Manual Básico de Ciberseguridad y Protección de Datos

Escuela de tecnologías digitales

edae

EXIT Editorial

MANUAL BÁSICO DE CIBERSEGURIDAD

y Protección de Datos

MANUAL BÁSICO DE CIBERSEGURIDAD

y Protección de Datos

Fernando Montero Romero
Francisco José Martínez Esteva
Juan Luis Rubio Sánchez
Francisco Toro
José Luis Villena
Pablo Luis Gómez Sierra
José Antonio Rubio Blanco
María Julia Martínez Martínez
Ángel García Collantes
Antonio Villaverde Herranz
Francisco Javier González Espadas
Francisco Tomás Prieto Moraleda
Sandra Ausell

Richard Mababu Mukiur
Juan Luis Rubio Sánchez
Gonzalo Ruiz Sánchez
(coord.)

1ª Edición *Manual básico de ciberseguridad y protección de datos*
Diseño de portada: Doce Calles

Exit Editorial S.L.
C/ De la Ribera, 36
28300 Aranjuez (Madrid)
Tel.: (+34) 616 985408
hola@exitcomunicacion.com
www.exitcomunicacion.com

ISBN: 978-84-9744-320-3
Depósito legal: M-28229-2020
Impreso en España

«Tuve la precaución de tomar las medidas adecuadas,
el resultado, seguimos funcionando»

Gruiz-Sánchez

Índice

Biografía de los autores

Fernando Montero Romero

Licenciado en Filología Inglesa por la Universidad Autónoma de Madrid, Máster en Educación en Nuevas Tecnologías y Grado en Ingeniería Informática por la UDIMA.

Actualmente da soporte a clientes en AvidTechnology, empresa que da soluciones para la creación, gestión y distribución de contenidos digitales no lineal. Anteriormente, trabajó como Solution Architect en Toboggan Services y Video Report empresa perteneciente al grupo MediaPro.

Francisco José Martínez Esteva

Programador full-stack de profesión durante más de 20 años especializado en desarrollo web y comercio electrónico. Es vicepresidente del Instituto Internacional de Privacidad y Seguridad y director de la revista Privacidad y Seguridad. Cofundador de varias empresas tecnológicas, de entre ellas Iberdatos especializada en protección de datos.

Juan Luis Rubio Sánchez

Doctor Ingeniero Industrial en Control de Procesos e Inteligencia Artificial (UPM).

Doctor en Ingeniería de Sistemas y Control por la UNED. Ingeniero Técnico Informática de Sistemas (UNED), Máster in Business Administration (ICADE). Vicerrector en la Universidad a Distancia de Madrid y profesor en las áreas de ingeniería del software y aplicaciones empresariales. Ha impartido numerosos cursos sobre ciberseguridad y es colaborador habitual de entidades de reconocido prestigio para la divulgación de la ciberseguridad.

Francisco Toro

Arquitecto de Seguridad y especialista en gestión de proyectos de ciberseguridad en BBVA Next (Banco BBVA). Apasionado de la seguridad y continuidad de negocio, centrado en la Inteligencia, Ciber-estrategia, así como en la continuidad de negocio en entornos de producción e infraestructuras críticas. Más de 20 años en el mundo de la tecnología y amplia experiencia en grandes entornos de producción, especialmente en Banca y en el área de Tecnología de información y Comunicaciones. Experiencia en formación en cursos especializados en Dirección de seguridad y ciberseguridad.

José Luis Villena

Subteniente de la Guardia Civil. Gabinete de Coordinación y Estudios (Secretaría de Estado de Seguridad). Graduado en Criminología por la Universidad a Distancia de Madrid (UDIMA). Máster en Análisis e Investigación Criminal (UDIMA). Profesor en el Curso Superior de Dirección de Seguridad Digital y Gestión de Crisis de la Universidad de Alcalá y Alianza Española de Ciberseguridad y Crisis. Profesor colaborador de

Criminología en la Universidad en la Universidad Internacional de Valencia (VIU) y en la Universidad Europea Miguel de Cervantes (UEMC).

