la necesidad del cumplimiento normativo y la importancia de la sensibilización de los empleados y proveedores de servicios externos. A continuación, se describen las etapas y recomendaciones y consideraciones para construir un plan de director de ciberseguridad.

1. Decálogo: recomendaciones sobre ciberseguridad

ASPECTOS CLAVE

1. **No hay Transformación Digital sin ciberseguridad** por diseño y por defecto. Como consecuencia de la propia dinámica competitiva, las empresas tienden a incrementar sustancialmente los riesgos tecnológicos e incluso a trasladar determinados procesos a proveedores externos, lo que amplifica el riesgo en materia de seguridad.

2. **Aportación al negocio.** La inversión en seguridad de los entornos empresariales no tendrá un retorno directo, no va a incrementar el negocio por sí misma, pero sí que evitará perdidas económicas, derivadas de sanciones impuestas por el regulador, pérdidas directas o por disminución del valor de la marca por daño reputacional.

3. La ciberseguridad está íntimamente ligada al **cumplimiento normativo.** Las empresas tienen que cumplir con la regulación en el ámbito de la seguridad, con **especial atención a la protección de la privacidad de los usuarios.** No solo es de obligado cumplimiento, sino que son medidas necesarias para la correcta gestión de la información de sus usuarios y clientes, seguridad con terceros (proveedores) e interna con sus empleados.

4. **Organización y gobierno de la ciberseguridad.** Dado que cada empresa es única, la gestión de los riesgos de la ciberseguridad requiere de figuras como el Responsable de Seguridad de la Información (Chief Information Security Officer**-CISO-**) y un **marco de gobierno interno propio** y exclusivo de la organización, **integrado con la gestión corporativa de riesgos** que cubra aspectos tecnológicos, organizativos, operativos y financieros.

5. Convendría que toda empresa cuente con una **normativa interna** bien definida, actualizada que describa sus políticas, procedimientos internos **y buenas prácticas** en materia de seguridad. Sería recomendable que dicha normativa esté disponible tanto para sus empleados como para sus proveedores externos.

PLAN PARA LA GESTIÓN DE LA CIBERSEGURIDAD

6. Un plan de ciberseguridad se inicia con una **identificación** y **mitigación** de los riesgos tecnológicos inherentes a los procesos de negocio de la compañía y de las exigencias existentes en términos de cumplimiento. Existen diversos marcos de gestión de riesgos que se pueden tomar como referencia: NIST, ISACA, ISO 27001, etc.

7. Una organización tendría que contar con las **herramientas** necesarias para permitir detectar y responder a los ataques a través de la **monitorización y análisis** constante de la actividad y de desplegar las actividades necesarias para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto.

8. La gestión del riesgo tecnológico no debería focalizarse únicamente en la protección, también conviene hacerlo en la **resiliencia y continuidad de negocio** en caso de ataque cibernético exitoso, puesto que esta situación es probabilísticamente factible en un entorno en permanente cambio y amenaza.

9. Conviene **dotarse de las competencias adecuadas,** no solo a nivel de las áreas de **Tecnología,** sino en el ámbito de **control de riesgos** y de **asesoramiento a la Alta Dirección y a los Consejos de Administración.**

10. **La sensibilización y concienciación de los empleados y proveedores** en relación al papel que juegan en materia de seguridad de la organización, a través de la formación y la comunicación continua deberían de estar presentes en cualquier plan de gestión de la seguridad.

2. Entendimiento de la ciberseguridad

Los consejeros y altos directivos de las compañías han sido tradicionalmente conscientes del concepto de riesgo operacional y tecnológico. En efecto, por experiencia saben que un problema en la continuidad del servicio, en la seguridad de las plataformas tecnológicas o fuga de información crítica se puede traducir en pérdidas económicas directas por sanciones del regulador (podrían alcanzar el 4% del volumen de negocios anual mundial de la compañía en base a la norma RGPD[1]) e incluso una depreciación del valor de la compañía como consecuencia de un problema reputacional de la misma. En este sentido, ya existe una respuesta global de los gobiernos y de los propios reguladores, emitiendo políticas de seguridad de obligado cumplimiento.

