El impacto en el CISO y el DPO de las notificaciones de incidentes

El marco regulatorio del tratamiento de datos personales y de prestación de servicios esenciales en la UE, va a consagrar, cada uno en su universo competencial, la notificación de incidentes de seguridad. Cuando se detecten deberán ser considerados como presuntos delitos si se ajustan a lo tipificado en la legislación penal. Además, pueden llevar aparejada la exposición, pérdida o sustracción de datos de carácter personal. Esta doble circunstancia va a tener consecuencias relevantes en la delimitación de funciones y competencias en la gestión (y, por tanto, en la notificación) de incidentes entre el CISO, el DPO, e incluso el Responsable de Enlace cuando se trate de un operador designado de infraestructura crítica.

Manuel Carpio Cámara

Descripción del problema inmediato

Ha querido el destino que en el intervalo de unas pocas semanas hayamos podido ver una conjunción astral de primera magnitud en el ya abigarrado universo regulatorio europeo: el Reglamento de Protección de Datos (GDPR) y la Directiva para la Seguridad de la Información y de las Redes (NIS).

Entre otras obligaciones, ambas regulaciones exigen la notificación de los incidentes de seguridad en el ámbito de las tecnologías de la información y las comunicaciones (TIC) que sufran los sujetos sometidos a la jurisdicción europea.

Como es habitual con estas novedades legislativas, el nivel de abstracción del texto original, las posibles incongruencias con otras regulaciones, así como el miedo a lo desconocido de sus consecuencias, dejan mucho margen a la interpretación, al tiempo que hacen crecer el desasosiego y esparcen la confusión en el sector.

¿Qué se pretende con las notificaciones?

En la exposición de motivos de la directiva NIS se justifica la notificación "para promover la cultura de la gestión de riesgos y asegurarse de que los incidentes más serios son reportados". Sin embargo, en la misma sección pero del GDPR se reconoce que una obligación genérica de declaración de brechas, no solo no ayudaría a la protección de datos, sino que supondría una carga administrativa y financiera para el "controlador". Por ello, limita la notificación solo a aquellos incidentes en los que peligren los derechos y libertades de los individuos o en los que el controlador no haya hecho previamente un análisis de impacto.

Es cierto que necesitamos compartir información acerca del origen de los incidentes, las amenazas y las vulnerabilidades que explotan, con el fin de preparar y coordinar nuestras defensas. Necesitamos también evaluar la magnitud real de sus consecuencias, cuantificar las pérdidas y favorecer su aseguramiento, hasta el punto en el que ojalá los actuarios pudieran llegar algún día a familiarizarse con este tipo de "siniestros", aquilatando sus primas y coberturas.

Necesitamos compartir información acerca del origen de los incidentes, las amenazas y las vulnerabilidades que explotan, con el fin de preparar y coordinar nuestras defensas; y también evaluar la magnitud real de sus consecuencias, cuantificar las pérdidas y favorecer su aseguramiento, hasta el punto en el que ojalá los actuarios pudieran llegar algún día a familiarizarse con este tipo de "siniestros", aquilatando sus primas y coberturas.

No obstante, existe aún renuencia a declarar voluntariamente los incidentes por evitar una imagen negligente y vergonzante frente a clientes u otras partes interesadas, o por miedo a sanciones del regulador. Para más detalle, remitimos a nuestro distinguido lector al informe que sobre este particular ha publicado recientemente la fundación ESYS (1).

¿Realmente hacía falta regular esto?

Hay tres enfoques diferentes para compartir información sobre incidentes de seguridad: 1) la regulación tradicional; 2) formas alternativas de regulación, tales como auto y co-regulación; 3) sistemas cooperativos de intercambio voluntario.

