Riesgo Tecnológico

En el contexto de la Banca Nacional

Objetivos

Finalizado este taller deberá ser capaz de comprender :

Riesgo Tecnológico

- Reconocer los distintos tipos de riesgos de TI
- Comprender la importancia de la evolución del riesgo TI
- Como establecer controles adecuados para mitigar el riesgo de TI

La Nube Como Riesgo

A todos nos cuesta caer..

- Facebook
  - 1 Día
  - 11.7M
- Twitter
  - 1 Día
  - 20K

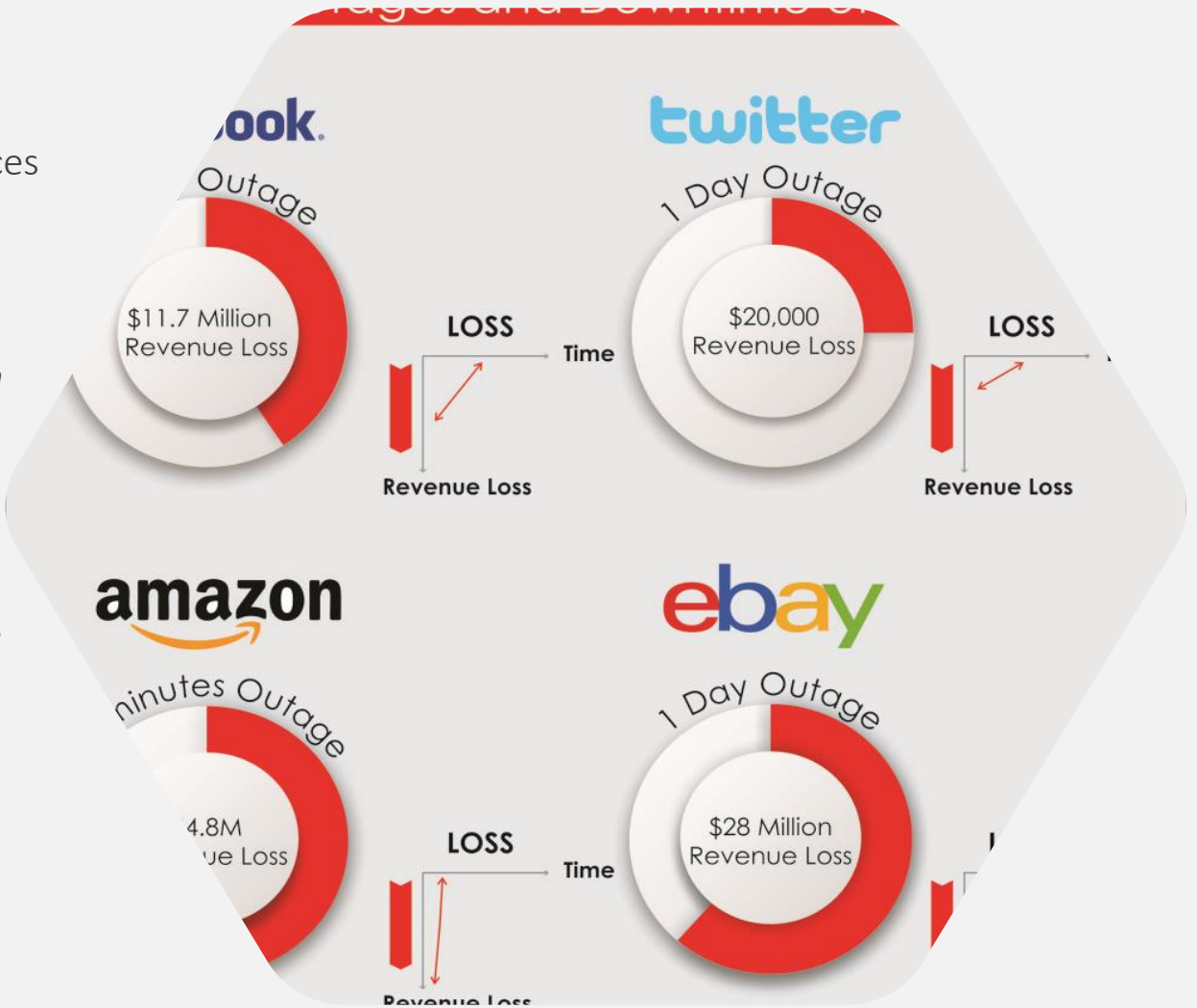
Amazon

- 40 Minutos
- 4.8M

- Ebay
  - 1 Día
  - 28M

La plataforma de servicios a terceros Amazon Webservices salió de servicio

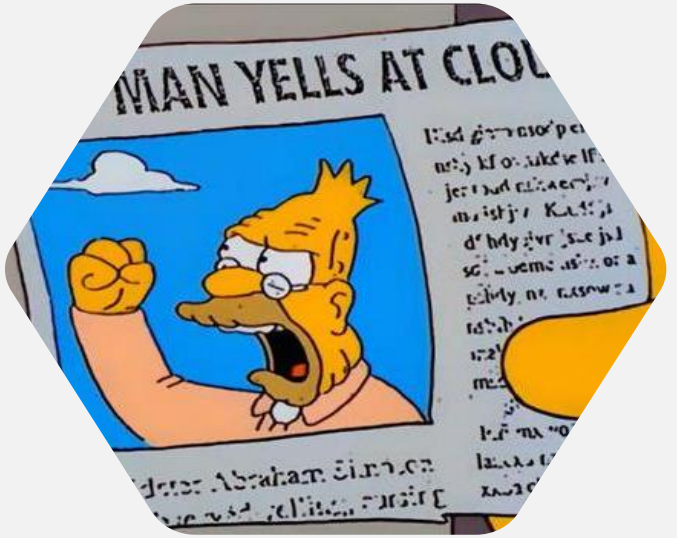
- Feb. 28 2017
- 100s websites offline
- SOP(*Standard Operation Procedure*)
- Comando mal digitado
- Un técnico ejecuto un cambio:
  - Modificar un servicio de un servidor
  - Aplicar el cambio
  - Reiniciar el equipo
  - Propagar el cambio
- El impacto fue colosal
  - 150M en perdida
  - El teclazo más caro del mundo https://n.pr/2A19k2K



