

TENDENCIAS

Programa Integral de Ciberseguridad para Operadores Críticos

Se describe un proceso metodológico para la ordenación de las actuaciones en materia de Ciberseguridad (CS) de un Operador Crítico (OC), para cumplimiento de las directivas NIS de la Unión Europea relativas a PIC (Protección de Infraestructuras Críticas). Para ello, se ha considerado un modelo tradicionalmente militar. Concretamente, se ha adoptado la rueda C3I como el principal paradigma de un marco de ciberseguridad.

La rueda C3I subsume otros modelos reconocidos, como son el bucle OODA, el ciclo de Deming y el “Cybersecurity Framework” de NIST, y permite tomar decisiones en función de los riesgos para planificar la estrategia de CS de un OC.

El resultado es un Programa Integral de Ciberseguridad (PIC) para Protección de Infraestructuras Críticas (PIC) – PIC2 –. PIC2 es una matriz de 16 agrupaciones de procesos, proyectos o servicios concretos que definen completamente la política de actuación de un OC en materia de continuidad de negocio y protección de sus servicios esenciales e Infraestructuras Críticas.

Hace más de dos décadas que la Unión Europea (UE) comenzó a dar importancia a la CS y a la Protección de Infraestructuras Críticas (PIC). En 2006, se publicó el Programa para la protección de Infraestructuras críticas europeas (EPCIP) de la UE para energía, transporte y economía [1], que comienza con la frase “Desastres



Julio Rives

Jefe de Servicios de Seguridad de la Información en XAIVO

jrives@xaivo.com



Álvaro Rodríguez

Director Técnico en XAIVO

arsoler@xaivo.com

naturales, ataques terroristas y actividades criminales pueden afectar a las infraestructuras de energía críticas de las que dependen los europeos...”. Durante casi una década, los expertos europeos evaluaron los progresos conseguidos en los proyectos piloto EPCIP (por ejemplo, EUROCONTROL y GALILEO), y aconsejaron que el programa adoptara un enfoque más práctico en el futuro.

En el 2016 las instituciones de la UE llegaron a un acuerdo que se recoge en la “Directiva NIS” [2], Directiva de la UE 2016/1148 del Parlamento Europeo y del Consejo el 6 de Julio de 2016, donde se hace referencia a las medidas comunes de gran nivel de seguridad de redes y sistemas de información. Bajo la Directiva NIS, las organizaciones que trabajan en sectores críticos como salud, energía y transporte, así como grandes proveedores TIC (Tecnologías de la Información y las Comunicaciones), están llamadas a implementar requisitos de seguridad y notificación. En breve se convertirá en algo obligatorio. Además, puesto que NIS es una ley de mínimos, se insta a los Estados Miembros a tomar medidas adicionales de CS. De hecho, algunos Estados Miembros, en el papel de estados fronterizos destacados, como España, deberían promover leyes de seguridad más exigentes que otros.

Dejando al margen este marco normativo, un OC no puede obviar el creciente clima de amenazas y la necesidad de tomar la iniciativa. Por ejemplo, no es remota la posibilidad de un ataque informático al sistema de control de una instalación química, produciendo pérdida de vidas, así como la degradación del medioambiente y otros daños físicos. Además, la complejidad de la amenaza crece, dada la relación de dependencia entre infraestructuras críticas que dan lugar a problemas en servicios o sectores adláteres, generando un efecto cascada catastrófico.

Sin recurrir al dramatismo de un ataque terrorista, recientemente se han producido ataques por motivos

económicos de alcance mundial, con desastrosas consecuencias en relación a la prestación de servicios esenciales para la ciudadanía, reputación de muchas empresas, y a la productividad del tejido industrial en general.

En las siguientes secciones se describe una estructura de actuaciones (iniciativas PIC) para que un OC pueda cumplir con la Directiva NIS, anticipándose a la trasposición nacional de la ley. Este propósito se ha abordado desde una perspectiva militar, como si se tratase de una campaña de las fuerzas armadas. Específicamente, se ha considerado la clásica rueda C3I [3] (*C3I wheel*) como el paradigma de un plan estratégico de CS.

Aproximación metodológica

Para proteger eficientemente a los países frente al terrorismo, los militares tuvieron que asimilar el uso de nuevas tecnologías en muy poco tiempo. Si bien, por un lado, esto significó un avance en la competencia y disposición

para la defensa, por otro los ciberataques surgieron como un nuevo paradigma de amenaza. En línea con esta tendencia, los militares han incorporado con éxito a su actividad general técnicas de Ciberdefensa.

La CS no es nada más que Mando y Control contemporáneo. En el plano táctico y operacional, las tecnologías de CS no sólo son cruciales para evitar ciberataques, sino que pueden ayudar a recuperarnos de un accidente y prevenir incidentes potenciales. En el plano estratégico, un planteamiento militar especializado en la protección de infraestructuras críticas sienta las bases para la intervención ordenada e integral destinada a maximizar los resultados de protección y operación sin costuras.