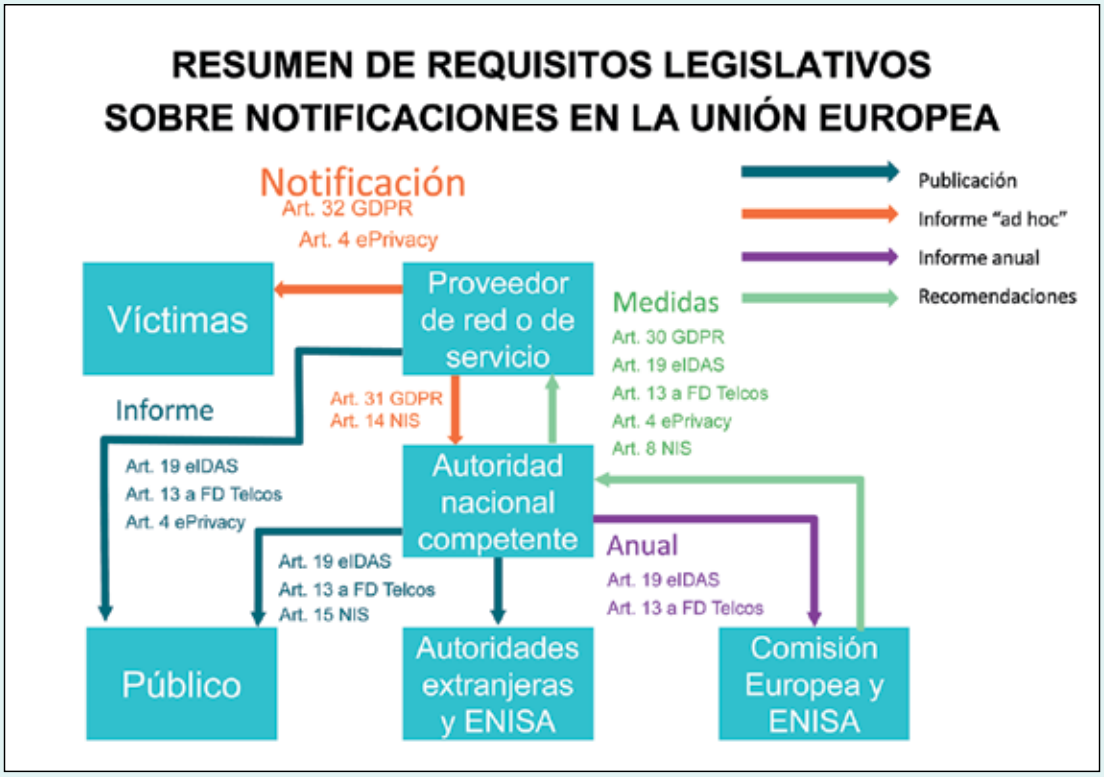
A pesar del creciente número de iniciativas nacionales para crear un marco legal que obligue a compartir información sobre incidentes, los enfoques cooperativos y de autorregulación son los más utilizados en los países de la UE (2) hasta el momento. Pero la ausencia del regulador en un grupo donde se comparte información no siempre es sinónimo de armonía y eficacia. Los principales retos para otras formas de compartición alternativas a la regulación son:

- Vacilación para compartir con terceros, cuando no se controlan las condiciones de acceso al grupo, y la supervisión de sus miembros es débil.
- Falta de mecanismos aceptados por la comunidad para hacer cumplir las reglas de sindicación de información.
- No se ven claros ni el beneficio propio ni otros aspectos positivos

para la comunidad por el mero hecho de intercambiar información.

• Visión parcial de lo que sucede en el sector, ya que a veces, las "partes interesadas" que participan en el grupo no son las "interesantes", las cuales no participan.

Y aun así, podríamos mencionar docenas de foros promovidos por y para el sector privado, tanto a nivel global (p.e. FIRST, FS-ISAC), europeo (p.e. ETIS, TNCEIP), o español (CCI, GTS), en los que sus miembros intercambian información acerca de incidentes desde hace ya muchos años.



Muchos de los operadores de servicios esenciales no tendrán que esperar hasta el verano del 2018 para comenzar a notificar por vía de la Directiva NIS, sino que lo harán mucho antes, por un atajo, por la vía de la Ley de Infraestructuras Críticas.

Un poco de historia con las notificaciones

El año 2002 marca el inicio de la obligación explícita de declarar los incidentes. Fue el senado californiano quien abrió el fuego con su Ley 1386, la cual en sus aspectos básicos ha sido secundada hasta hoy día, tanto por el regulador norteamericano como el europeo, en materia de protección de datos de carácter personal. La notificación había que hacerla individualmente a los sujetos afectados, y si esto resultaba muy caro, o no se sabía con certeza quiénes eran, se les debía avisar a través de los medios de comunicación pública.

