RESUMEN EJECUTIVO

GUÍA DE ACTUACIÓN ANTE INCIDENTES DE SEGURIDAD QUE REQUIERAN NOTIFICACIÓN

Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI)

Grupo de Trabajo de Seguridad y Calidad

Septiembre 2017

INDICE

EXPERTOS DEL GRUPO DE CALIDAD Y SEGURIDAD DE AUTELSI QUE HAN PARTICIPADO EN LA ELABORACIÓN DE ESTA GUIA.

En primer lugar, queremos manifestar nuestro agradecimiento a las empresas representadas en el Grupo de trabajo de Seguridad y Calidad de AUTELSI; y a sus vocales, que han contribuido activamente al desarrollo y resultado positivo de esta iniciativa. En especial queremos destacar la colaboración de los siguientes integrantes:

Presidente del Grupo de Trabajo

Lázaro Anguís, Francisco, CISO de Renfe Operadora. Ingeniero de Telecomunicaciones. Con más de 25 años de experiencia en el ámbito de la seguridad de la información, posee la habilitación por el Ministerio del Interior como Director de Seguridad. Presidente del Grupo de Calidad y Seguridad de AUTELSI, Director del Centro de estudios de movilidad e Internet de las cosas (CEM) del ISMS Forum, Vicepresidente de la Asociación Española Evidencias Electrónicas (AEDEL), Vocal en comisiones de normalización como SC27 o el Subcomité de Seguridad de las TI del CTN 196 Protección y Seguridad de los ciudadanos. Editor de la norma UNE 71505-1 Sistema de Gestión de Evidencias Electrónicas, y autor de diversos artículos y libros.

Vocales del Grupo de Trabajo

Álvarez Sánchez, Luis Eladio, Ingeniero Superior Industrial del ICAI y Perito de la Corte de Arbitraje de la Cámara de Comercio de Madrid para el sector de las TICC. Lleva más de 30 años de experiencia profesional en el sector de las TIC con responsabilidad creciente, entre otras, en el área de Seguridad, llegando a ser Director de Tecnología, Operaciones y Seguridad de Carrefour durante 13 años. En la actualidad es especialista en estrategia de Seguridad.

Asenjo Muñiz, Javier, HR Manager en NCR España. Licenciado en Psicología Industrial por la UCM. Máster en RRHH, Máster en PRL. Experto en HR Analytics y tecnología para RRHH.

Benito Gómez, Mariano J., Director de Seguridad / CISO de GMV Secure eSolutions, donde ha desarrollado su carrera profesional desde 1998. Ha sido premiado por la revista SIC (2012) por su trayectoria profesional y por Cloud Security Alliance (2015) e ISMS Forum (2013) por sus contribuciones en la Seguridad Cloud Computing. MBA por el Instituto de Empresa, es Ingeniero de Telecomunicaciones por la Universidad de Valladolid y cuenta con las certificaciones CGEIT, CISM, CISA y CRISC, por ISACA, CISSP por (ISC)2, e ISO 27001-LA y BS 25999-LA. En GMV, es responsable de su Sistemas de Gestión de Seguridad de la Información (ISO 27001, desde 2004) y de Continuidad de Negocio (ISO 22301, desde 2010).

Berciano Alonso, Javier, Responsable de respuesta a incidentes en INCIBE/CERTSI. Con más de 13 años de experiencia en el ámbito de la seguridad de la información ha desarrollado parte de su carrera profesional en diversas empresas privadas y sector público. Cuenta con las certificaciones CISSP, GCFA, GNFA y CISA. Desde el año 2007 lidera la respuesta a incidentes en el CERT y realizando tareas de gestión de incidentes, análisis forense, detección, análisis y monitorización de amenazas.

Carmona, Juan Manuel, Consultant & Quality Manager en Seguridad y Privacidad de Datos S.L. - FORLOPD. Director del Departamento de Normas ISO y del Departamento de Calidad Interno de FORLOPD. Licenciado en Derecho por la Universidad de Belgrano (Argentina) y en trámite de homologación en España con más de 15 años de ejercicio de la profesión.