Es por ello por lo que se ha adoptado C3I como el arquetipo que soporta una estrategia de CS. Es lo suficientemente genérico como para contener otros modelos similares como el bucle OODA (observación, orientación, decisión, y acción) [4], lo suficientemente simple como para alojar funcionalidad específica, y lo suficientemente pragmático para que se traduzca en un conjunto de requisitos precisos de CS. Dicho modelo contempla las siguientes categorías de procesos:

- **Control:** Visualización y supervisión del estado operativo actual.

En esta dimensión espacial se estudia cómo están las cosas, recopilando información extraída de sistemas de captación de datos y reportes del escalón más operativo. Esta información facilita el entendimiento de la situación, la adopción de medidas cautelares en su caso, y la preparación del curso de acción. En pocas palabras, *control* significa recopilar, compilar y canalizar.

- **Construcción:** Decisión sobre qué hacer y cómo para llegar de la situación actual al estado objetivo marcado por *Control*.

Es un espacio de deliberación, diseño y desarrollo de posibles implementaciones del curso de acción seleccionado. Se administran, operan, protegen y refuerzan los elementos de la dimensión de control, los llamados “controles”. Además, en base a constricciones de la situación, se desarrolla un programa de medidas óptimas y tareas estructuradas como planes de reacción, respuesta o recuperación, que son notificados a las partes implicadas. En resumen, *construcción* es componer, coordinar y comunicar.

- **Comando:** Dirigir a la organización para que consiga su objetivo con rendimiento óptimo.



Aunque la ejecución debe estar planificada al máximo, con frecuencia requiere improvisación, refinamiento, o información adicional. Actividades habituales de esta categoría son la reorganización de recursos, la reasignación de tareas del personal (tasking) y la reacción ante situaciones cambiantes. Asimismo, la ejecución requiere hacer un meticuloso seguimiento de los planes, incluyendo la ejecución de las órdenes emitidas y la evolución de las operaciones. Por ello, *comando* es sinónimo de conformar, corregir y conducir.

Estas tres categorías interactúan entre sí: tareas de observación, análisis, decisión y acción se repiten, son recurrentes y cíclicas.

Además de éstas, el lector probablemente echa en falta una categoría globalizadora, imbricada con las anteriores. Corresponde a la "I" del acrónimo C3I, que trata de interoperabilidad, integración, identificación o inteligencia:

- **Inteligencia:** Adquisición de conocimiento situacional, y evaluación de riesgos y de resultados de los cursos de acción para dirección de toda operación.

Implica un análisis en profundidad del grado, presente y deseado, de protección de infraestructuras críticas y de garantía de la continuidad de negocio. El resultado sirve para orientar a los responsables de las categorías de control, construcción y comando, normalmente a través de notificaciones formales, políticas y normativas.

Inteligencia es un proceso sin fin que mide la eficiencia y efectividad de las medidas tomadas desde la perspectiva corporativa, y obtiene indicadores concluyen-

tes. Específicamente, la inteligencia es el nexo entre el curso de acción de ciberseguridad y el negocio, y, por tanto, aporta el análisis y la decisión sobre CS al más alto nivel.

Esta visión militar es consonante con planteamientos, normas y estrategias comunes publicadas en la literatura especializada como, por ejemplo, la ISO/IEC-27001:2014 que incorpora el ciclo de Deming (Planificar-Hacer-Verificar-Actuar) en base a un ISMS (Information Security Management System). Igualmente, el modelo iterativo de identificar-protector-detectar-reaccionar definido en CSF [5] y similares pueden considerarse submodelos de C3I.

Adicionalmente a las categorías C3I (dimensión espacial), a la hora de estructurar actuaciones CS, se considera necesario añadir una nueva dimensión, la temporal, que indica un plazo de inspección o acción: pasado o **preparación**, presente o **comprensión**, corto y medio plazo o **intervención**, y largo plazo o **prevención**.

Ciberseguridad PIC²

PIC² es el resultado de acomodar todas las actuaciones CS (procesos, proyectos o servicios), con una visión integral, en una categoría C3I y en otra de plazo de acción, conformando así una matriz 4x4 de procesos CS. Por ejemplo, si escogemos la columna de Inteligencia: en el pasado reciente (preparación) es necesario llevar a cabo una gestión de la configuración TI; si enfocamos al presente (Comprensión), lo esencial es la valoración de amenazas y la determinación de estrategias y planes de tratamiento de riesgos; en el futuro próximo (Intervención) es necesario ir relacionando la CS con las necesidades cambiantes del negocio y de la legislación; por último, a largo

