Risk & Compliance

//Julieta Torcello - Ethics & Compliance Corp
//Federico Abud Rey - IT Risk & Resilience
//Florencia Vilardel - IT Risk

IT BOARDING
BOOTCAMP

// Risk & Compliance

¿Quienes somos?

Gabriela Colombo

Rocío Balestra
Fintech Risk & Compliance

Gustavo Regner
Commerce Risk & Compliance

Federico Abud Rey
IT Risk & Resilience

Damián Falcone
CORP Risks

Andrea Saccullo
Ethics & Compliance

¿Qué hacemos?

RISK

COMPLIANCE

RESILIENCE

¿Por qué lo hacemos?

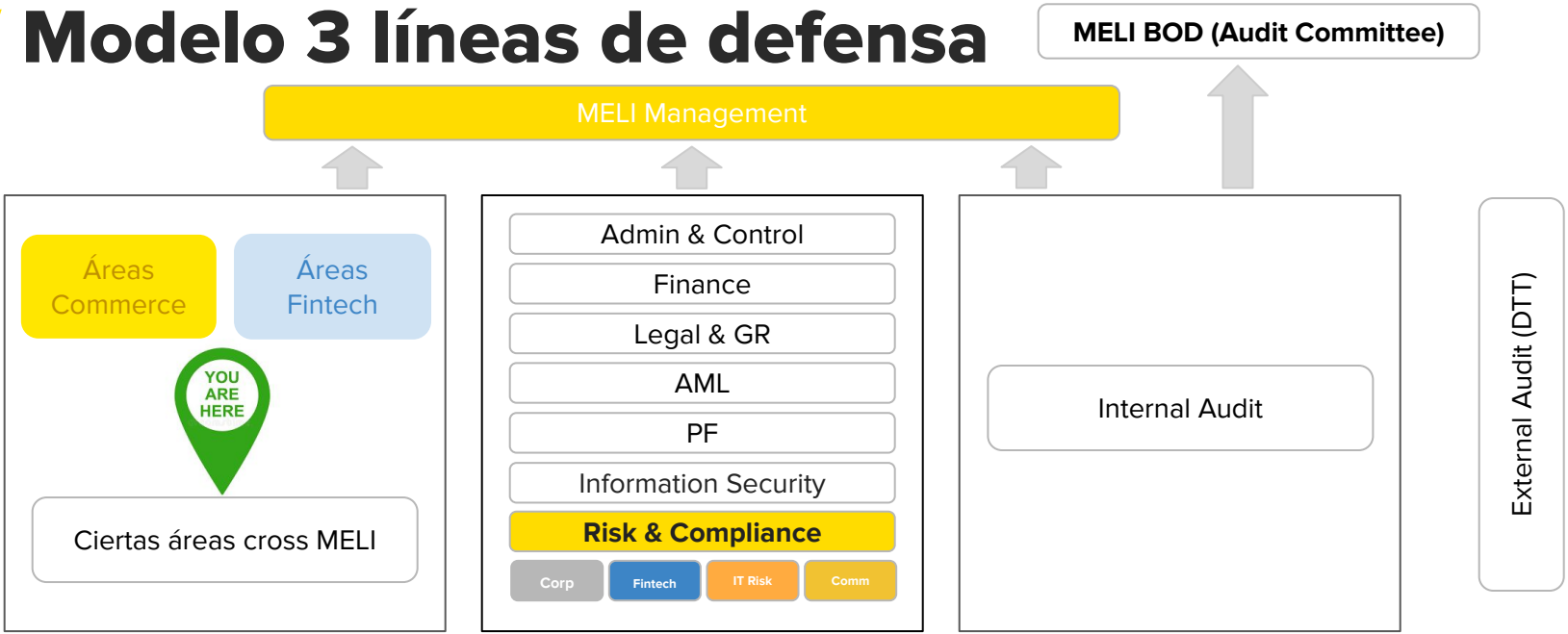
Porque emprendemos tomando **riesgo a conciencia**.

