



Sesión 1 : Importancia de la seguridad de las aplicaciones

Introducción a la seguridad de aplicaciones y mejores prácticas en codificación



Mauricio Sotelo

- Ingeniero de Seguridad Nivel III
- Seguidor de las Buenas Prácticas, Marcos de Trabajo y Estándares de Seguridad.
- Amo las actividades al aire libre y hacer todo con música de fondo
- https://calendly.com/mauricio_sotelo



Recomendaciones Importantes



Identifícate en Zoom usando tu nombre y apellido.



Silencia tu micrófono durante el curso.



Utiliza el chat para hacer preguntas en la sección asignada para ello.



Centra tus preguntas en el tema presentado.

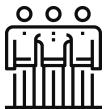


Mantén tu cámara encendida durante toda la sesión.

Academy Código de Conducta



Sé respetuoso, no hay preguntas o ideas malas.



Sé empático y paciente.



Sé cuidadoso con las palabras que eliges.

Objetivo de la Sesión

Al final el módulo, se pretende darte una visión actualizada en materia de seguridad para:

- Comprender de manera integral la importancia y los desafíos de la seguridad en las aplicaciones.
- Reconocer la importancia de mantener una mentalidad proactiva y con un enfoque prioritario en la seguridad.

Tabla de contenido

Importancia de los principios CIA

Enfoque en seguridad

Tema uno

Importancia de los principios CIA



ISO 27001

Año: 2017



Tipo de Ataque: Ransomware NotPetya

Impacto a las operaciones:

- 4,000 servidores
- 45,000 PCs
- 2,500 aplicaciones

Actual Recovery Time (ART): 10 días

La compañía estimó sus pérdidas debido al ataque entre **\$250 y \$300 M.**



Cyber attack update

June 28, 2017

A.P. Møller - Mærsk A/S — cybe

We can confirm that Maersk has
and select business units.

We have contained the issue and

We have shut down a number of
Maersk Tankers, Maersk Training
operations.

Maersk Line vessels are maneu

We continue to assess and man

Business continuity plans are be

Copenhagen, 28 June 2017

Contact person:

Head of external relations, Signe

ANNOUNCEMENT

A.P. Møller - Mærsk A/S — cyber attack update

Podemos confirmar que Maersk fue afectado como parte de un ciberataque global llamado Petya el 27 de junio de 2017. Los sistemas informáticos están fuera de servicio en varios sitios y en ciertas unidades de negocio.

Hemos contenido el problema y estamos trabajando en un plan de recuperación técnica con socios clave de TI y agencias globales de ciberseguridad.

Hemos cerrado varios sistemas para ayudar a contener el problema. En este punto, nuestras entidades Maersk Oil, Maersk Drilling, Maersk Supply Services, Maersk Tankers, Maersk Training, Svitzer y MCI no se ven afectadas operativamente.

Se han tomado medidas preventivas para garantizar la continuidad de las operaciones.

Los buques de Maersk Line son maniobrables, capaces de comunicarse y las tripulaciones están a salvo. APM Terminals se ve afectado en varios puertos. Continuamos evaluando y gestionando la situación para minimizar el impacto en nuestras operaciones, clientes y socios de la situación actual.

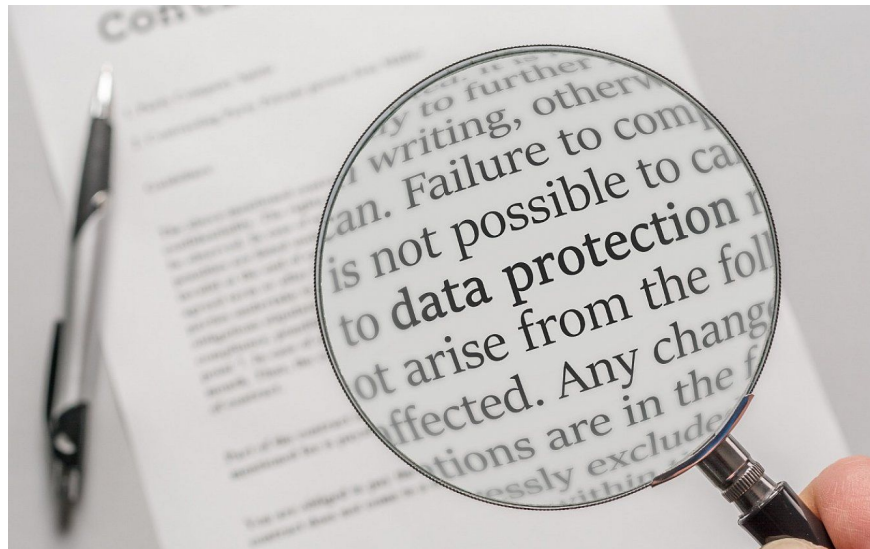
Se están implementando y priorizando planes de continuidad del negocio. Se está evaluando el impacto agregado en nuestro negocio.