Chávez Rivas, Rodrigo, Director de la práctica de seguridad de UNISYS en España. Ingeniero de Telecomunicaciones y Master en Seguridad de la Información por la UPM. Cuenta con más de 20 años de experiencia en desarrollo de negocio y gestión de proyectos/servicios TIC en diferentes sectores de la industria en España y Latinoamérica. Posee las siguientes certificaciones: PMP (del PMI), CISM, CISA, CRISC, CGEIT (de ISACA), ITIL V3, CCNA (de CISCO), Six Sigma (Black Belt – Unisys) y CNE (de Novell). Miembro activo del Grupo de Calidad y Seguridad de AUTELSI y del capítulo Madrid de ISACA.

García-Romanillos Henríquez de Luna, Javier, Information Security Officer en Centros Comerciales Carrefour. Con más de trece años de experiencia en el ámbito de la seguridad de la información, ha desarrollado gran parte de su carrera profesional como consultor y auditor de riesgos y tecnologías de la información en EY. Es Ingeniero Técnico Informático (UPSAM) y posee las certificaciones CISA, CISM y CRISC por ISACA; Lead Auditor ISO 27001 por BSI; Lead Auditor ISO 22301 por Tüv Nord; Experto Técnico por EuroPriSe; ITIL v3.

Gutiérrez González, José Antonio, Manager de Seguridad de la Información en GRUPO DIA. Con más de diez años de experiencia en el ámbito de la Ciberseguridad, ha desarrollado parte de su carrera profesional como Consultor de Ciberseguridad en ATOS SPAIN. Ingeniero Técnico Informático (UPSAM) con Máster en Seguridad de la Información. CISA, ITIL v3 y PCI-QSA (2012-2015).

Hernández González, Rafael, Responsable de Seguridad de Sistemas de Información de Cepsa (CISO). CISO de Infraestructuras Críticas. Responsable de la definición de las políticas y normativas del entorno industrial. Seguridad de la Información & GRC.

López Bernal, **Pedro Pablo, G**erente GRC & PIC (Gobierno, Riesgos, Compliance & Protección, Infraestructuras y Continuidad Global) de Rural Servicios Informáticos. Máster Auditoría Informática 1991, CISA y Máster Seguridad Global, Curso Superior Infraestructuras Críticas GET/UNED/Instituto Gutiérrez Mellado y Profesor del mismo. Desde 1985 en Servicios Informáticos: ENTEL (hoy INDRA), Citibank, Banco Santander Y RSI, diversos puestos y funciones TIC (Auditoría, Seguridad, Riesgos, Continuidad, Calidad, Procesos, Sistemas, Fraude, Compliance, Privacidad, Gobierno). Miembro Fundador Instituto Continuidad Negocio Español (CONTINUAM) y del Observatorio de Seguridad Integral, Gestión de Emergencias y Continuidad Operativa (SIGECO), actual Presidente de ambas asociaciones desde 2015.

Montalbán Carrasco, Rocío, Ingeniera Superior de Telecomunicación por la Universidad de Cantabria, executive MBA por el Instituto de Empresa. Funcionaria del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración General del Estado. Promoción XVI. Directora de la División de Tecnologías de la Información y las Comunicaciones del Ministerio de Justicia (actualidad) y Subdirectora General Adjunta de Tecnologías de la Información y las Comunicaciones en el Ministerio de Industria, Energía y Turismo (febrero 2009 - junio 2017) Contadora de la Junta Directiva de la Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas.

Ortiz González, Ramón, Ingeniero Técnico Informática Gestión; CISA, CISM por ISACA; PA Compliance en IE y CDPP por ISMS; Comenzó a trabajar en la Televisión en 2001 en el Área de Organización y Procesos de la División de Tecnologías, posteriormente en la empresa de grupo concesionaria de publicidad –Publiespaña- en el Departamento de Desarrollo Estratégico. Desde 2006 es CISO de Mediaset, siendo responsable de Seguridad de los Sistemas IT, Broadcast, Protección de datos y Cumplimiento.