Porque **protegemos** a MELI para que siga creciendo

Porque debemos asegurar el **cumplimiento de las normas** externas e internas

IT BOARDING
BOOTCAMP

// Modelo 3 líneas de defensa



1° línea

Define, implementa y ejecuta controles

2° línea

Asesora al management en la gestión de riesgos. Propone controles. Foco preventivo

3° línea

Evalúa la eficacia de los procesos de gestión de riesgos, control y gobierno

Let’s Play

Kahoot!

https://kahoot.it/

IT BOARDING
BOOTCAMP

// Compliance

Construcción de una cultura de integridad con base en valores comunes, políticas transparentes y en el marco de la ley, que permita un diferencial de negocio, una buena gestión de riesgos y un ambiente de trabajo ético y saludable.

Riesgos a prevenir:

- El daño reputacional.
- La imposición de importantes multas y sanciones.
- Las pérdidas de negocio / licencias.

Cumplimiento de normas

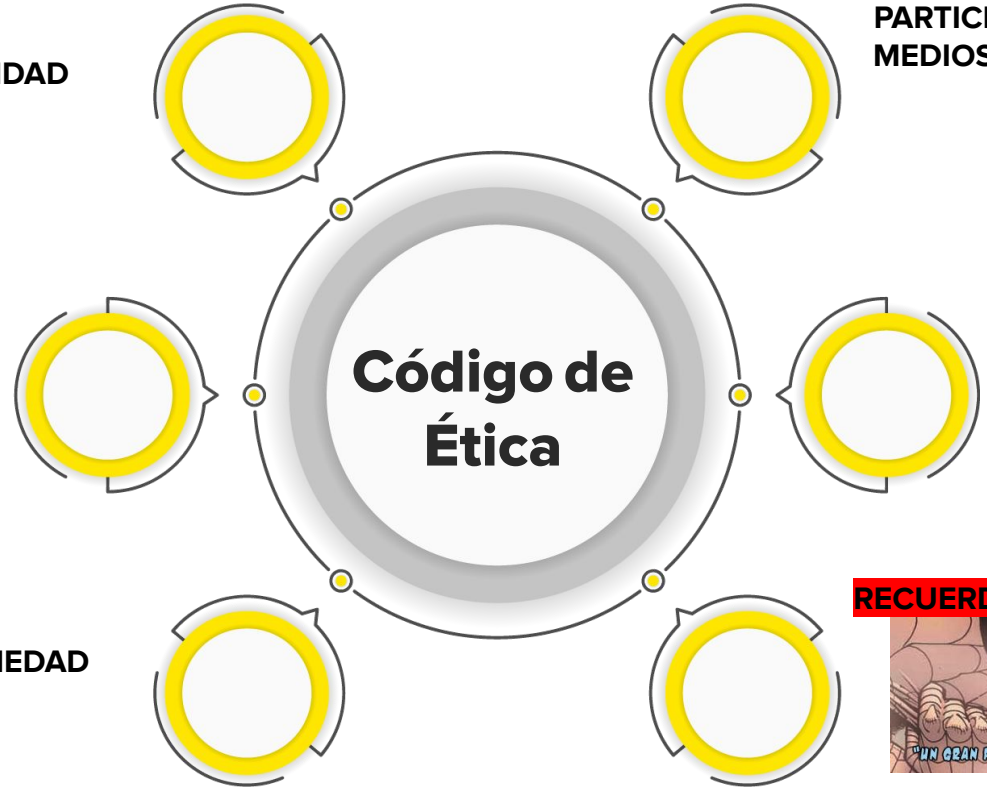
Normas externas

- Leyes y Regulaciones

Normas internas

- Código de Ética
- Políticas internas

Capítulos Clave - CDE



CONFIDENCIALIDAD

PARTICIPACION EN MEDIOS DIGITALES

ACTIVIDADES LABORALES EXTERNAS

USO DE INTERNET, EMAILS Y RECURSOS

DERECHOS DE PROPIEDAD INTELECTUAL

RECUERDA AL TÍO BEN!!!

Tod@s somos responsables del cumplimiento del Código de Ética

// Linea de denuncias

Contamos con altos estándares de ética y transparencia.