En 2009 el Parlamento Europeo enmienda la Directiva "ePrivacy", dirigida a desarrollar ciertos aspectos de la protección de datos en el sector de las telecomunicaciones. Entre otros, se menciona el asunto de la notificación (3). Este "gancho" legislativo sirvió más tarde, en 2013, para "colgar" el Reglamento 611, donde ya aparecen rampantes los detalles del procedimiento y del contenido de la notificación, tanto a la Autoridad Competente como, en su caso, a los individuos afectados.

Curiosamente, unos meses antes, el Departamento de Salud y Servicios Sociales de los EE.UU. había publicado un reglamento similar para la notificación de brechas de seguridad de datos bajo la Ley HIPAA. Se observan algunas diferencias no obstante entre ambas regulaciones; así en el caso norteamericano se da un plazo de 60 días para la notificación, mientras que en el europeo se urge a hacerlo antes de las 24 horas desde que se tuviera conocimiento.

Sin abandonar el sector de los prestadores de servicios de comunicaciones nos desplazamos ahora a otro ámbito competencial: el de la calidad del servicio. La Directiva Marco de Telecomunicaciones del año 2009, en su Art. 13, también había dejado otro cimiento legislativo sobre el que las Autoridades Nacionales pudieran edificar posteriormente una reglamentación de notificación de disrupciones de los servicios básicos, utilizando como guía las recomendaciones de ENISA (4).

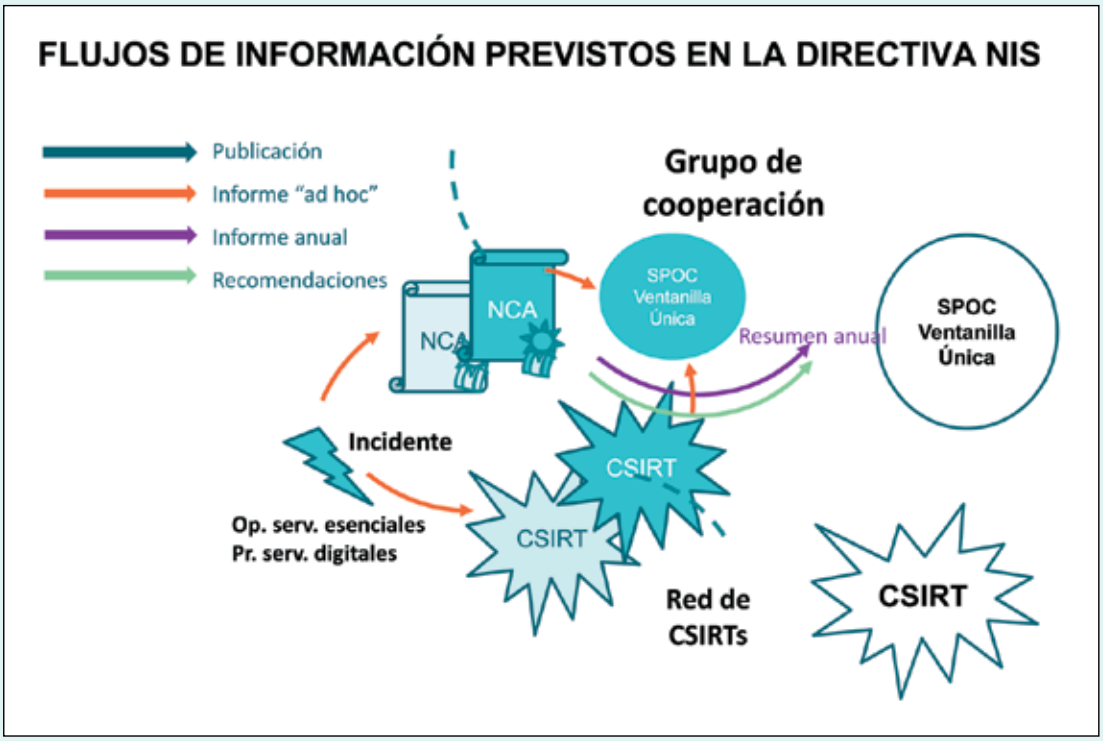
Otro sector de especial cariño en cuanto a la regulación notificadora es el financiero. En 2005 la Federal Deposit Insurance Corporation (FDIC) norteamericana publicó una guía no vinculante para que las entidades financieras establecieran un programa de respuesta a incidentes, uno de cuyos procedimientos debía ser la notificación a los clientes. Más tarde, en 2011, la SEC otra guía con recomendaciones para que las entidades que cotizan en aquél país informen a los potenciales inversores acerca de los riesgos específicos de ciberseguridad que afronta la entidad, y las medidas que ha adoptado para evitarlos.