Caso Amazon

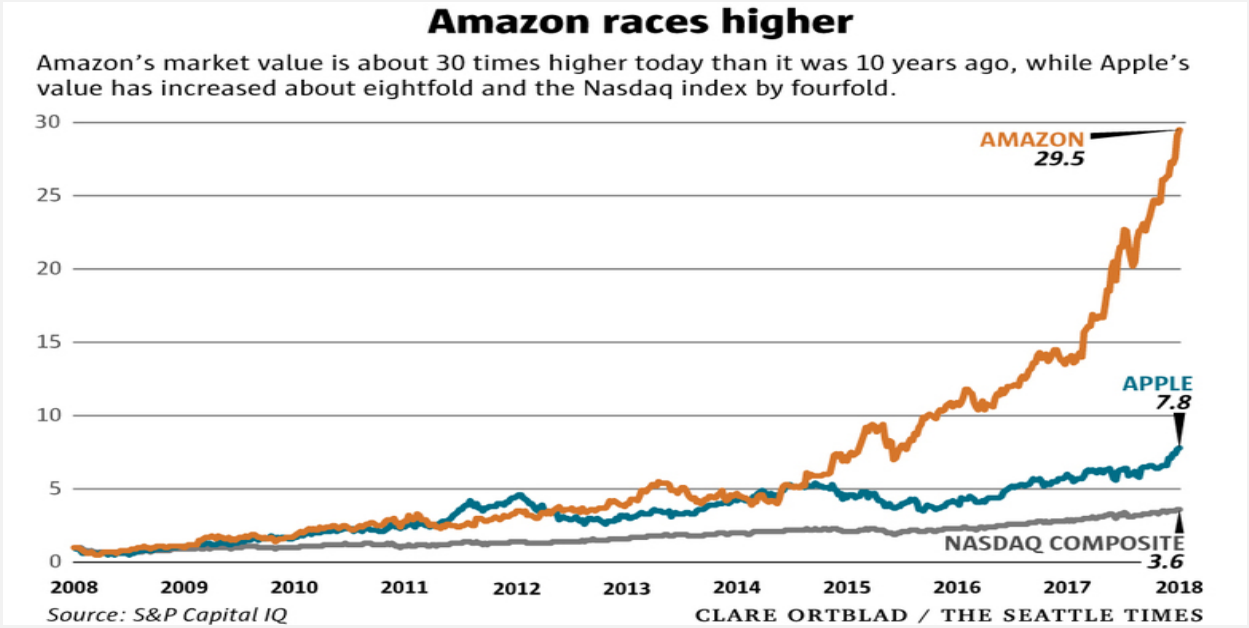
Tipos de Amenazas

- Accidental
  - Alguien se equivoco afectando el servicio
- Manejo de Riesgos de Empleados
  - Mantener un staff capacitado y al día
- Riesgo Operacional
  - Fallos de procesos y personal interno



Le puede pasar a Cualquiera…

- No es cuestión de dinero
  - Amazon vale por encima del Trillón de Dólares
