RESUMEN/ABSTRACT

Arturo Ribagorda Garnacho

PANORAMA ACTUAL DE LA CIBERSEGURIDAD

Se comenzará definiendo la ciberseguridad, para a continuación exponer las causas de la inseguridad de los sistemas y redes basados en las TIC. Seguidamente, para tomar conciencia del tema, se presentan las cifras de la inversión anual que origina y la gran cantidad de puestos de trabajo que está creando. En el núcleo del artículo, se tratarán las amenazas y vulnerabilidades de aquellos sistemas y redes, para dar después una visión de las herramientas de ataque y las principales plataformas y dispositivos afectados. Se concluirá con una somera descripción de los diversos tipos de controles de ciberseguridad existentes.

Palabras clave: Ciberseguridad, amenazas, vulnerabilidades, ataques, controles de seguridad.

In this article, and after defining cybersecurity, the causes of the insecurity of systems and networks based on the ICT are exposed. To increase awareness on the topic, figures of associated investment and jobs are presented. The core of the article discusses the threats and vulnerabilities of those systems and networks, giving a vision of the attack tools and the main platforms and affected devices. It concludes with a brief description of the various types of existing cybersecurity controls.

Keywords: *cybersecurity, threats, vulnerabilities, attacks, cybersecurity controls*

Luis Fernández Delgado

ESPAÑA Y LA CIBERSEGURIDAD: HORA DE REMANGARSE

Este artículo describe la evolución y perspectivas del mercado de la ciberseguridad en España, describiendo los ofertantes y sus servicios, los demandantes y sus necesidades, desde una perspectiva de comparación internacional en la que se puntualiza el reto de aumentar el apoyo público.

Palabras clave: ciberseguridad, España, agentes privados, apoyo público, comparativa internacional

This article describes the evolution and perspectives of the cybersecurity market in Spain, describing both supply and demand sides from an international comparison perspective in which the challenge of increasing public support is pointed out.

Keywords: *cybersecurity, Spain, private stakeholders, public support, international comparative*

Ana I. Ayerbe Fernández-Cuesta

LA CIBERSEGURIDAD DE LA INDUSTRIA 4.0: UN MEDIO PARA LA CONTINUIDAD DEL NEGOCIO

La Industria 4.0 o la Internet Industrial consiste en digitalizar, conectar máquinas, sistemas, empresas, recogiendo cantidades ingentes de datos para tomar decisiones informadas lo más rápidamente posible, con el objetivo de incrementar la productividad y el volumen de negocio. Además de múltiples beneficios, la digitalización y la conectividad aumentan la superficie de exposición de las empresas a ciberataques y las consecuencias de un ciberataque, perpetrado por cibercriminales pueden revestir diferentes niveles de gravedad. Si queremos tener una industria 4.0 resiliente es fundamental considerar la ciberseguridad en el diseño y operación de los proyectos de Industria 4.0.

Palabras clave: Industria 4.0, ciberseguridad, continuidad de negocio

Industry 4.0 or the Industrial Internet consists on digitalization, the connection of machines, systems and companies, and the collection of huge amounts of data to take informed decisions in the shortest time, with the final goal of increasing productivity and the business volume. In addition to multiple benefits, digitalization and connectivity increase the exposure area of companies to cyberattacks and the consequences of a cyberattack perpetrated by cybercriminals, can have different severity levels. If we want to have a resilient Industry 4.0, it is fundamental to consider cybersecurity in the design and operation of Industry 4.0 projects.

Keywords: *Industry 4.0, cybersecurity, business continuity*

Juan González Martínez

INNOVACIÓN EN CIBERSEGURIDAD. ESTRATEGIAS Y TENDENCIAS

Este artículo trata el contexto de la innovación en ciberseguridad desde dos puntos de vista. Desde un punto de vista estratégico, por la importancia del creciente mercado en ciberseguridad donde Europa es principalmente un importador de tecnología y por la dependencia externa en un sector considerado crítico para la economía y para la sociedad. Desde un punto de vista tecnológico, donde se expondrán las principales tendencias en innovación en materia de ciberseguridad.