Pablo Luis Gómez Sierra

Criminólogo. Máster Universitario en Ingeniería de Sistemas de Información. Dirección de Proyectos Informáticos. Especialidad en Seguridad e Investigación Digital. Profesor en el Máster Investigación y Análisis Criminal en UDIMA. Experiencia de 25 años en trabajos relacionados con las Ciencias Policiales.

José Antonio Rubio Blanco

Doctor en Ciberseguridad, cuenta con certificaciones internacionales como CISA, CISM, CRISC, Auditor Jefe ISO 27001, Especialista Implantador ISO 27001 o Especialista Implantador ISO 22301 entre otras. Ha ejercido como Coordinador Nacional del ISO/IEC JTC 1/SC 27/WG 4 y WG 5 de AENOR, siendo actualmente Secretario del UNE/CTN 320/SC 4 sobre Servicios y Controles de Seguridad. Miembro del Club de Roma y del Consejo Asesor de ISACA Madrid, ha formado parte del Comité de Expertos para la elaboración de la Estrategia Nacional de Ciberseguridad de España, siendo actualmente miembro de las vocalías del Foro Nacional de Ciberseguridad, dependiente del Consejo de Seguridad Nacional.

María Julia Martínez Martínez

Licenciada en Ciencias Económicas y Empresariales. Ha desarrollado su carrera profesional en distintos ámbitos del sector financiero como analista de riesgos, donde se ha especializado en metodología, detección de vulnerabilidades, valoración de los sistemas de prevención y mitigación de riesgos. En la actualidad cursa el Programa de Doctorado en Derecho y sociedad de la UDIMA

Ángel García Collantes

Actualmente Decano del Colegio Profesional de la Criminología de la Comunidad de Madrid. Doctor en Derecho, Licenciado en Criminología y Psicología. Máster en Criminología y Deficiencia Juvenil. Máster en Psicopatía Criminal y Forense. Director de la Cátedra de Análisis de Conducta de la Universidad a Distancia de Madrid (UDIMA) y actualmente Decano del Colegio Profesional de la Criminología de la Comunidad de Madrid.

Antonio Villaverde Herranz

Ingeniero de Telecomunicaciones por la Universidad Politécnica de Madrid. Gerente en la multinacional ATOS, donde lleva más de 20 años trabajando en proyectos relacionados con la seguridad y las tecnologías de la información. En la actualidad es responsable de negocio del área de ciberseguridad, habiendo participado en distintos proyectos nacionales e internacionales. Esta actividad la combina con la docencia y la investigación en la UDIMA, donde colabora en acciones formativas en distintos ámbitos TIC y lidera distintos proyectos académicos universitarios.

Francisco Javier González Espadas

Abogado. Socio of Counsel de Ceca Magán Abogados. Presidente del Comité de Expertos Mediación «RGPD» de la Asociación Europea de Arbitraje y CDPP (Certified Data Privacy Professional) por ISMS FORUM. Árbitro y Mediador.

Francisco Tomás Prieto Moraleda

Abogado especializado en Conflictología y ADRS/ODRS, (mediación, negociación, abogacía colaborativa, arbitraje). Especialista Delegado en Protección de Datos.

En los últimos años ha apostado por la innovación, el emprendimiento y la tecnología, volcado en Phi Economy con el proyecto de #RealCoin. Embajador de Economía Phi. Consultor de Blockchain en Alcuadrado Consultoría. Autor del libro Guía Urgente de eMediación y Abogacía Online

Sandra Ausell Roca

Abogada. Compliance & Advisory Career Counselor. GOVERTIS Advisory Services. TELEFÓNICA TECH CYBERSECURY. Docente en WoltersKluwer España. Ha trabajado en IVAC-Instituto de Certificación como evaluadora certificando a Delegados de Protección de Datos. Máster en Sistemas y Servicios de la Sociedad de la Información. Cuenta con certificados ACP-B videovigilancia y Auditoria de seguridad y LOPD por Asociación Profesional Española de Privacidad.

I. MANUAL DE CIBERSEGURIDAD

1. Ciberseguridad y organizaciones civiles

1.1. Ciberseguridad de dispositivos móviles

1.1.1. Resumen del trabajo

Autor: Fernando Montero Romero

El presente documento refleja el estado actual de la ciberseguridad en dispositivos móviles prestando importancia a al uso de las aplicaciones móviles y como hay grupos como OWASP.