		EJE ESPACIAL			
		INTELIGENCIA	CONTROL	CONSTRUCCIÓN	COMANDO
EJE TEMPORAL	PREPARACIÓN	GESTIÓN DE LA CONFIGURACIÓN TI	ADMINISTRACIÓN DE CONTROLES DETECTIVOS DE ANOMALÍAS	ADMINISTRACIÓN DE CONTROLES PROTECTORIOS DE INFORMACIÓN	CONSCIENCIA DE CRISIS
	COMPRENSIÓN	GESTIÓN DE RIESGOS	DETECCIÓN DE ANOMALÍAS	CONCIENCIACIÓN EN PROTECCIÓN Y CONTINUIDAD	GESTIÓN DE EMERGENCIAS Y CONTINGENCIAS
	INTERVENCIÓN	INTEGRACIÓN CIBERSEGURIDAD - NEGOCIO	CONTROL DE ACCESOS	IMPLANTACIÓN Y MANTENIMIENTO DE TECNOLOGÍA PROTECTORIA	GESTIÓN DE LA RESPUESTA A INCIDENTES
	PREVENCIÓN	GOBERNANZA DE LA CIBERSEGURIDAD	VIGILANCIA PERMANENTE	CULTURA DE PREVENCIÓN	GESTIÓN DE LA RECUPERACIÓN

Figura 1. La matriz espacio - temporal PIC2 de actuaciones CS.

plazo (Prevención) hay que establecer los instrumentos de gobernanza de la CS, tales como organización, marco normativo específico y canales de coordinación PIC.

Se presentan a continuación, muy resumidamente, los objetivos para cada una de las actuaciones CS de la matriz.

Gestión de la Configuración TI: Se identifican, clasifican y categorizan datos, información, conocimiento, dispositivos, software y sistemas, y se relaciona la importancia de estos con los objetivos de negocio o de protección de servicios esenciales.

- ▶ **Gestión de riesgos:** Se valoran las vulnerabilidades, se tipifican las amenazas, se examinan los riesgos que afectan a empleados, activos y operaciones, se determinan y usan las prioridades, restricciones, niveles de tolerancia de riesgo y normativa vigente para soportar decisiones de riesgo operacional, y finalmente se decide qué riesgos deben mitigarse, aceptarse, tolerarse o transferirse.
- ▶ **Integración CS – Negocio:** Se revisa el contexto del OC, y se analizan, priorizan y resumen los objetivos de CS desde la perspectiva de protección de servicios esenciales o infraestructuras críticas y de continuidad de negocio. Se identifican y estructuran jerárquicamente los servicios, procesos y activos críticos para el negocio y para la prestación de servicios esenciales, y se llevan a cabo análisis de impacto como consecuencia de una indisponibilidad o un escenario de accidente o ataque a una Infraestructura Crítica.
- ▶ **Gobernanza de la CS:** Se define y mantiene un marco regulatorio (política y normativa de seguridad), se establece una organización específica para CS, se realiza la comunicación y coordinación con otros actores PIC y se establecen los requisitos legales o regulatorios en materia CS (y se vigila su cumplimiento).
- ▶ **Administración de controles detectivos de anomalías:** Se definen, mantienen y prueban controles de detección que sirvan para reconocer rápida y adecuadamente eventos potencialmente anómalos de cualquier tipo. Se determinan los umbrales de alerta y se analiza el posible impacto de una actividad anómala.
- ▶ **Detección de anomalías:** Se implantan y utilizan controles para detectar actividad anómala en tiempo real, o en el pasado reciente. Tras una detección, las posibles amenazas se evalúan, se confirman y se notifican, y finalmente se refina el control.
- ▶ **Control de accesos:** Se definen privilegios y permisos dependiendo de roles, tipos de acceso (interno o ex-



terno, o por dominios de seguridad) y personas, y se gestiona la limitación del acceso a procesos y dependencias (y activos asociados) a aquellos usuarios que estrictamente lo requieran.

- ▶ **Vigilancia permanente:** Los activos son controlados por monitorización automática en la medida de lo posible, y a intervalos discretos en función del perfil de las amenazas, a fin de identificar posibles incidentes y verificar la eficiencia de las medidas de detección de anomalías y control de acceso. Los registros de vulnerabilidades y los niveles de protección de dichos activos se actualizan periódicamente, así como cualquier otra información necesaria para la Gestión de la Configuración TI.
- ▶ **Administración de controles protectorios de información:** En consonancia con la estrategia de riesgo de la organización, se planifica la protección de datos y documentación a fin de asegurar la confidencialidad, integridad y disponibilidad de la información. También se aplican políticas y procedimientos sobre objetivos operacionales, responsabilidades, compromisos de gestión y conductos de comunicación que permitan proteger los activos y sistemas de información.
- ▶ **Concienciación en protección y continuidad:** Se infunde concienciación sobre CS, protección y continuidad de negocio a empleados y otras partes interesadas, y se completa con un adecuado entrenamiento para que puedan llevar a cabo sus obligaciones en cuanto a seguridad en función de su responsabilidad y en relación a las políticas y acuerdos vigentes.