  - US$ 1,000,000,000,000.00
- Todo falla en algún momento
  - No poner todos los huevos en una canasta
  - Siempre plan B, C, …,Z (YGTI -You Got The Idea)



Riesgo Tecnológico

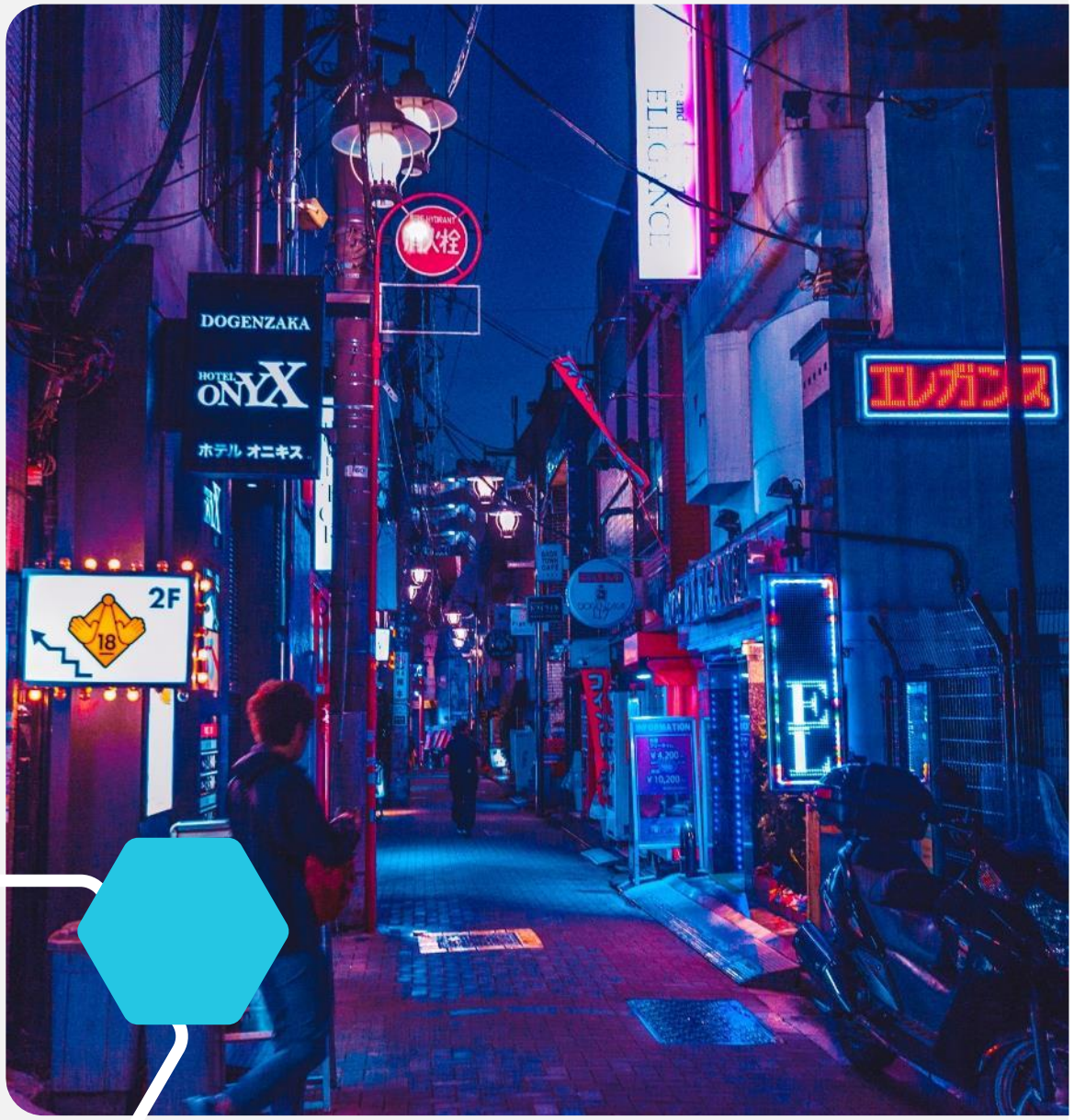
Es el riesgo derivado de la implementación de tecnologías de la información para llevar a cabo los procesos del negocio