Adicionalmente, la revolución tecnológica a la que se enfrentan las compañías está transformando su actividad e incrementando el perfil de riesgos tecnológicos asumidos, al ser gran parte de los procesos de la compañía susceptibles de digitalización, y al trasladar determinados procesos fuera de las puertas de la propia compañía.

Este hecho hace que los riesgos tecnológicos se conviertan en uno de los capítulos más importantes a la hora de gestionar el riesgo operacional de la compañía, lo que suele implicar inversiones relevantes y potenciar las tres líneas de defensa en la organización (habitualmente tecnología, riesgos y auditoría interna).

No obstante, se podría decir que la falta de presupuesto constituye en sí mismo otro de los agujeros de seguridad. Tradicionalmente se ha considerado a los Responsables de Seguridad de la Información (CISOs[2]) y a sus departamentos como especialistas técnicos con un alto grado de autogestión por lo específico de su función y sin un marco de *reporting* propio. Afortunadamente ha habido una evolución al respecto, en especial hacia la objetivación y demostración del saber hacer que han experimentado estos departamentos, y como consecuencia, se puede defender la petición de presupuestos en estas materias con argumentos más sólidos.

En cualquier caso, es imprescindible presentar planteamientos rigurosos basados en parámetros importantes para el negocio para conseguir la financiación. Toda la práctica de Seguridad Integral, incluso con leyes como la PIC[3] encima de la mesa, se tambalea si no se alinea con el negocio. El planteamiento de "se debe cumplir la Ley" es claramente insuficiente.

Esta situación, por muy trivial que parezca, sigue siendo una asignatura pendiente en muchas organizaciones. No obstante, se han dado pasos de gigante y los estándares de gestión de seguridad y similares han aportado herramientas bastante rigurosas en esta dirección.

Para ilustrar este hecho se pueden ver, por ejemplo, los estudios de Gartner que estiman en 96.000 millones de dólares el gasto mundial para 2018 dedicado a la ciberseguridad, lo que supone un 8% más que el año anterior.

1. Reglamento General de Protección de Datos en vigor desde mayo de 2018
2. Chief Information Security Officer
3. Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011)

Contexto actual

2.1 La ciberseguridad está en la calle

Después del ataque ocurrido el 12 de mayo de 2017 que se estima que encriptó los datos de 300.000 ordenadores en más de 150 países dejándolos totalmente inutilizados, se ha manifestado una "popularización" de la ciberseguridad. Los conceptos "ciberataque", *"ransomware"* o "parche" formaban parte de las conversaciones cotidianas, aunque solo fuera por unos días.

Esta situación, muchas veces criticada desde el ámbito más profesional, trae consigo efectos positivos, puesto que eleva el nivel de sensibilización de la población, algo bastante demandado durante muchos años. Conviene aprovechar el momento para poder elevar la ciberseguridad al lugar donde le corresponde: servir y proteger, ya sea a las organizaciones, a los países o a los particulares.

La labor de evangelización sigue siendo imprescindible. No solo se trata de ser excelente en la actividad que se realiza, también hay que demostrarlo y difundirlo.

2.2 Ataques sofisticados, que requieren respuestas sofisticadas

Las amenazas a las se enfrentan las empresas son bien conocidas, al igual que las motivaciones de quienes intentan materializarlas. Tampoco es novedosa la sofisticación con la que se orquestan y ejecutan ciertos ciberataques actuales pero sí llama la atención que, en general, la respuesta desde el "lado del bien" tiene recorridos de mejora. No se trata de responder atacando, más bien a la contención de los daños y recuperar la situación de normalidad, es decir, a la resiliencia.

En un escenario real las empresas deberían asumir que serán atacadas, ya sea de forma sofisticada o burda, y que probabilísticamente alguno de esos ataques será exitoso. Por lo tanto, parece razonable incrementar los esfuerzos para minimizar el impacto de los ataques. Es cierto que cuanto más sofisticado sea el ataque, más difícil será de detectar y cuanto más se tarde en detectar, la exposición al riesgo será mayor. Esto se puede mitigar utilizando inteligencia de ciberseguridad.

La Inteligencia requiere analizar una cantidad enorme de información, para lo que se utilizan las tecnologías de análisis predictivo depuradas adecuadamente dependiendo del contexto en el que se utilicen. Por ejemplo, en la lucha contra el fraude bancario se requiere definir y refinar algoritmos de análisis de comportamientos que se salen "de lo normal" para poder detectar y proteger intentos de fraude provocados por software malicioso.