Por brevedad debida, tan solo podemos mencionar aquí que también existen regulaciones específicas

en sectores como el de la defensa o los denominados prestadores de servicios de confianza (Reglamento eIDAS).

Pero volvamos al tema central de este artículo: por mor del GDPR y de la Directiva NIS, en el verano de 2018 las empresas europeas comenzarán a notificar sus incidentes, o en caso contrario podrían ser sancionadas. ¿Cómo serán? ¿Qué datos pedirán? ¿Qué sistema deberemos usar? ¿Bajo qué procedimiento?

La implementación del Reglamento 611 y la trasposición del Art.13 de la Directiva Marco, en el sector de telecomunicaciones, pueden darnos una aproximación de cómo serán las notificaciones a partir de entonces para el resto de empresas. Y es que, tanto el GDPR como la Directiva NIS, reconocen y preservan las disposiciones sectoriales preexistentes en esta materia. Para mantener el debido equilibrio en el mercado, es de esperar que los reguladores nacionales dejen a un lado la creatividad en esta ocasión, a la hora de desarrollar en detalle el articulado, so pena de crear agravios comparativos entre sectores de actividad empresarial.



El régimen sancionador previsto en alguna de las regulaciones, y que aún está por definir, actuará de inhibidor de la notificación, que si finalmente progresa, abocará a interminables diatribas sobre si fue o no fue lo que fue, y que terminarán en costosos litigios entre reguladores y regulados.

¿A quiénes hay que notificar y cuándo?

En España, si alguien no lo remedia, para decidir a quién habrá que notificar y cuándo, lo mejor sería construirse un ordinograma, que tendría varios "if-then-else" anidados.

Buena parte de los incidentes de seguridad son consecuencia de actos delictivos. Lo primero, por tanto, será denunciarlos como tales a la policía judicial. La Ley Enjuiciamiento Criminal establece en su Art. 259 la obligación para todo ciudadano que tiene conocimiento de la perpetración de un delito, de ponerlo en conocimiento de la autoridad competente o de sus agentes. El Art. 450 del Código Penal tipifica el delito de omisión de los deberes de impedir delitos o de promover su persecución. Aunque la denuncia debemos interponerla personándonos ante cualquier dependencia o puesto de las fuerzas y cuerpos de seguridad del Estado, los hechos punibles pueden notificarse mediante los formularios de contacto habilitados en las páginas web de la policía o de la Guardia Civil, donde podremos realizar cualquier consulta o informar expresamente con datos de que dispongamos sobre la comisión de este tipo de ilícitos.

También la Fiscalía de Sala de Criminalidad Informática dispone de un formulario web para tal fin, y por supuesto, tanto la Fiscal Coordinadora como sus fiscales adscritas abrirán diligencias, si el caso lo requiere, desde su sede de Madrid.

Ahora bien, si en el incidente están involucrados datos de carácter personal, y la empresa es prestadora de servicios de comunicaciones el incidente debe comunicarse además a la AEPD utilizando el formulario que al efecto tiene publicado en su sede electrónica, antes de las 24 horas de tenerse conocimiento del incidente (Reglamento 611). A partir del verano del 2018, todas las empresas estarán obligadas, y en un plazo no superior a las 72 horas (GDPR). Note el lector la sutil diferencia entre denuncias de quiebras de seguridad, cuando son interpuestas voluntariamente por terceros, y notificaciones, cuando lo son a instancias del responsable y por imperativo legal.

Sigamos. Si el incidente ha supuesto la interrupción de un servicio básico de comunicaciones, aplican la

Ley General de Telecomunicaciones, y la Orden Ministerial de Calidad del Servicio, donde se establecen los parámetros y umbrales para la declaración y clasificación de incidentes. Aunque hay que emplearse a fondo para encontrarlos, la SETSI publica en su web el listado de incidentes reportados. Por su parte, ENISA hace lo mismo con los incidentes a nivel europeo en un informe anonimizado de periodicidad anual.