No toleramos comportamientos que atenten contra la ley o que no cumplan con estos estándares.

https://denunciasmeli.lineaseticas.com/Complaints/Company

// IT Risk

IT BOARDING
BOOTCAMP

// IT GOVERNANCE

What's IT Governance?

What we talk when we talk about Compliance?

IT Governance

// Qué es?

- **Responsable**: Dirección y ejecutivos
- **Gobierno Corporativo**
- Asegura ->
  - IT **alineada** con el negocio
  - Uso **responsable** de los recursos de IT
  - Administración apropiada de **riesgos**.

//IT Risk

What it is and how it helps?

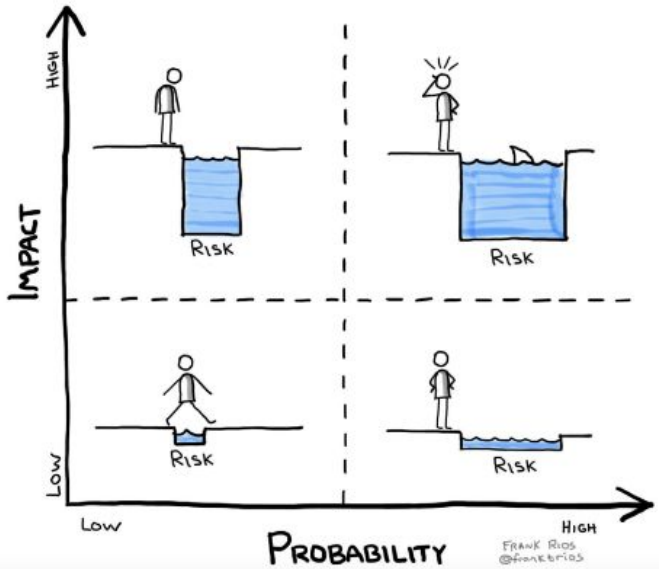
// Risk Analysis

Riesgo -> Probabilidad que algo pase, y si pasa cómo nos impacta.

Elementos del riesgo:

- **Probabilidad** -> Posibilidad de que un evento ocurra
- **Impacto** -> Daño potencial asociado

- **Amenazas** -> daño potencial asociado a una explotación de una vulnerabilidad.
- **Vulnerabilidad** -> falta o ausencia de control o debilidad de éste.



Ayudarlos a identificar los riesgos y vulnerabilidades, reduciendolos a un nivel aceptable e implementar acciones para mantener ese nivel.

// ¿Donde encontramos los riesgos en MELI?

A lo largo de toda la organización. Se relacionan a procesos y se clasifican según su naturaleza

- Ingeniería Social (Phishing, Shoulder surfing).
- Accesos a Bases de Datos (Dataleak).
- Trashing / Clean Desk.
- Actividades del usuario no autorizadas.

- API´s sin protección
- Validaciones de datos
- Descarga de archivos sin protección.
- Virus / Malware (código malicioso).
- Ausencia de control de cambios

- Denegación del servicio.
- Ausencia de Rollbacks.
- Ausencia de Contingencias.
- Acciones humanas – intencionales o accidentales.

- Migración BD de una a otra sin revisión.
- Configuración de parámetros autoescalable
- Integridad de Casos de Uso.

PERFORMANCE

- Deployments sin requerimientos.
- Pasaje a producción sin testing.
- Falta autorización de las implementaciones en producción.
- Respuestas a Requerimientos regulatorios sin validar.

COMPLIANCE

// ¿Cuándo podría generar un riesgo?

- **Al codear**: ¿Estoy desarrollando lo que necesitamos o lo que entiendo/creo?.
- **Al conectar un device o instalar un app**: ¿Está autorizada? ¿Securizada? ¿Es confiable?.
- **Cuando compartimos información**: ¿Es sensible? ¿Se trata de info del Negocio? ¿Sobre interés general? ¿Existen bases ya securizadas donde acceder?.
- **Al testear:** ¿Estoy probando antes de implementar? ¿Cubrí todos los casos y/o los más críticos? ¿Hice pruebas con el user?.
- **Cuando Deployamos**: ¿Comunique a mi equipo y al resto de las áreas interesadas (CX, Producto, Negocio)?, ¿evalué el impacto?, ¿tengo procesos de rollback?. ¿Tengo un requerimiento y/o evidencia asociada a ese pasaje?.
- **Al gestionar**: ¿Tengo accesos y permisos que excedan mis funciones? ¿Me exime de responsabilidad?.