2.3 Gestión de las vulnerabilidades, paso de gigante

Paradójicamente, el nivel de sofisticación de los ataques contrasta muchas veces con la simplicidad de ciertos métodos que se repiten constantemente.

Resulta curioso, a la vez que frustrante, constatar que muchos de los ciberataques más exitosos aprovechan vulnerabilidades conocidas desde hace años y fáciles de resolver empleando una dotación mínima de recursos. No obstante, también es cierto que existen ataques más masivos que emplean técnicas de ingeniería social, no tan sencillos de resolver

En el primer apartado del documento se habla en gran medida de la gestión del riesgo, entendiendo por riesgo la combinación de la probabilidad de que se materialice una amenaza junto con el impacto que provocaría, la gestión de las vulnerabilidades incide principalmente en la probabilidad, disminuyéndola de forma significativa y, por lo tanto, disminuyendo el riesgo.

Esto unido al hecho de que raro es el ciberataque que no hace uso de una vulnerabilidad no resuelta, se puede concluir que una gestión de vulnerabilidades profesional y bien articulada puede suponer un paso de gigante en la gestión de la seguridad en una organización, aunque también es cierto que en ocasiones prima la estabilidad de los sistemas sobre la resolución de la vulnerabilidad. La gestión de las vulnerabilidades es una práctica bien conocida por los departamentos de ciberseguridad de las organizaciones, se lleva haciendo muchos años y cada vez se refina más.

Los procedimientos de gestión de la seguridad se han estandarizado y se han generado metodologías cíclicas que se inician en una identificación de la vulnerabilidad para posteriormente corregirla y definir protocolos de monitorización, y recuperación de la situación en caso de ataque exitoso.

Por último, conviene recordar que siempre cabe la posibilidad de que una empresa sea víctima de un ciberataque, aunque se haya minimizado el impacto que provocaría en la organización. Por lo tanto, las medidas preventivas, como la gestión de vulnerabilidades, tendrían que complementarse con medidas de respuesta y de recuperación.

2.4 Concienciación y sensibilización

Lamentablemente, con bastante frecuencia las empresas tienden a creer que no van a ser una víctima de un ciberataque. Frases del estilo "a mí… ¿quién me va a atacar?", son frecuentes, especialmente en el sector industrial, donde la concienciación sobre los riesgos tecnológicos quizás es mejorable y las medidas efectivas de ciberprotección de estas compañías no suelen estar tan maduras como en otros sectores, sobre todo en las instalaciones y redes industriales.

Situaciones parecidas se han ido encontrando los responsables de ciberseguridad de las organizaciones a lo largo del tiempo: han tenido que sensibilizar y concienciar a su organización de los riesgos a los que están expuestos los activos corporativos (sobre todo los riesgos sobre la información) y cómo inculcar una cultura que equilibre la seguridad con la usabilidad.

No es una tarea fácil lograr una cultura de seguridad en una organización. Desde el ámbito de la ciberseguridad, se trabaja activamente en enfocarlo según grupos afectados de manera especial. Se muestran dos ejemplos:

- **Dirigido a Dirección o Gerencia.** El objetivo es instaurar una cultura de ciberseguridad a través del ejemplo. Se trata de que cada persona de la organización vea y aprenda comportamientos seguros de la persona inmediatamente superior en el organigrama. Adicionalmente es recomendable el uso de campañas de concienciación específicas basadas en los impactos en negocio y difusión de noticias relacionadas con la seguridad.

- **Dirigido a Departamentos Técnicos.** El objetivo es aumentar la involucración del personal altamente cualificado en materia de ciberseguridad, siempre y cuando las medidas tecnológicas de seguridad implantadas faciliten su labor del día a día (de lo contrario serán inútiles).

Toda la experiencia de la práctica de ciberseguridad alcanzada en los últimos años puede ser de aplicación también en los entornos industriales, con su necesaria particularización.

Incluso es factible aprovechar el impulso que está dando el negocio alrededor de las iniciativas denominadas "Industria 4.0", para poder incorporar la ciberseguridad desde el inicio de los planes de transformación y no a posteriori, cuando ya sería demasiado tarde.