Perdiguero Ruiz, Marian, Ingeniero Superior en Informática por la Universidad Politécnica de Madrid. Desde 2013 Gerente de Seguridad Lógica en Telefónica España. Este puesto conlleva la función de CISO y de Responsable de Continuidad de Negocio en Telefónica España. Anteriormente ha desempeñado otros puestos gerenciales relacionados con los Sistemas y Redes en Telefónica España, Sanitas, Colegio de Farmacéuticos y CSIC.

Pérez San-José, Pablo, Gerente de Ciberseguridad del área Risk Advisory IT de Deloitte. Cuenta con más de 15 años de experiencia profesional en empresas como GfK, BBVA, INTECO-INCIBE, Red.es y la Comisión Nacional del Mercado de las Telecomunicaciones. Ha dirigido y participado en proyectos de asesoramiento en la estrategia, organización y mejora de las capacidades de ciberseguridad para distintos organismos públicos y empresas, así como en numerosas investigaciones en seguridad, privacidad y confianza digital para el BBVA Global Observatory, el Observatorio de la Seguridad de la Información, el Observatorio de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) o el Grupo de Análisis y Prospectiva de las Telecomunicaciones (GAPTEL), entre otros.

Rincón López, Ana, Experta en Seguridad de la Información en Telefónica de España. Ingeniera en Informática (UPSAM) y BSc en Computing & IT (University of Wales), con Máster en Seguridad de la Información y certificaciones CISA por ISACA e ITIL v3. Anteriormente, ha trabajado como Consultora de Seguridad y Procesos en GMV.

Santos Agudo, Gisela, Asociada Senior del Departamento de Derecho Mercantil de GARRIGUES en el área de Nuevas Tecnologías y Protección de Datos. Colegiada del Ilustre Colegio de Abogados de Madrid y licenciada en Derecho y Administración y Dirección de Empresas por la Universidad Carlos III de Madrid.

Santos García, Rafael L., Jefe de Área de Seguridad Informática/CISO del Ministerio de Fomento desde 2012. Funcionario de carrera del Cuerpo Superior de Tecnologías de la Información y las Comunicaciones desde 1992. Ha ocupado puestos en diversos Organismos y Ministerios de la AGE en temas relacionados con la Seguridad Informática recibiendo para ello formación específica en Centros de la Administración y en Empresas y Universidades: (PIC – Programa en Innovación en Ciberseguridad – Curso de Postgrado – Universidad de Deusto.)

Agradecemos especialmente al **Centro Criptológico Nacional (CCN)** , al **Centro de Protección de las Infraestructuras y Ciberseguridad (CNPIC)** sus aportaciones y revisión del documento.

También queremos manifestar nuestro agradecimiento a **GMV** por patrocinar el Desayuno en el que se presentó esta Guía el 5 de octubre de 2017 y a **Red.es** por la cesión de sus instalaciones para celebrarlo.

Introducción

Las redes y sistemas de información desempeñan actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

Durante el año 2018 está previsto que se adopten diferentes normativas que exigirán, a los operadores de servicios esenciales y a los organismos y entidades pertenecientes al Sector Público y privado de los estados miembros de la Unión Europea, la notificación de incidentes significativos que sufran en las redes y servicios de información ante las autoridades competentes para cada caso.

La adopción de esta normativa constituye un hito importante para el refuerzo de la resiliencia en materia de ciberseguridad. Se establecen requisitos en materia de notificación y seguridad en todos los sectores que son vitales para nuestra economía y nuestra sociedad y que, además, dependen en gran medida de las TIC, tales como la energía, el transporte, el agua, la banca, las infraestructuras de los mercados financieros, la sanidad y la infraestructura digital.

Las autoridades competentes ejercerán las funciones de vigilancia derivadas, y aplicarán el régimen sancionador, si procede. Así mismo, promoverán el desarrollo mediante reglamentos y documentos técnicos de las obligaciones que la normativa imponga, en consulta con el sector y con las autoridades que ejerzan competencias por razón de la materia sobre aquel, para evitar crear obligaciones duplicadas, innecesarias o excesivamente onerosas.