// ¿Como puedo mitigar un IT Risk?

Logs de auditorías

RCA / Post Mortem

Definiendo Indicadores

Control de accesos (sobre todo los fallidos)

Capacitaciones / Trainings

DRPs

Utilizando bases securizadas

Testeando

Comunicando a Stakeholders

Segregar / separar las funciones según rol / área

Gracias.

Nos podes encontrar en
Slack (#IT-Risk) y Workplace (Risk & Compliance)

IT BOARDING
BOOTCAMP

// Schedule

IT Risk

01 Context

02 IT Governance

03 Compliance

04 Riesgos TI

05 IT Risk CID

Código de Ética

IT BOARDING
BOOTCAMP

// Capítulos clave del CDE

Código de Ética

CONFIDENCIALIDAD

Identificamos y resguardamos la información confidencial a la que tenemos acceso.

ACTIVIDADES LABORALES EXTERNAS

Realizamos actividades externas con responsabilidad y no competimos con Mercado Libre

DERECHOS DE PROPIEDAD INTELECTUAL

Acuerdo sobre los derechos de propiedad intelectual, datos personales, derecho de voz e imagen.

Tod@s somos responsables del cumplimiento del Código de Ética

Compliance

// Qué es?

- Procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan.
- Establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos.
- Riesgos a prevenir -> Aquellos que conllevan consecuencias como:
  - El daño reputacional.
  - La imposición de importantes multas y sanciones.
  - Las pérdidas de negocio / licencias