La ciberseguridad conviene que sea un facilitador y adquiere especial protagonismo en tres actividades clave:

1. **Prevención,** garantizando la preparación ante las amenazas existentes;

2. **Contención,** minimizando al máximo el impacto de un ataque;

3. **Recuperación,** restableciendo la normalidad lo antes posible después de una contingencia sufrida.

2.5 Cumplimiento, en todos los frentes

Hoy día la actividad de ciberseguridad está íntimamente ligada al cumplimiento normativo. Convendría además que las organizaciones se dotaran de una normativa interna de ciberseguridad de obligado cumplimiento por parte de toda la compañía, a las que se añaden las leyes y regulaciones externas.

Además, a nivel personal, un Consejero Delegado (CEO por sus siglas en inglés) puede asumir responsabilidades directas por actuaciones negligentes o por falta de responsabilidad proactiva en materia de ciberseguridad. Por lo tanto, conviene tener un buen asesoramiento e incrementar las competencias en ciberseguridad y privacidad por parte del propio CEO.

En el caso de España se puede resaltar el Reglamento General de Protección de Datos (RGPD) o la Ley de Protección de Infraestructuras Críticas (LPIC), por mencionar algunas, y en algunos sectores aplica regulación específica, como las exigencias del Banco Central Europeo (BCE) en las entidades financieras, o el Esquema Nacional de Seguridad (ENS) en las Administraciones Públicas españolas.

Existe la postura, lamentablemente frecuente, de considerar la legislación en materia de ciberseguridad como algo muy complejo de acometer y con un impacto económico importante para la organización, lo que puede provocar una dinámica totalmente reactiva ante el cumplimiento, que se intenta solucionar una vez que se recibe una denuncia.

Este hecho está relacionado con una visión de la normativa que siempre lleva acarreado un régimen sancionador, en lugar de verlo como una oportunidad de mejora que, además, podría acarrear una sanción importante en términos económicos y reputacionales si no se lleva a cabo.

2.6 Mayor nivel de exigencia por parte de la demanda

Las organizaciones están demandando un incremento de la excelencia de prestación de servicios por parte de los proveedores en materia de seguridad.

Atrás quedaron los tiempos en los que la demanda de soluciones y servicios de ciberseguridad estaba basada en criterios tecnológicos, o promovida por el miedo o, simplemente, porque aseguraba un mayor nivel de protección presente y futuro.

A las ya de sobra conocidas razones de soporte y ayuda al negocio, que paradójicamente parece el eterno "debe", el momento actual exige firmeza a la hora de prepararse y hacer frente a las ciberamenazas que nos rodean. Varios factores contribuyen a este hecho, si bien se pueden destacar al menos tres como se comenta a continuación.

Por un lado, el enemigo está fuerte. La virulencia, la organización y la consistencia de sus ataques demuestran que los atacados deberían mejorar en los mismos parámetros. Si el ataque se prevé fuerte, conviene contar con contramedidas fuertes; si los atacantes están organizados y son capaces de orquestar adecuadamente un ataque sofisticado, así debe ser la colaboración en el lado de "los buenos"; si el lado del mal persiste en su empeño, las organizaciones no deberían bajar la guardia en ningún momento.

Por otro lado, el talento escasea ahora más que nunca debido al elevadísimo grado de especialización requerido, algo que se ha agudizado con el paso del tiempo. En el campo de la

ciberseguridad existe una sensación crónica de obsolescencia de conocimiento, que se puede resumir como "lo que era válido hace 5 años, quizá no lo sea ahora". Esto ha pasado siempre, pero en los momentos actuales se detecta una elevadísima exigencia que recae sobre los profesionales que, además de estar totalmente actualizados en conocimientos técnicos de una materia concreta, de conocer cada vez más los procesos de negocio que tienen que proteger y la normativa que deben cumplir, tienen que poder colaborar con equipos multidisciplinares y, además, ser capaces de cambiar la percepción existente de "que bloquean cualquier iniciativa por motivos de seguridad".

Y, por último, aunque en general se celebran las numerosas iniciativas que a nivel legislativo o regulatorio se están llevando a cabo, se constata la visión cortoplacista, una vez más, a la hora de cumplir con la legislación y no aprovechar la oportunidad de incremento del nivel de ciberseguridad interno que eso supone.