La notificación de incidentes forma parte de la cultura de gestión de riesgos, de tal manera que la nueva regulación va a definir el marco de protección para la entidad notificante y a todo empleado que informe sobre incidentes ocurridos; reservándose la información confidencial de su divulgación al público o a otras autoridades distintas de la notificada y se permita la notificación de incidentes aun cuando no sea obligada su comunicación.

Los Equipos de Ciberseguridad y Gestión de Incidentes (CSIRT, por sus siglas en inglés de *Computer Security Incident Response Team;* o CERT*, Computer Emergency Response Team*) como equipos de respuesta a incidentes monitorizan las redes para detectar posibles incidentes, difundir alertas sobre ellos y aportar soluciones para mitigar sus efectos. Dichos CSIRT son la puerta de entrada de las notificaciones de incidentes, lo que permitirá organizar rápidamente la respuesta a los mismos.

Estos CSIRTs o CERTs pueden ser públicos o privados. Las autoridades CCN (Centro Criptológico Nacional) y CNPIC (Centro Nacional de Protección de Infraestructuras y Ciberseguridad) disponen ya en la actualidad de CERTs; en concreto son los denominados CCN-CERT y el CERTSI (CERT de Seguridad e Industria) bajo la coordinación del CNPIC e INCIBE (Instituto Nacional de Ciberseguridad de España).

Los CERTs gubernamentales nacionales, prevén la utilización de una plataforma común para la notificación de incidentes, de tal manera que los operadores no deban efectuar varias notificaciones en función de la autoridad a la que deban dirigirse.

Este deber de informar implica el cumplimiento de una serie de formalidades en unos plazos establecidos, definidos en cada una de las regulaciones correspondientes. Estas obligaciones, junto a las que ya están establecidas en normativas ya en vigor en 2017, se detallarán a lo largo del presente documento.

Los cambios regulatorios van a provocar que la notificación de Incidentes, las sanciones por incumplimiento en la notificación y la identificación de las responsabilidades vayan a formar parte de nuestra realidad cotidiana.

Los operadores no pueden ser ajenos a esta realidad, ya que el operador es responsable de resolver los incidentes y reponer las redes y sistemas de información afectados a su funcionamiento ordinario.

Analizando todo lo anterior, el Grupo de Calidad y Seguridad de AUTELSI ha identificado como del máximo interés para los asociados la elaboración de una "**Guía de Actuación ante Incidentes de Seguridad que requieran notificación"**. El alcance de la Guía se va a ceñir a las regulaciones que se detallan en el apartado "Normativas que me obligan a notificar".

La metodología para elaborar esta guía ha consistido en responder a las preguntas que las organizaciones se plantean cuando ocurre un Incidente de Seguridad cualquier percance relacionado con la Seguridad de la Información, si bien, la obligación de notificar establecida en su caso en cada regulación será de aplicación o no en función de que tengan efectos significativos en los servicios esenciales que prestan y de la información afectada por ese incidente o percance.

Para elaborar las respuestas, se han creado varios subgrupos de trabajo, enfocados en el estudio de cada regulación identificada.

A continuación, se desarrollan unas respuestas a preguntas básicas.

Qué es un Incidente de Seguridad

A lo largo de la presente guía, hablaremos de los Incidentes de Seguridad, si bien cada regulación revisada tiene una definición de este término, lo cierto es que son similares, aunque con ciertos matices. En cada sub-apartado se definirá lo que cada una de esas regulaciones entiende por Incidente de Seguridad.

Leyes que obligan a notificar

Esta guía pone el foco en las leyes o reglamentos que afectan a la información, a los sistemas que la tratan y a los datos de carácter personal, pero con un ámbito de aplicación de carácter general. Quedan fuera de su ámbito otras normas más específicas. Por ejemplo, PCI DSS (para

el uso de las tarjetas de crédito/débito); Ley 7/2014 de Seguridad Privada ya que, si bien su uso está extendido, no tiene tanta repercusión como las regulaciones objeto de este trabajo; Ley 34/2002 o LSSICE, que establece obligaciones de reporte de incidencias en sector de Telecomunicaciones; y otras.