A partir del verano de 2018, con la entrada en vigor de la Directiva NIS, los operadores de servicios esenciales y prestadores de servicios digitales, encuadrados en los sectores listados en su Anexo II, y con más de 250 trabajadores en nómina, deberán comunicar sus incidentes al CERTSI; pero ojo, ya no solo aquellos incidentes que tengan como consecuencia una interrupción del servicio, sino también, por ejemplo, los relativos a pérdidas de confidencialidad.

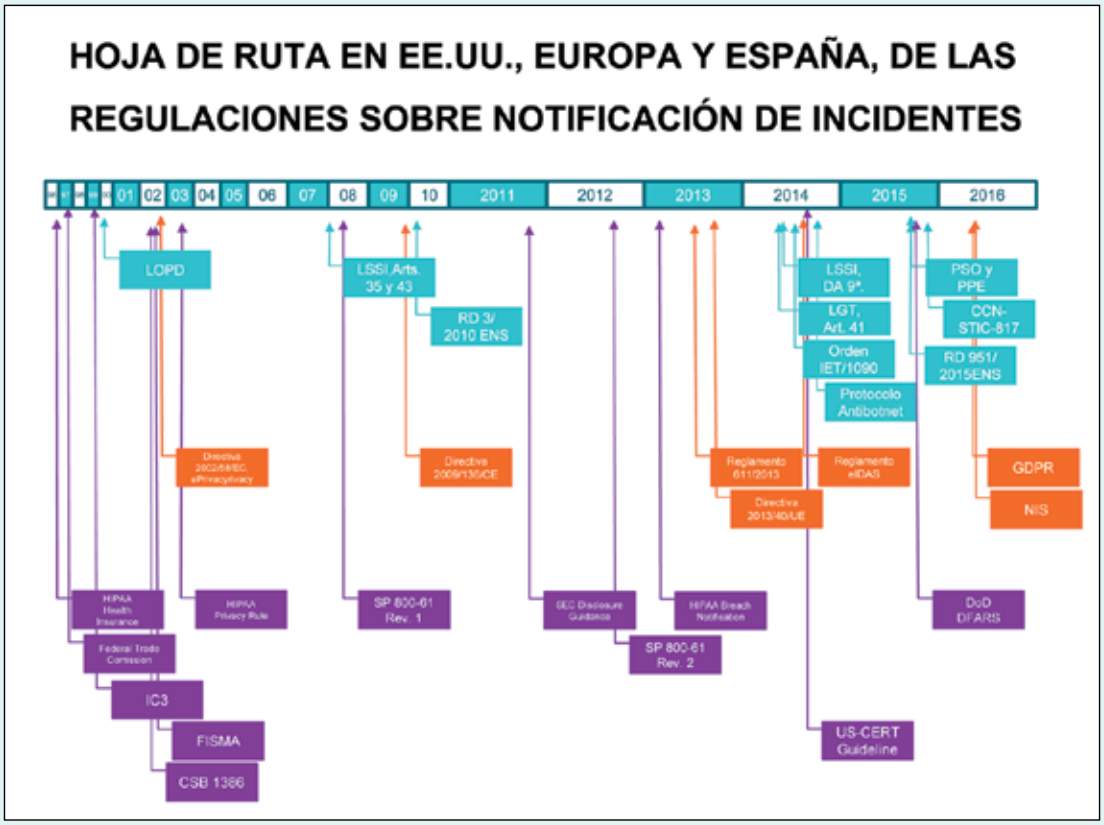
Tras intensos debates al respecto, que por caridad cristiana ahorraremos al lector, en la Directiva no se dice nada aún ni de umbrales ni de plazos. Serán La Comisión y ENISA quienes fijen estos parámetros para los prestadores de servicios digitales a nivel Europeo, y localmente en cada país para los operadores de servicios esenciales.

El pasado 25 de Junio, en la sede de la SETSI, tuvo lugar una reunión interministerial durante la que se informó a representantes de otras Secretarías de Estado y se les pidió una puesta en común, por si las hubiera con carácter sectorial, de este tipo de notificaciones de incidentes.