3. Plan

3.1 Introducción y *frameworks* de referencia

Según el INCIBE (Instituto Nacional de Ciberseguridad), un Plan Director de Seguridad *"consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial."* De esta definición se obtienen los principales conceptos base para la construcción de un plan:

- **"Definición y priorización de un conjunto de proyectos ".** El objetivo final no es solo definir los proyectos de ciberseguridad necesarios, sino que debe existir una priorización de los mismos.
- **"Objetivo de reducir los riesgos".** Todo plan de ciberseguridad y todas sus acciones posteriores deberían estar enfocadas a la gestión del riesgo.
- **"Hasta unos niveles aceptables".** Partiendo de la base que el riesgo nunca desaparece del todo.
- **"A partir de un análisis de la situación inicial".** Adaptando siempre el plan a la realidad particular de la organización y a su potencial mejora.

En la construcción de un plan director de seguridad se suele seguir una aproximación en fases aprovechando las numerosas metodologías de gestión de riesgos, estándares, buenas prácticas y textos legales existentes. A continuación se muestran algunos ejemplos de documentación de referencia.

- NIST. National Institute of Standards and Technology
- ISACA. Information Systems Audit and Control Association
- Familia ISO 31000: gestión de riesgos
- Familia ISO 27000: sistemas de gestión de seguridad de la información
- ENS: Esquema Nacional de Seguridad
- MAGERIT. Metodología de análisis y gestión de riesgos
- NERC CIP. North America Electric Reliability Corporation. Critical Infrastructure Protection
- PSO (Plan de Seguridad del Operador) y PPE (Plan de Protección Específico) según Ley PIC (Protección de Infraestructuras Críticas)

A modo de ejemplo se muestra una representación gráfica de uno de los marcos de referencias disponibles como es el de ISACA.

Representación gráfica metodología ISACA.

3.2 Elaboración del Plan

Una vez seleccionado un marco de referencia, la construcción de un plan de ciberseguridad podría distribuirse de forma genérica en las siguientes fases:

1. Análisis de requerimientos

El plan de seguridad, en aquellos sectores en los que aplique, debe cubrir los requerimientos demandados por los supervisores de cada industria, por lo que es importante recopilar dichas necesidades e incluirlas en el alcance del plan.

A su vez, es necesario realizar una identificación y análisis de los activos tecnológicos y proyectos existentes o en curso de manera centralizada para la obtención de requerimientos pasados en materia de riesgo tecnológico que tienen que ser parte del alcance del plan.

Por último se recomienda analizar las tendencias del mercado en el ámbito de la seguridad con especial foco en mejores prácticas y en empresas de referencia del sector.

2. Autoevaluación

Adicionalmente a los requerimientos obtenidos en la primera fase, es necesario un entendimiento de la situación actual e identificar los gaps existentes en materia de seguridad respecto al modelo aspiracional.

Para ello, la recomendación sería apoyarse en uno de los cuestionarios con los que cuentan los principales marcos de referencia comentados en el bloque anterior que permitirían cubrir todos los ámbitos de prevención, securización, respuesta, monitorización y gobierno.

Dicho cuestionario debería ser respondido tanto por cada uno de los responsables de área indicando los impactos asociados de negocio de cada evento e identificando cuáles

son sus activos críticos, como por sus departamentos de sistemas soporte, evaluando el riesgo inherente y mitigado tras la aplicación de las medidas de seguridad que están implantadas.

Una vez completado el cuestionario se habrán identificado los *gaps* respecto al modelo de gestión de seguridad que se desea implantar.

3. Priorización y definición de acciones mitigadoras

Cada uno de los *gaps* identificados en la fase anterior deberían ser priorizados en función del riesgo asociado y probabilidad de que éste suceda.

A partir de esta priorización será necesario definir una acción mitigadora para reducir el riesgo inherente y el esfuerzo asociado estimado e identificar dependencias si existieran en la elaboración del plan temporal.

En esta fase se recomienda la definición de indicadores de riesgo que permita medir la evolución y el éxito de la acción implementada y la monitorización durante el proceso de mejora continua.