Por otra parte, la propia dinámica del marco regulatorio y su evolución en el tiempo hace que, forzosamente, la guía se refiera al estado de la regulación vigente en la fecha de fin de los trabajos de análisis, 15 de junio de 2.017. La aparición de nuevas regulaciones que impliquen el deber de comunicación de incidencias y/o enmiendas y modificaciones realizados por los Legisladores del marco vigente en esa fecha no pueden ser incluidos (por desconocidos) en este documento).

Por tanto, esta guía no pretende ser un catálogo pormenorizado y exhaustivo de todas las regulaciones, sino una guía centrada en aquellas que aplican a la gran mayoría de los sectores profesionales de España. Estas normativas de las que se tratará en este documento son:

- RGPD: Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Este reglamento será de obligado cumplimiento a partir del 25 de mayo de 2018.

- LPIC: Ley del 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas.

- NIS: Directiva UE 2016/1148 del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión Europea.

- RD 3/2010: Real Decreto por el que se regula el Esquema nacional de Seguridad en el ámbito de la administración electrónica. Última modificación el 4 de noviembre de 2015 con el RD 951/2015.

A quién va dirigida la Guía

Esta “Guía de actuación” va dirigida tanto al sector público como al sector privado español con independencia del tamaño o sector de actividad de la empresa.

Respecto a la persona o puesto, va dirigida al responsable de comunicar, y a veces gestionar, los incidentes de seguridad, que suele ser típicamente el Responsable de Cumplimiento, o el Responsable de Seguridad, o el Delegado de Protección de Datos o similar.

Función de la Guía

La función de la presente guía es dar soporte a los profesionales de la seguridad de la información, a los distintos componentes del comité de crisis/seguridad o responsables en esta

materia para que puedan informar, a tiempo, dichas situaciones con un criterio homogéneo a los organismos correspondientes.

Esta guía también pretende servir de elemento de sensibilización y de acercamiento de dicha problemática a los distintos órganos de Dirección de las empresas y entes públicos.

Objetivo de la Guía

Se pretende que esta guía sea eminentemente práctica y breve para que pueda cumplir con su objetivo que es: “Ayudar a identificar de manera rápida y eficaz las principales obligaciones de las empresas y entes públicos ante una notificación de un incidente de seguridad”.

¿Por qué debemos notificar?

Se considera esencial establecer buenas prácticas sobre notificación, utilización de una taxonomía común de incidentes y procedimientos para la notificación de los mismos, incluyendo los eventos sobre los que se desconoce el impacto.

Los operadores tienen que habituarse a notificar de forma natural incidentes potencialmente significativos como elemento fundamental para la detección y respuesta en tiempo oportuno. Hay que ser conscientes de que, si queremos mejorar la resiliencia global en materia de ciberseguridad, todo empieza en la notificación de incidentes.

Por último, no se puede pasar por alto que debemos notificar un incidente de seguridad a la autoridad de control competente en su materia porque es, o va a ser, un requisito obligatorio de la normativa correspondiente y así evitar posibles sanciones.

Beneficios de la notificación de incidentes

El legislador y los entes regulatorios consideran que la notificación de los incidentes de seguridad es un beneficio para todos: los estados, la sociedad, las empresas y las personas, ya que los incidentes comunes, que afecten a varias empresas o entes públicos, pueden relacionarse e identificarse de manera anticipada o temprana y solucionarse con una mayor celeridad.

Es innegable también la información que aportan a la función de monitorización y supervisión de las autoridades competentes. Conocer el volumen, tipo e impacto de los incidentes, permiten a autoridades y empresas, dimensionar adecuadamente recursos y esfuerzos que se deben dedicar a paliar los incidentes, y de forma más eficiente a prevenir aquellos incidentes que se repiten o a identificar carencias y vulnerabilidades que favorecen su aparición.

Además, como es el caso del RGPD, se busca informar al titular de los datos como persona afectada de los hechos acontecidos que afectan a su información de carácter personal. Esto es posible porque esta notificación va a permitir que, a nivel nacional se pueda coordinar e intercambiar información con los organismos adecuados del país y, a nivel de la Unión Europea los distintos organismos de los países miembros puedan comunicarse entre ellos de forma eficiente para gestionar con diligencia los distintos incidentes.