Sin embargo, muchos de los operadores de servicios esenciales no tendrán que esperar hasta el verano del 2018 para comenzar a notificar por vía de la Directiva NIS, sino que lo harán mucho antes, por un atajo, por la vía de la Ley de Infraestructuras Críticas.

Efectivamente, en aras a cumplir con lo establecido en la resolución de la Secretaría de Estado de Seguridad que aprobó los contenidos mínimos de los PSOs y de los PPEs, el pasado 19 de abril, y también en la sede de la SETSI, tuvo lugar una reunión con los CISOS de representantes de los operadores designados hasta ahora como críticos durante la que INCIBE y CNPIC presentaron los mecanismos para comunicaciones de ciberincidentes y ciberamenazas de dichos operadores.

Por último, no debemos olvidar que las Administraciones Públicas y empresas estratégicas que deban cumplir con el Esquema Nacional de Seguridad, deben notificar al CCN-CERT los incidentes catalogados con niveles Alto, Muy Alto y Crítico, como parte del proceso de gestión de ciberincidentes descrito en la guía de seguridad CCN-STIC-817.



Es imprescindible que las distintas instancias reguladoras, fiscalía y fuerzas de seguridad del Estado, colaboren sobre el terreno y armonicen la definición conceptual, los requerimientos, procedimientos y sistemas de notificación de incidentes. Estamos ante la oportunidad de evitarle a la empresa española una sobrecarga administrativa de dudosa utilidad.

¿Qué datos se piden en las notificaciones?

Siguiendo la RFC 2350 del IETF, el CERTSI ha publicado sus requisitos de información para la gestión de incidentes. Nada sorprendente. Junto con los datos identificativos del informante y de tipo de incidente se piden los del (los) ordenadores atacantes y de los atacados: dominios,

ORGANIZACIONES QUE COMPARTEN INFORMACIÓN SOBRE INCIDENTES

NIVEL	SECTOR	ORGANIZACIÓN
Global	Multi-sector (CSIRTs)	FIRST
Global	Multi-sector	Meridian Conference
Global	Intra-sector (Financiero)	Financial Services Information Sharing and Analysis Center (FS-ISAC)27
EU	Multi-sector	European Advanced Cyber Defence Centre (ACDC)12
EU	Multi-sector	Europol (Joint Cybercrime Action Taskforce team)
EU	Intra-sector (Energía)	Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)
EU	Intra-sector (Financiero)	European Financial Institutes – Information Sharing and Analysis Centre (European FI-ISAC)16
EU	Intra-sector (Servicios Internet)	ENISA Electronic Communications Reference Group (ECRG)
Germany	Multi-sector	Kooperation zwischen Betreibern Kritischer Infrastrukturen (UP KRITIS)20
Finland	Multi-sector	FICORA
España	Intra-sector	CCI Centro de Cooperación Interbancario

direcciones IP, puertos, protocolos, servicios afectados, etc., y cómo no, un amplio campo de texto libre para aportar cualquier detalle adicional. En descargo del IETF debemos decir que el campo de texto libre y desestructurado es un "clásico" de todos los formularios de reporte.

En la "Orden de calidad" de la SETSI, a la que nos hemos referido anteriormente, se solicitan la extensión geográfica y el número de usuarios afectados en el servicio de acceso básico telefónico e internet, la proporción de avisos de avería por línea en acceso fijo y el tiempo de reparación de dichas averías.

El GDPR, además de la cantidad de registros comprometidos y el tipo de datos, exige incluir los datos identificativos y de contacto del DPO, así como las medidas que se han dispuesto para mitigar las consecuencias del incidente.

En su magnífica guía, el CCN categoriza los incidentes y ofrece incluso métricas para su evaluación. Instruye a las AA.PP. en el cuidado debido a la hora de recopilar y custodiar las evidencias, así como la importancia de canalizar cualquier intercambio de información acerca del incidente a través del CCN. La combinación de procedimientos detallados, en lenguaje ingenieril, más una herramienta de soporte como LUCÍA, adaptada al proceso de gestión, constituyen un tándem sólido y predecible, más cómodo y menos ambiguo para el CISO.