4. Plan

Finalmente en esta última fase será necesario calendarizar las acciones definidas en la fase anterior en base a la priorización, dependencias y esfuerzo requerido. Con frecuencia este plan se suele denominar ISMP por sus siglas en inglés *(Information Security Management Plan)*.

En relación al equipo, de trabajo es importante considerar que este debe contar con las capacidades necesarias y experiencia en el ámbito de la seguridad tanto para dar respuesta al formulario, por la sensibilización de la criticidad del riesgo, como en la elaboración del plan y garantizar el éxito de la ejecución del mismo.

Esto en sí mismo puede ser un reto, ya que según estimaciones del *Center for Cyber Safety and Education*, se espera un déficit de 1,8 millones de profesionales de ciberseguridad para 2022 a nivel global. Por tanto, un elemento crítico del plan es precisamente dotarse de las capacidades adecuadas, bien sea de forma interna o apoyándose en especialistas externos.

3.3 Mejora continua

Se considera buena práctica adoptar una dinámica de mejora continua a la hora de elaborar un Plan Director de Seguridad. La propia naturaleza de los riesgos es cambiante, el plan debe ser capaz de actualizarse y mejorarse de forma natural, como puede apreciarse en la siguiente figura:

Plan de mejora continua
Fuente: elaboración propia.

1. **Alcance y priorización:** establecimiento de las prioridades estratégicas desde el punto de vista de negocio y regulatorio, identificando los entornos críticos y la tolerancia al riesgo.

2. **Orientación:** identificación de amenazas y vulnerabilidades de los sistemas.

3. **Identificación del perfil *As-Is:*** identificación del perfil de riesgo de la entidad y ubicación en la categoría del *framework*.

4. **Medición del riesgo:** análisis de la probabilidad de que se produzca un evento de ciberseguridad e impacto de los mismos. Permite objetivar el riesgo incurrido.

5. **Definición del perfil *To-Be:*** definición del perfil de riesgo *To-Be* en relación a la situación actual y a la medición realizada.

6. **Análisis de *Gaps:*** análisis de las diferencias entre el perfil *As-Is* y *To-Be* estableciendo una priorización en función de análisis coste-beneficio.

7. **Plan de implantación:** lanzamiento y monitorización de las acciones necesarias para dar cobertura al *Gap*.

3.4 Consideraciones particulares

3.4.1 Ciberseguridad aplicada a la Protección de Infraestructuras Críticas

En los últimos años existe el debate de la convergencia de dos mundos aparentemente separados, el de la "Seguridad Física" y el de la "Seguridad Lógica" o ciberseguridad. La Ley PIC[4] encara esta situación mediante un enfoque integral y se está comprobando que los Operadores Críticos están viendo esta imposición como una oportunidad de aprovechar lo mejor de ambos mundos.

La práctica de ciberseguridad ha alcanzado un nivel de madurez muy alto en los últimos años, a veces a marchas forzadas, a veces aprendiendo de errores significativos y a veces transformándose en un proceso como otros tantos dentro de una organización. Actualmente puede aportar mucho valor en los sectores críticos. A continuación se muestran algunos ejemplos en relación a este aporte de valor

3.4.2 El caso del código fuente en *Apps* o aplicaciones *web*

En este entorno se agudiza más si cabe la criticidad del descubrimiento y de la gestión de vulnerabilidades que en el entorno TIC tradicional.

Claramente es más difícil encontrarlas. Se necesita analizar no solo el código fuente, sino también su diseño, es decir, un análisis estático de la aplicación. Pero también se analiza la aplicación funcionando, viendo cómo se comporta. Además, las aplicaciones suelen necesitar otros componentes de base, como los servidores de aplicaciones o las máquinas virtuales, cuyo código no pertenece a la aplicación y que, lamentablemente, es un vector de entrada muy frecuente y, por lo tanto, otros componentes a añadir en el análisis exhaustivo de nuestra aplicación.

¿Y qué decir tiene de la gestión de las debilidades encontradas en la aplicación? Que la dificultad se incrementa sensiblemente, debido a que:

- Si la vulnerabilidad reside en programación insegura, se debe atajar en el propio código fuente, cuya gestión suele depender de empresas externas.