OWASP
Open Web Application Security Project

IT Governance

// Regulaciones y Frameworks

CIS Center for Internet Security
CIS Controls

COBIT 5
AN ISACA FRAMEWORK

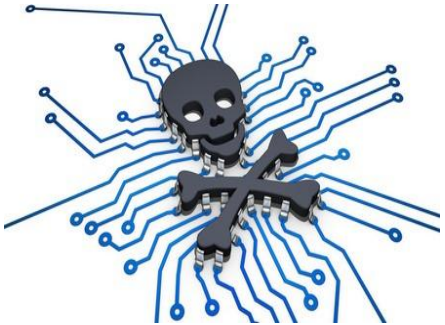
PCI DSS COMPLIANT

NIST
National Institute of Standards and Technology

ISO 27001

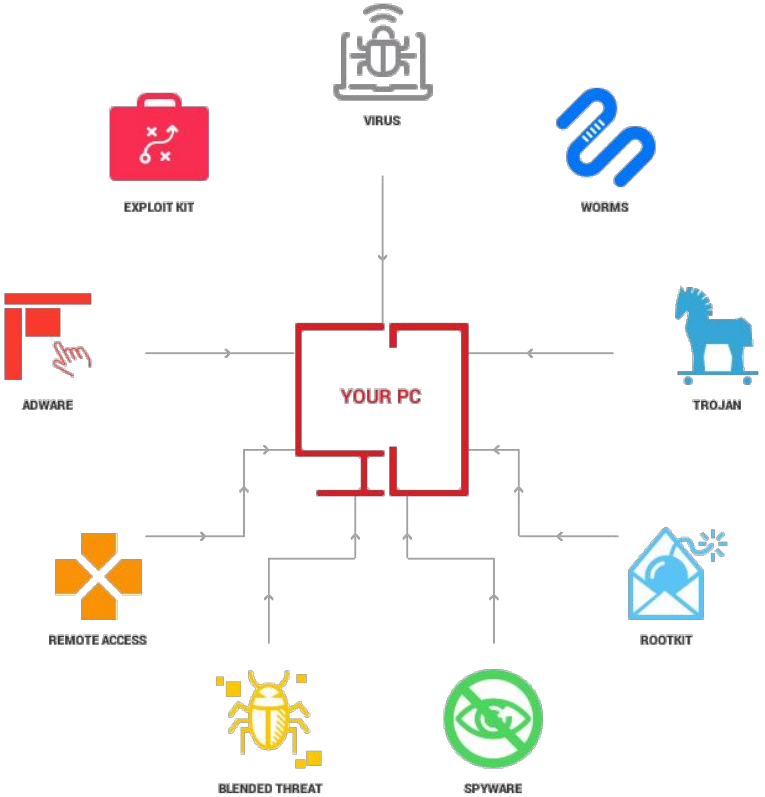
Malware

// Qué es?



MALWARE:

Todo tipo de programa o código informático malicioso que tenga como propósito dañar a un sistema o provocar un mal funcionamiento del mismo



Siguiente

Infección

// Ransomware

1

Un usuario abre un correo electrónico con un enlace o archivo adjunto malicioso

El malware se propaga a otras computadoras de la red.

2

PROPAGACIÓN

ENCRIPCIÓN

3

Comienza la encriptación

Se entrega la nota de rescate al usuario

4

NOTIFICACIÓN

RECUPERACIÓN

5

Pago del rescate en Bitcoins o restauración mediante backup (si existe)

Siguiente

Estafas

// Compras online

01 LAS FOTOS NO SON REALES

Ninguna de las publicaciones del vendedor tienen fotos reales de los productos

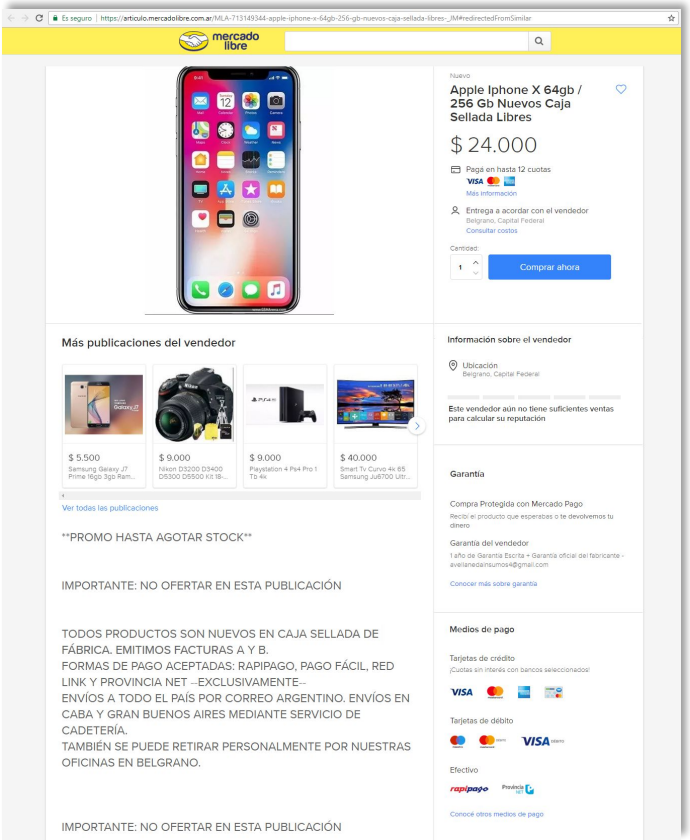
02 LA PUBLICACIÓN NO CUMPLE CON LAS NORMAS