La aparición de los dispositivos móviles ha transformado todo el ecosistema digital hasta ahora conocido. Hasta hace relativamente poco considerábamos el ordenador de nuestra casa u oficina el lugar donde almacenábamos nuestra información, en la actualidad todo esto ha cambiado. Información personal, financiera o de empresas es transportada en nuestros bolsillos permitiendo un acceso instantáneo. Los dispositivos móviles rápidamente se han convertido en omnipresentes, a través de nuestros dedos podemos acceder a nuestros datos bancarios o comprobar nuestro correo electrónico.

La irrupción de estas nuevas tecnologías lleva consigo la aparición de nuevos crímenes, la denominada, ciberdelincuencia. Estos cibercriminales desean acceder a nuestros dispositivos con varios objetivos:

- Substracción en provecho de otros.
- Robo de información y posterior extorsión.
- Seguimiento del dispositivo para obtener nuestros hábitos.
- Utilizar nuestro dispositivo para poder suplantar y desde nuestro dispositivo realizar ataques.

Las aplicaciones móviles son parte fundamental en estos dispositivos.

En la actualidad se calculan que existen más de 2 millones de aplicaciones cubriendo un gran espectro de funciones: banca *online*, apuesta, mensajería instantánea por mencionar unas pocas. Estas aplicaciones son en la mayoría de las veces extensiones de los servicios que se ofrecen al navegar en sus respectivas páginas web, haciendo que la aplicación móvil en la mayoría de los casos sea un espejo de su página web.

Las aplicaciones móviles están afectadas por un gran número de vulnerabilidades, muchas de las cuales vienen heredadas de los ataques tradicionales a las páginas web y aplicaciones de escritorio. Sin embargo, en otros muchos casos el ataque se realizar específicamente sobre dispositivos móviles centrándose en el camino en que las aplicaciones móviles son usadas.

Tomando en consideración el ataque a las aplicaciones móviles los desarrolladores deben tomar en consideración que:

- La mayoría de las aplicaciones móviles realizan algún tipo de comunicación en red, ya que es en si misma la razón por las que fueron creadas. Esta comunicación se puede realizar desde una red seguro o totalmente vulnerable como un café, hotel o biblioteca. El desarrollador tiene la obligación de implementar aplicaciones que aseguren un tránsito seguro de datos.
- Los aparatos móviles son transportados todo el día aumentado la posibilidad de robo o pérdida. Cualquier intento de recuperación de la información por los ciberdelincuentes debe ser obstruida, no permtiendo el acceso al *file system* del aparato. Cualquier contenido residual de la cache deber ser eliminado.
- Cada vez que aceptamos el acceso por parte de unas aplicaciones estamos dando acceso a dispositivos tipo Bluetooth, fotos, contactos, cámara.

En relación a toda esta problemática surge la OWASP.

La OWASP (https://www.owasp.org/index.php/Main_Page) es una iniciativa creada sin ánimo de lucro y que tiene como objetivo dar a conocer y concienciar sobre los diferentes problemas de seguridad en dispositivos móviles.

La OWASP hace una revisión anual para identificar los riesgos más críticos para un amplio tipo de organizaciones e individuos. Para cada uno de estos riesgos, se proporciona información genérica sobre la probabilidad y el impacto técnico. Atendiendo a la Top 10 del año en 2016 la siguiente ((https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10):

A1. Uso inadecuado de la plataforma. La característica definitoria de los riesgos en esta categoría es que la plataforma (iOS, Android, etc.) proporciona una característica o una capacidad que está documentada y bien comprendida. Son los usuarios quienes deben entender el uso de las aplicaciones.

A2: Almacenamiento de datos inseguros. Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII).

Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.

En colaboración con la
Cátedra Universitaria Udima - Edae

www.epostgrado.com

c/ Fernán González, 50
28009 – Madrid
91 402 00 61

Acreditaciones y Certificaciones

Cámara Certifica
Empresa certificada
Sistema de gestión
ISO 9001

Madrid Excelente
341.S/41/223/09.

ISBN-13: 978-84-9744-320-3