Palabras clave: ciberseguridad, innovación, estrategia

This article addresses the context of innovation in cybersecurity from two points of view. From a strategic point of view, due to the importance of the growing market in cybersecurity where Europe is mainly an importer of technology and because of the external dependence in a sector considered critical for the economy and for society. From a technological point of view, where the main tendencies in cybersecurity innovation will be presented.

Keywords: *cybersecurity, innovation, strategy*

Tomás Castro Alonso

CIBERSEGURIDAD EN *ONE STOP SHOP*, UNA VENTAJA COMPETITIVA

La Agrupación Empresarial Innovadora (AEI) de Ciberseguridad y Tecnologías Avanzadas reúne a empresas, asociaciones, centros de I+D+i, universidades y entidades públicas o privadas interesadas en la promoción del sector de las Tecnologías Avanzadas o emergentes, especialmente a la Ciberseguridad, sus industrias afines y auxiliares, y sectores emparejados con el mismo, que deseen contribuir a los fines de la Agrupación. Mediante el lanzamiento del HUB de Ciberseguridad y Tecnologías Avanzadas de Castilla y León, la AEI pretende dar solución con un modelo de ventanilla única a los principales problemas del sector TIC y del ámbito de la Ciberseguridad: la dificultad para captar y retener talento especializado en las empresas, el fomento de la I+D+i industrial, el trabajo en co-desarrollo, la formación especializada o la tutela de emprendedores.

Palabras clave: ciberseguridad, tecnología, economía digital, digitalización, emprendedores

The Innovative Business Group in Cybersecurity and Advanced Technologies brings together companies, associations, R & D centers, universities and public or private entities interested in promoting the Advanced or Emerging Technologies sector, especially Cybersecurity, its related industries and auxiliaries, and sectors paired with it, who wish to contribute to the aims of the Association. The main handicaps of the ICT sector and in the field of Cybersecurity are: the difficulty to attract and retain specialized talent in companies, the promotion of industrial R+D+i, work in co-development, specialized training or tutelage of entrepreneurs.

Keywords: *cybersecurity, technology, digital economy, entrepreneurs*

Roberto Baratta Martínez

GOBIERNO DE LA CIBERSEGURIDAD

El gobierno de una función como la ciberseguridad, que es a la vez operativa y tremendamente técnica como procedimental, regulatoria y jurídica, complica su enfoque dentro de las organizaciones. Este artículo expone las expectativas de esta función, cómo las organizaciones pueden y deben contemplarla y afrontarla en sus procesos internos, y especialmente cómo tenerla en cuenta en las decisiones corporativas donde la diligencia debida, la responsabilidad social y penal, la regulación y la operación y actividad financiera deben reflejarla.

Palabras clave: ciberseguridad, gobierno, cumplimiento, corporativo, seguridad

Governance in a function such as cybersecurity that is both operational and tremendously technical, as well as procedural, normative and legal, introduces a great complexity within organizations. This article exposes the expectations of this function, how organizations can and should integrate it in their internal processes, and especially how to consider it in corporate decisions where due diligence, social and criminal responsibility, regulation and the operation and financial activity must reflect it.

Keywords: *cybersecurity, governance, compliance, corporate, security*

Alberto Hernández Moreno

DE INTECO A INCIBE: UN PROCESO DE TRANSFORMACIÓN PARA EL FOTALECIMIENTO DE LA CIBERSEGURIDAD DE LOS CIUDADANOS Y EMPRESAS EN ESPAÑA

El presente artículo hace un repaso a la Estrategia de Ciberseguridad Nacional, detallando de forma más precisa aquellas acciones orientadas al desarrollo de la ciberseguridad en el ámbito del ciudadano y la empresa, las cuales se enmarcan en los objetivos y líneas de acción en los que INCIBE contribuye decididamente. Como centro de excelencia digital del Gobierno de España, INCIBE ha reforzado sus capacidades de prevención, concienciación, detección y respuesta frente a los ciberataques a ciudadanos y empresas y desarrollado un ambicioso plan de fortalecimiento, dinamización e internacionalización de la industria nacional de ciberseguridad, dado que la ciberseguridad no sólo supone un reto a la seguridad nacional sino también una oportunidad para el desarrollo nuestra economía.