Por su más reciente aparición, dejamos para el final la "Guía de reporte de ciberincidentes para el Operador Crítico" editada por CERTSI y avalada por CNPIC e INCIBE. En dicho borrador, de difusión limitada, se reflejan los distintos niveles del Plan Nacional de Protección de Infraestructuras Críticas y los requisitos de respuesta a los incidentes que conlleva cada uno de dichos niveles.

En esta guía para operadores críticos se definen 12 tipologías de incidentes, frente a las 41 de la taxonomía propuesta en la guía del CCN. Sin embargo, en la del CERTSI, se establecen plazos límite, tanto para la notificación por parte del operador que ha sido víctima del incidente, como para el propio CERTSI, requisitos temporales que no aparecen por ningún lado en la guía del CCN. Este compromiso sobre los tiempos de respuesta máximos del CERTSI resulta encomiable por venir, de oficio, de un organismo público, emulando prácticas habituales del sector privado. Ahora bien, del lado del operador crítico se exige una notificación inmediata, o a lo sumo en 4 horas desde la detección, en algunas de las tipologías de la ta-

MATRIZ RASCI DE GESTIÓN DE INCIDENTES EN UNA GRAN MULTINACIONAL

ACTIVIDAD	ROLES						
	SegInfo local	SegTI/Red local	SegInfo Corp	SegTI/Red Corp	DPO local	DPO Corp	Resp.Cont. Negocio local
Gestionar localmente, comunicar y registrar los incidentes de seguridad	R	S	I		I		
Supervisar y registrar los incidentes de seguridad globales	I		R	S			
Implantación de las medidas correctoras que disminuyan la probabilidad de ocurrencia del incidente	A	R	I	S	I	I	I
Registrar los incidentes de seguridad relevantes	I		R				
Gestionar notificaciones a organismos oficiales si afectan a datos personales	I				R	I	
Gestionar los planes de continuidad como consecuencia del incidente	I						R
Análisis forense del incidente	R	S					

ROL		Tarea
R	Responsible	Responsable de realizar la actividad
A	Accountable	Aprueba la actividad realizada
S	Supportive	Proporciona recursos adicionales para realizar la actividad
C	Consulted	Es consultado y posee información para realizar la actividad
I	Informed	Es informado sobre el progreso y resultados de la actividad

bla. En muchos casos, en ese plazo, ni siquiera el CISO ha llegado a ser informado internamente.

Recomendaciones y profecías

Es imprescindible que las distintas instancias reguladoras, fiscalía y fuerzas de seguridad del Estado, colaboren sobre el terreno y armonicen la definición conceptual, los requerimientos, procedimientos y sistemas de notificación de incidentes. Estamos ante la oportunidad de evitarle a la empresa española una sobrecarga administrativa de dudosa utilidad.

Las autoridades competentes deben prestar especial atención a la confidencialidad de la información intercambiada sobre incidentes manteniendo el equilibrio entre el derecho de los ciudadanos a ser informados y el daño reputacional que ello podría causar a los prestadores de servicios. Como dijo mi amigo Juan Carlos Gómez: "No hagamos a las empresas doblemente víctimas por el hecho de tener que notificar el incidente"

El régimen sancionador previsto en alguna de estas regulaciones, y que aún está por definir, actuará de inhibidor de la notificación, que si finalmente progresa, abocará a interminables diatribas sobre si fue o no fue lo que fue, y que terminarán en costosos litigios entre reguladores y regulados. ■

Manuel Carpio Cámara
Experto en Ciberseguridad
mcarpio@outlook.es
https://twitter.com/M_Carpio_
https://www.linkedin.com/in/manuelcarpio

REFERENCIAS

1. ESYS, Fundación. *Necesidades y Dificultades de Comunicación de Incidentes de Ciberseguridad en las Empresas*. Madrid. Fundación ESYS, 2014.
2. Jo De Muynck, Dr. Silvia Portesi, Deloitte Bedrijfsrevisoren Belgium. *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. Bruselas. ENISA, 2015.
3. Andreas Rockelmann, Joshua Budd, Michael Vorisek – IDC CEMA. *Data breach notifications in the EU*. Bruselas. ENISA, 2010.
4. Dr. Marnix Dekker, Christoffer Karsberg. *Technical guidance on the incident reporting in Article 13a*. Bruselas. ENISA, 2014.