Copenhague, 28 de junio de 2017. Persona de contacto: Jefa de relaciones externas, Signe Wagner, tel.: +45 33 63 19 01.

Entendiendo la seguridad de las aplicaciones

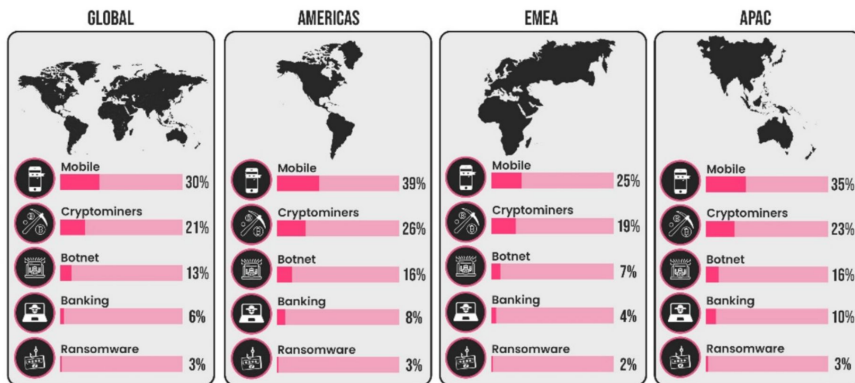
Publicación especial del NIST 800-39: Gestión del riesgo de seguridad de la información

Amenaza: Cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), activos organizacionales, individuos, otras organizaciones o a la Nación, a través de un sistema de información, mediante acceso no autorizado, destrucción, divulgación, modificación de información y/o negación de servicio.



Entendiendo la seguridad de las aplicaciones

Tendencias de ciberataques por región en 2019
Imagen: Check Point



Estados Unidos experimentó muchas más brechas de datos que cualquier otro país en el segundo trimestre de 2023.



Q2 2023 saw 2.6 times more data breaches than Q1 2023

Q2 2023 saw a 156% increase in breached accounts. 110.8M accounts were leaked in total, with 855 accounts being leaked every minute.



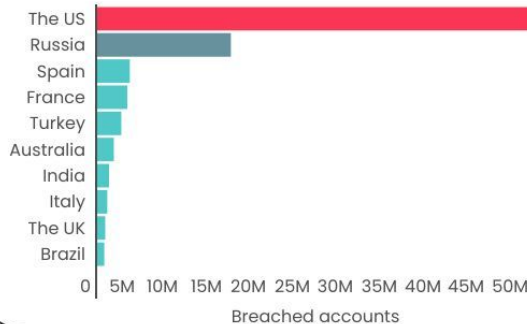
156%

more breached accounts globally in Q2 2023 compared to Q1 2023

Breached accounts

2M 10M 18M 26M 34M 40M

Most-breached countries in Q2 2023



Almost 1 in 2

accounts breached in Q2 2023 were of American origin



This image is licensed under the Creative Commons Attribution-Share Alike 3.0 International License - <https://creativecommons.org/licenses/by-nc-sa/3.0/>



Descanso

5 minutos.





Tabla de Contenido

Importancia de los principios CID



Enfoque en seguridad



Tema dos

- World Economic Forum:
Cybersecurity film
2023.





Q&A



Enfoque en seguridad



Importancia de la formación continua y las actualizaciones

Escenarios reales:

- Heartbleed (2014)
- Apache Struts (2017)
- SolarWinds (2020)



Papel del liderazgo: Fomentar un entorno de seguridad



Microsoft



Google

"La seguridad no es solo una función. Es una mentalidad."

- Satya Nadella, CEO de Microsoft.

- **El liderazgo establece el rumbo.** Si la seguridad es una prioridad en la cima, lo es en toda la organización.
- **La seguridad no es solo un departamento;** es una inversión. Los líderes deben asignar recursos, ya sea en herramientas, personal o capacitación.
- **Las políticas son cruciales.** Pero sin una aplicación rigurosa por parte del liderazgo, son solo palabras en papel.



Q&A





TM

Gracias.