Palabras claves: ciberseguridad, España, ciberespacio, Internet, tecnología, amenazas, virus informáticos

This article reviews the Spanish´s National Cybersecurity Strategy, detailing more precisely those actions aiming to citizens and companies. INCIBE, as the reference cybersecurity office of the Government of Spain, has strengthened its capacities for prevention, awareness, detection and response to cyberattacks, and has developed an ambitious plan to strengthen, boost and internationalize the national cybersecurity industry, given the challenge/opportunity dual nature of the topic.

Keywords: *cybersecurity, Spain, cyberspace, Internet, technology, threats, computer viruses*

Fernando J. Sánchez Gómez

POLÍTICAS Y CAPACIDADES DE CIBERSEGURIDAD DEL MINISTERIO DEL INTERIOR EN RELACIÓN CON LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Dentro del Ministerio del Interior, el Centro nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) tiene una doble orientación: una, dirigida a la protección de las infraestructuras críticas y los servicios esenciales; y una segunda, dedicada a funciones de coordinación de la ciberseguridad, a través de su oficina de Coordinación Cibernética. El presente artículo trata de abordar el funcionamiento y misiones de este órgano recientemente creado.

Palabras clave: *ciberseguridad, infraestructuras críticas, CNPIC*, Spain

Within the Spanish Ministry of the Interior, the National Center for the Protection of Infrastructures and Cybersecurity (CNPIC) has a double orientation: one, aimed at the protection of critical infrastructures and essential services; and a second, which is dedicated, through the Cyber Coordination Office, to harmonizing cybersecurity tasks. This article addresses the working patterns and missions of this newly created body.

Keywords: *cybersecurity, critical infraestructures, CNPIC, España*

Miguel Ángel Amutio Gómez

EL ESQUEMA NACIONAL DE SEGURIDAD, AL SERVICIO DE LA CIBERSEGURIDAD DEL SECTOR PÚBLICO

El Sector Público está particularmente expuesto a los ciberataques. El Esquema Nacional de Seguridad (ENS) ofrece un planteamiento común de principios, requisitos y medidas de seguridad. A las empresas proveedoras de servicios y soluciones tecnológicas les es exigible el cumplimiento del ENS y han de poder demostrar la correspondiente conformidad. En este artículo se exponen el contexto, objetivos y condiciones establecidas en el ENS, se dimensiona el alcance y situación de implantación del ENS, así como su impacto en las empresas proveedoras de servicios y soluciones al Sector Público, a la luz de los informes de seguimiento y de los mecanismos de conformidad desplegados; finalmente se enuncian retos a afrontar.

Palabras clave: administración digital, ciberseguridad, seguridad de la información, Esquema Nacional de Seguridad, acreditación, certificación, conformidad, instrucciones técnicas de seguridad, ISO 17065, auditoría de la seguridad.

Public Sector is particularly exposed to cyber-attacks. The National Security Framework (Esquema Nacional de Seguridad - ENS) establishes a common approach to principles, requirements and security measures. Services and technological solutions providers are required to comply with the ENS. This article presents the context, objectives and conditions established by the ENS, its scope and implementation level, as well as its impact on providers, according to the monitoring reports and the compliance mechanisms deployed. The article concludes with some challenges to be addressed.

Keywords: *digital government, cybersecurity, information security, national security framework, accreditation, certification, compliance, technical security instructions, ISO 17065, security audit.*

Miguel García Menéndez

UN PANORAMA (CASI) GLOBAL DE LAS POLÍTICAS PÚBLICAS Y LA AUTORREGULACIÓN PARA COMBATIR LA FRAGILIDAD DIGITAL EN LA INDUSTRIA

Este artículo ofrece los principales hallazgos y conclusiones de un análisis realizado en el ejercicio 2017-18 sobre las diferentes aproximaciones por las que han optado una serie de países, y sus empresas, para combatir la fragilidad digital de su Industria. Se han estudiado tanto los aspectos regulatorios (políticas públicas en materia de estrategias de ciberseguridad), como los auto-regulatorios (códigos de buen gobierno corporativo de las sociedades industriales cotizadas).