Con carácter preventivo, esta información compartida puede utilizarse para prepararse mejor ante incidentes futuros mejorando la seguridad tanto de los sistemas como de los datos. Finalmente indicar, que en los casos que sean obligatorios y donde haya sanción, la notificación y la cooperación desde el primer instante, puedan repercutir en una menor sanción. De esta manera, en el caso de la transposición de la Directiva NIS, a la hora de tipificar las infracciones y sanciones, la ley se decanta por impulsar la subsanación de la infracción antes que su castigo, el cual, si es necesario dispensarlo, será proporcionado pero severo, en línea con lo ordenado por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

Tabla resumen

La siguiente tabla resume cada una de las cuestiones que se desarrollan en detalle a lo largo de los distintos epígrafes de esta Guía:

	NIS	RGPD	ENS	LPIC
Regulación que establece la obligación de notificar				
Normativa	Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016	Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016	Real Decreto 3/2010, de 8 de enero, Esquema Nacional de Seguridad en el ámbito de la Administración electrónica	Ley 8/2011, de 28 de abril
Vigencia	Plazo límite para su transposición 9 de mayo de 2018	25 de mayo de 2016, pero de obligado cumplimiento a partir de 25 mayo de 2018	En vigor	En vigor
¿Quién está sujeto?	Operadores de servicios esenciales (OES's) y proveedores de servicios digitales (DSP's)	Personas físicas y jurídicas responsables de datos de carácter personal	Entidades ámbito aplicación Sector Público	Operadores de infraestructuras críticas
Autoridad	Pdte. de definir en la transposición nacional	AEPD	CCN (CNI)	CNPIC
¿Qué incidentes deben notificarse?				
	Incidentes que tengan efectos significativos en los servicios esenciales que prestan OES y DSP	Incidentes que afecten a los datos de carácter personal	Incidentes con impacto significativo en la seguridad de la información manejada o servicios prestados (CCN-STIC-817)	Incidentes que afecten a los servicios esenciales

	NIS	RGPD	ENS	LPIC
¿Qué información se debe notificar?				
Descripción del incidente	X	X	X	X
Usuarios afectados	X	X	X	
Extensión geográfica	X			
Duración del incidente	X		X	
Grado/Alcance/Impacto de perturbación	X		X	X
Categorías de los datos de carácter personal afectados		X		
Clasificación/Tipificación/Nivel del incidente	X		X	X
Información de contacto	X	X	X	
Número y tipología de sistemas afectados	X		X	X
Información relativa a efectos transfronterizos	X			
Descripción de posibles consecuencias		X		
Descripción de medidas adoptadas o propuestas		X	X	X
Recopilación de evidencias	X		X	
¿A quién se debe notificar?				
	CSIRT de referencia	AEPD	CCN-CERT	CERTSI
¿Quién debe notificar?				
	Operadores de servicios esenciales o Prestadores de servicios digitales.	Responsable del tratamiento de los datos personales (**DPO**)	Entidades ámbito aplicación Sector Público. Habitualmente a través del Responsable de Seguridad de la Información (**CISO**)	El Responsable de Seguridad y Enlace, a través del Responsable de Seguridad de la Información **(CISO)**

	NIS	RGPD	ENS	LPIC
¿Cuándo hay que notificar?				
	Lo antes posible	Menos de 72h.	Lo antes posible	Lo antes posible, la guía de notificación de ciber incidentes establece unos plazos (ventanas) en función del tipo de incidente (gravedad)
¿Cuál es la sanción máxima si no se notifica?				
	Pdte. de definir en la transposición nacional	Contempla multas administrativas de 10.000.000 (siendo la no notificación una de las causas) o 20.000.000 de euros, o en el caso de que se trate de una empresa, de una cuantía equivalente al 2% o al 4% como máximo del volumen de negocio anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.	-	-
¿Cuáles son los canales de notificación?				
	A la Autoridad Competente, a través del CSIRT de referencia	Sede Electrónica AEPD	• Herramienta LUCÍA • incidentes@ccn-cert.cni.es	pic@certsi.es incidentes@ccn-cert.cni.es (dependiendo de la naturaleza del operador: privada o pública)


autelsi