- ▶ **Implantación y mantenimiento en tecnología protectoria:** Se manejan soluciones técnicas de seguridad para reforzar el aguante y la resiliencia de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos vigentes. Se realiza asimismo mantenimiento y reparaciones de componentes de sistemas industriales, logísticos y tecnológicos en comunión con la gobernanza de CS.
- ▶ **Cultura de prevención:** Se re/definen planes de respuesta y recuperación ante incidentes de seguridad y se llevan a cabo simulacros de accidentes o ataques. Se diseminan los resultados de la ejecución de planes, se revisa la eficiencia de las políticas de protección y se comparte la experiencia.
- ▶ **Consciencia de crisis:** Desde las perspectivas de protección de servicios esenciales y de continuidad de negocio, se realizan estudios holísticos y profundos de las posibles situaciones de crisis o combinaciones de riesgos materializados, así como de las posibles respuestas y tareas de recuperación ante dichas situaciones.
- ▶ **Gestión de emergencias y contingencias:** Se ejecutan (y mantienen) planes de reacción ante situaciones de crisis para contener la expansión de sus efectos, y mitigarlos o suprimirlos.
- ▶ **Gestión de la respuesta a incidentes:** Se ejecutan (y mantienen) planes de respuesta ante la detección de un incidente de seguridad. Después, se evalúa la respuesta dada en cuanto a su rendimiento y, en comparación con el archivo histórico, se revisan las vulnerabilidades y se documentan las lecciones aprendidas.
- ▶ **Gestión de la recuperación:** Se ejecutan (y mantienen) los planes de recuperación para asegurar la puntual restauración de los sistemas o activos afectados por incidentes de seguridad.

Implantación de PIC²

La implantación del marco integral PIC² para un OC específico debe ordenarse cronológicamente. Por ejemplo, la Administración de controles protectorios precisa en gran medida de la Gestión de la Configuración TI, y la Administración de controles detectivos debería preceder a la Detección de anomalías. Además, dichas actuaciones deben priorizarse dependiendo de las circunstancias del OC según el grado de integración o nivel de asimilación de la CS a alcanzar.

Un PIC² requiere factorizar cada una de las 16 actuaciones en varios proyectos o servicios concretos. El orden cronológico de estos se puede establecer a partir de la estimación del índice de Necesidad (la importancia de que se realice un proyecto o servicio desde la perspectiva de la protección de servicios esenciales y sus infraestructuras críticas o de la continuidad de negocio) y de Éxito esperado (una medida de hasta qué punto la realización de dicho proyecto o servicio, dadas las circunstancias actuales del OC, está exento de riesgos integrales desde el punto de vista de ejecución de proyectos). También es necesario considerar restricciones de Prelación temporal, que obligan o recomiendan alcanzar un nivel de madurez determinado en una actividad para iniciar otra. Por supuesto un último criterio a considerar para la planificación de la implantación de PIC² es la Inversión necesaria para cada proyecto o servicio.

Referencias

1. "Communication COM/2006/0786 from the European Commission"; Official Journal of the European Union - 52006DC0786; 12 Dec 2006.
2. "Directive EU 2016/1148 of the European Parliament and of the Council"; Official Journal of the European Union - 32016L1148; 6 Jul 2016.
3. Y.A.J.R. van de Vijver and J.G. Stil; "A road map to the NATO virtual enterprise"; NLR-TP-2001-198; 2001.
4. Frans Osinga; "Science Strategy and War, The Strategic Theory of John Boyd"; Abingdon, UK: Routledge -ISBN 0-415-37103-1; 6 Dec 2006.
5. NIST (National Institute of Standards and Technology); "Framework for Improving Critical Infrastructure Cybersecurity v1.0"; 12 Feb 2016.

Cibersecurity of a Critical Operator

A methodological process is described to order the action issues for the Cibersecurity of a Critical Operator, to ensure the compliance of the NIS directives of the European Union related to CIP (Critical Infrastructure Protection). For this matter a traditional military model is being considered. In particular, we

have adopted the CI3 wheel as the main paradigm for the cybersecurity framework.

The CI3 wheel subsumes similar models such as the OODA loop, the Deming cycle, and the Cybersecurity Framework, and enables risk-based decision making to plan the Critical Operator's cybersecurity strategy.

The result is a Cybersecurity Integral

Program (CIP) for Critical Infrastructure Protection (CIP) – CIP2 –.

CIP2 is a matrix of 16 specific groups of specific processes, projects or services that completely define the policy of a Critical Operator in terms of business continuity and protection of its essential services and Critical Infrastructures.