Palabras clave: autorregulación, ciberseguridad industrial, estrategia, fragilidad digital, gobierno corporativo, regulación

This article offers the main findings and conclusions of an analysis conducted in the financial year 2017-18 on the different approaches that a number of countries, and their companies, have chosen to combat the digital fragility of their Industry. Both the regulatory aspects (public policies on cyber security strategies), as well as the self-regulatory ones (codes of good corporate governance of listed industrial companies) have been studied.

Keywords*: corporate governance, digital fragility, industrial cyber security, regulation, self-regulation, strategy*

Antonio Troncoso Reigada

DEL PRINCIPIO DE SEGURIDAD DE LOS DATOS AL DERECHO A LA SEGURIDAD DIGITAL

Este estudio analiza las principales novedades que presenta el Reglamento General de Protección de Datos de la Unión Europea y el Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales en el ámbito de la seguridad. Así, se destaca que el Reglamento no contiene las medidas de seguridad a emplear, sino que deja esta decisión en manos del responsable del tratamiento para que aplique aquellas medidas técnicas y organizativas adecuadas al nivel de riesgo, lo que supone un cambio profundo en relación con el ordenamiento jurídico español y con la propuesta de Reglamento de la Comisión. También se estudian otras previsiones del Reglamento como la notificación de una violación de la seguridad de los datos personales a la autoridad de control y la comunicación al interesado. Finalmente se analiza el derecho a la seguridad digital en el Proyecto de Ley Orgánica.

Palabras clave: seguridad del tratamiento de datos; protección de datos; Reglamento General de Protección de Datos de la Unión Europea, Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales

This study analyses the main changes presented by the General Data Protection Regulations of the European Union and the Draft Organic Law on the Protection of Personal Data and Guarantee of Digital Rights in the field of security. Thus, it is highlighted that the Regulation does not contain the security measures to be used but leaves this decision in the hands of the data controller to apply those technical and organisational measures appropriate to the level of risk, which represents a profound reform in relation to the Spanish legal system and the Commission's proposed Regulation. Other provisions of the Regulation are also analysed, such as notification of a breach of the security of personal data to the supervisory authority and communication to the data subject. Finally, the study analyses the right to digital security in the Draft Organic Law.

Keywords*: data processing security; data protection; General Data Protection Regulations of the European Union, Draft Organic Law on Personal Data Protection and Guarantee of Digital Rights.*

Francisco Lázaro Anguís

DE LAS OBLIGACIONES VIRTUD

Un número muy importante de empresas y organismos nacionales, deben cumplir simultáneamente, dos o más Leyes y Normas, en las que la seguridad de la información tiene un peso relevante; tales como, el Reglamento General de Protección de Datos (RGPD), el Esquema Nacional de Seguridad (ENS), la Ley de Infraestructuras Críticas (PIC) o la Ley de trasposición de la Directiva de Seguridad de redes y Sistemas de información (NIS). Estas organizaciones, tienen el reto de hacer convivir, de la forma más eficaz y eficiente posible, las obligaciones que, en materia de seguridad de la Información, les imponen cada una de ellas. El

articulo analiza los requerimientos comunes y cómo "hacer de la obligación virtud", cumpliendo con todas ellas y aprovechando ese esfuerzo para incrementar el nivel de seguridad.

Palabras clave: *gobernanza, políticas, estrategia, buenas prácticas, ciberseguridad, amenazas, normativa*

Many companies and national organizations must comply simultaneously many regulations dealing with information security such as the General Data Protection Regulation (GDPR), the National Security Scheme (ENS), the Critical Infrastructure Law (PIC) or the Directive on security of network and information systems (NIS). These organizations are challenged to meet in the most effective and efficient possible way every information security requirements. This article analyzes core shared requirements of the many pieces of regulation and how to take advantage while ensuring compliance.

Keywords: *governance, policies, strategy, best practices, cybersecurity, threats, regulation*