Indica a los usuarios no realizar la compra mediante el sitio

03 EL VENDEDOR NO ES CONFIABLE

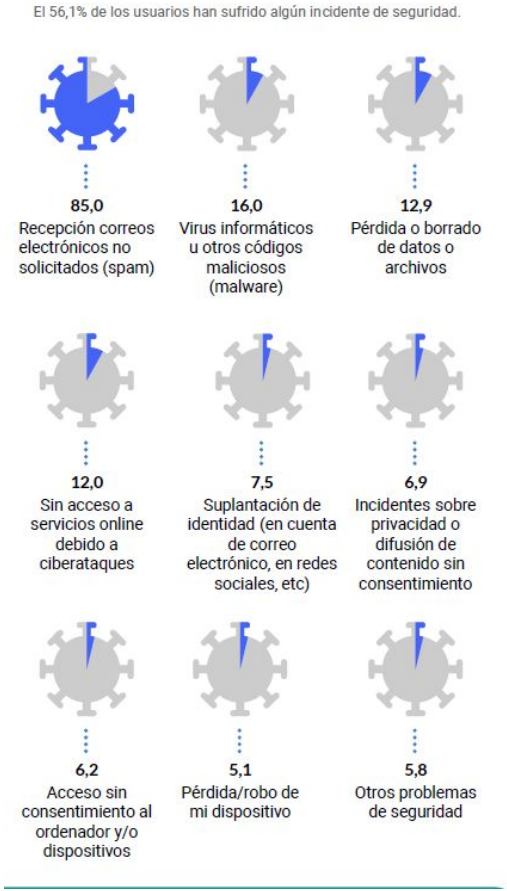
No posee suficientes ventas para mostrar su reputación en el sitio

Ofrece el contacto para la transacción en la sección GARANTÍA



Volver

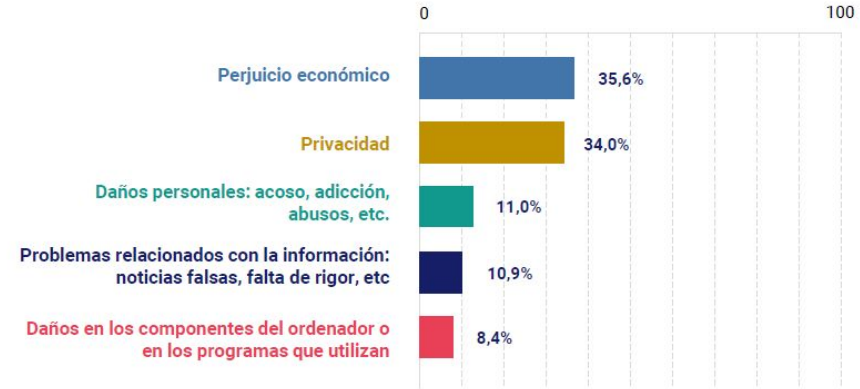
// Encuesta – España 2020



Fuente: ONTSI Enero-Junio 2020 https://www.ontsi.red.es/es/estudios-e-informes/Hogares-y-ciudadanos/Estudio-sobre-la-ciberseguridad-y-confianza-del-0

// Riesgos 2020 Usr final

¿A QUÉ RIESGOS DECLARAN ESTAR MÁS EXPUESTOS LOS INTERNAUTAS?



VALORACIÓN DE LOS PELIGROS AL NAVEGAR POR INTERNET
(Bastante o muy importante)

83,5%
Infección de malware en el equipo/dispositivo

82,2%
Acceso, compartición, pérdida o robo de archivos personales

79,4%
Cesión voluntaria de datos personales

67,1%
Cesión de información sobre hábitos, tendencias y usos de Internet

Fuente: ONTSI Enero-Junio 2020 https://www.ontsi.red.es/es/estudios-e-informes/Hogares-y-ciudadanos/Estudio-sobre-la-ciberseguridad-y-confianza-del-0

// IT BOOTCAMP

Intro General

- Que es compliance / porque hay regulaciones / empresa regulada (SOX / BACEN / LGPD)
- Porque tenemos equipos de riesgo / compliance / auditoria (explicaciòn)
- Porque es necesario nuestro rol

IT Risk

- Tipos de Riesgos: (Definición y ejemplos de cada uno)
  - Confidencialidad
  - Disponibilidad
  - Integridad
  - Performance
  - Compliance

- Riesgo de IT (No solo afecta de Soft/Hard!)
  - Brecha Seguridad (Dataleak, Ramsonware) / Downtimes / Compliance Reg
  - Tecnología Core Business: Clientes, Proveedores, Partners, Reguladores, Información Negocio.