4. *Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011)*

- Si la vulnerabilidad reside en un componente de base, debe ser resuelto por el proveedor del componente a través de parches, pero los parches hay que instalarlos. Hay que decir que compañías como Microsoft, Apple, Adobe, Oracle, etc, son especialmente diligentes para anunciar vulnerabilidades y publicar parches, aunque también son los que más ataques sufren.

- Si todo lo anterior se dilata mucho en el tiempo, en el caso de aplicaciones *web* siempre está la posibilidad de implementar una solución WAF *(Web Application Firewall),* que exige normalmente la involucración de los departamentos de comunicaciones y de ciberseguridad.

Por lo tanto, en este entorno tanto el descubrimiento como la gestión de las vulnerabilidades resulta más complejo que en el TIC tradicional. Afortunadamente, existen probadas metodologías y herramientas para afrontar el reto de una manera sistemática, que requieren, una vez más, del talento especializado.

3.4.3 El caso de los Entornos Industriales

En este caso afecta a los Sistemas de Control Industrial y a las Redes OT *(Operational Technology).*

Harto complicada resulta la tarea del descubrimiento de vulnerabilidades en estos entornos. Existe una razón de peso: la disponibilidad de los Sistemas de Control Industrial y de las Redes OT debe ser máxima, absoluta, y todo aquello que perturbe la disponibilidad no se permitirá. Por lo tanto, si el descubrimiento de vulnerabilidades añade latencias, solo se permitirá en las paradas programadas de mantenimiento del entorno industrial, si fuera el caso. Así que en muchos casos hay que conformarse con análisis tipo "table-top".

Y en el caso de la gestión, también existen dificultades. Las actualizaciones de *software* base, como sistemas operativos u otros componentes plataformados, es prácticamente inviable por las razones de disponibilidad anteriormente expuestas. Además, la instalación de *software* de protección, como *antimalware* o *whitelisting,* siempre requiere de la aprobación del fabricante industrial del sistema, por lo que se adivina las situaciones de bloqueo más frecuentes.

Por lo tanto, en los entornos ndustriales de debe vivir con la asunción del riesgo que supone saber que ni se pueden descubrir las vulnerabilidades ni se pueden gestionar con la "facilidad" de los entornos TIC tradicionales.

No todo está perdido, ni mucho menos. De hecho se aplican medidas preventivas y paliativas basadas en las buenas prácticas y no como reacción a un fallo detectado. Por ejemplo, en los Centros de Control Industrial se suelen instalar los Sistemas de Supervisión del correcto funcionamiento del proceso industrial, lo que comúnmente conocemos como SCADAs. Los SCADAs se consideran aplicaciones críticas, por lo que no se permiten cambios del software de ningún tipo en aquellos servidores donde se encuentran instalados. En ese escenario, una actualización del sistema operativo del servidor con los últimos parches de seguridad resultaría inviable, pero se pueden realizar labores de revisión de configuraciones incorrectas, o limpieza de aplicaciones instaladas anteriormente, o la verificación de los permisos de acceso de todos y cada uno de los usuarios dados de alta, etc.

4. Bibliografía y referencias

CEOE (2018). Plan Digital 2025: La digitalización de la sociedad española.

Círculo de Empresarios (2018): Alcance e implicaciones de la transformación digital: principales ámbitos de actuación.

Círculo de Empresarios (2018): Alcance e implicaciones de la transformación digital: estrategia y movilización

Comisión Europea (2017). Europe's Digital Progress Report.

Comisión Europea (2018). Digital Economy and Society Index (DESI) 2018.

Gartner (2017). Press Releases: Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017.

INCIBE. Plan Director de Seguridad. Colección: Protege tu Empresa (https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad)

ENISA (European Union Agency for Network and Information Security). Listado de metodologías de análisis de riesgos: http://rm-inv.enisa.europa.eu/methods/

Center for Cyber Safety and Education (2017). Global Information Security Workforce Study.

NIST (National Institute of Standards and Technology). Cybersecurity framework: https://www.nist.gov/cyberframework

ISACA (Information Systems Audit and Control Association). https://www.isaca.org/

World Economic Forum (2017). Digital Transformation Initiative (DTI).

Marqués de Villamagna, 3 - 11ª Planta - 28001 Madrid
www.circulodeempresarios.org