// IT BOOTCAMP

Relacionado con el Código de Conducta:

- Manejo Seguro de Dispositivos / Apps / Información. Manejo Consciente del rol de Dev.
- Confidencialidad (Redes Sociales / Divulgación de Información Sensible)
- Propiedad del Código (Que es mío, que de Meli)

Relacionado con BAU del rol

- Estoy desarrollando lo que necesitamos o lo que entiendo/creo?
- Usuarios de Prueba en Entornos Productivos (Necesidad, Uso, Control, Trazabilidad, Impacto)
- Participación / Comunicación del usuario final en los planes de prueba
- Comunicación de Encendidos de Productos a las áreas de CX, Negocio, Producto.
- Permisos de Despliegue a Producción (Responsabilidad, Control, Impacto, Procesos de Rollback)
- Securitización de las APIS (AppSec)
- Integraciones con terceros (Autenticación, Cifrado)
- Código Confidencial no securizado (abierto al resto). Ej: Reglas de Fraude
- Segregación funciones (dentro la organización). Alertas, esto no exime responsabilidad
- Deployments sin requerimientos previos

// Conceptos Cubiertos x SecInf

Data Privacy

- Dataleak / Impacto Reputacional
- LGPD (Datos Personales) Personal Data Sensitive Data
- Privacy by Design (Información consumida y compartida desde y hacia las APIs)
- Database, que informacion resguardo, debo hacerlo? quien accede? hay bases vault donde consumirla?
- Creacion de Admins acceso información

AppSec

- Software Requirements, Software Design,Software Construction, Software Testing, Software Configuration Management and Software Monitoring
- Threat Modeling
- OWASP

WebSec

- Concepto Vulnerabilidad / Riesgo
- Manejo de Accesos Usuarios / Inputs de Usuarios y Monitoreo Actividad

// Risk Analysis

Riesgo -> Probabilidad de ocurrencia de un evento multiplicado por el impacto del mismo, en caso de que se materialice.

Elementos del riesgo:

- **Probabilidad** -> posibilidad de que un evento ocurra.
- **Amenazas** -> daño potencial asociado a una explotación de una vulnerabilidad.
- **Vulnerabilidad** -> falta o ausencia de control o debilidad de éste.

Tipos de controles:

- **Preventivos** -> intenta que incidente no ocurra. Por ej: procedimientos, clasificación de la información, control de accesos, contraseñas.
- **Detectivos** -> permite identificar incidentes potenciales. Por ej: logs de auditoría, alarmas.
- **Correctivos** -> mejora o arregla un sistema o componente de un servicio después de que incidente ocurrió. Por ej: imagen de windows en las estaciones de trabajo, Rollbacks.

Ayudarlos a identificar los riesgos y vulnerabilidades, reduciéndolos a un nivel aceptable e implementar mecanismos para mantener ese nivel.

// ¿Cuándo podría generar un riesgo?

Momento	Foco
Al programar	Confidencialidad - Integridad - Disponibilidad
Conectar algún device no segurizado en la Pc	Confidencialidad - Integridad
Compartir información sensible	Confidencialidad
Acceder dónde no correspondía por mi rol/función	Disponibilidad - Integridad
No testear antes de enviar a implementar	Performance - Disponibilidad
Subir el código fuente en plataformas no seguras ni de MeLi	Confidencialidad - Integridad
Utilizar datos de producción para el desarrollo (PII)	Confidencialidad
No enmascarar ni ofuscar datos	Confidencialidad - Compliance
Comunicar de a lista de distribución de forma incorrecta	Compliance
APIS abierta	Confidencialidad - Integridad - Compliance

// Código de Ética

IT BOARDING
BOOTCAMP

// Confidencialidad

Identificamos y resguardamos la información confidencial a la que tenemos acceso.

// Actividades laborales externas

Realizamos actividades externas con responsabilidad y no competimos con Mercado Libre

// Derechos de propiedad intelectual

Acuerdo sobre los derechos de propiedad intelectual, datos personales, derecho de voz e imagen.

// Participación en medios digitales

Somos responsables con nuestras opiniones y posteos en internet.

// Uso de internet, correos electrónicos y recursos

Hacemos un correcto uso de los accesos a herramientas, sistemas e información.