Lo Básico

- Evitar
- Transferir
- Mitigar

Lo Difícil

- Aceptar



Evitar

El riesgo mas Seguro es el que no se asume.

Windows XP / Windows 7

- Fuera del ciclo de soporte
- Múltiples fallas de seguridad
- Usar WINDOWS 10

No siempre es posible evitar el riesgo

- Algunos procesos del negocio están intrínsecamente ligados a la tecnología – Tarjetas de Crédito
- La tecnología suele agregar un buen balance entre costo y beneficio – Economía de Escala
- Muchos de estos riesgos están bien estudiados y pueden asumirse con seguridad

Transferir

Es posible delegar en un tercero aquellos procesos que nos sean difíciles de manejar.

Servicios

- Infraestructura
  - Correo Electrónico
  - Recuperación de Desastres
    - Backup / Recuperación
    - Sitio Alterno
  - Archivado

Servicios en Línea

- Sistemas de Gestión
  - CRM – Manejo de Clientes
  - Paginas corporativas
  - Ambientes de Prueba
  - Análisis de Información

Seguros contra perdidas

Mitigar

El objetivo es reducir el riesgo a un nivel aceptable

Como…

- Agregando controles
  - DLP – Fuga de Información
  - Navegación – Proxy/Firewall
  - WebApp - WAF

Recuerde

- Nuestra meta no es eliminar todos los riesgos

Mitigación – Documentos Esenciales

	Planes	Descripcion	Ejemplos	Cuando	Periodo
IRP	Plan de Respuesta a Incidentes	Acciones que una organozacion toma durante un incidente	Listado de pasos a seguir durante el desastre Captura de Inteligencia, Análisis de Información	La ocurrencia de un incidente	Inmediatamente, reacción en tiempo real
DRP	Plan de Recuperación de Desastres	• Preparación en caso de ocurrir un desastre • Estrategia para limitar las perdidas antes y durante el desastre • Paso a paso de como volver a la normalidad	Procedimiento para la recuperación de la información Procedimiento para restablecer el servicio perdido Procedimiento de apagado para la protección de la data y los sistemas	Justo cuando el incidente se convierte en desastre	Recuperación en Poco tiempo
BPC	Plan de Continuidad de Negocios	Etapas para asegurar la continuidad del negocio cuando la escala del desastre sobrepasa la capacidad del DRP	Estepas de preparación para la activación del Segundo data center Establecimiento del sitio alterno en la localidad remota	Inmediatamente cuando el desastre amenace las operaciones del negocio	Largo Plazo

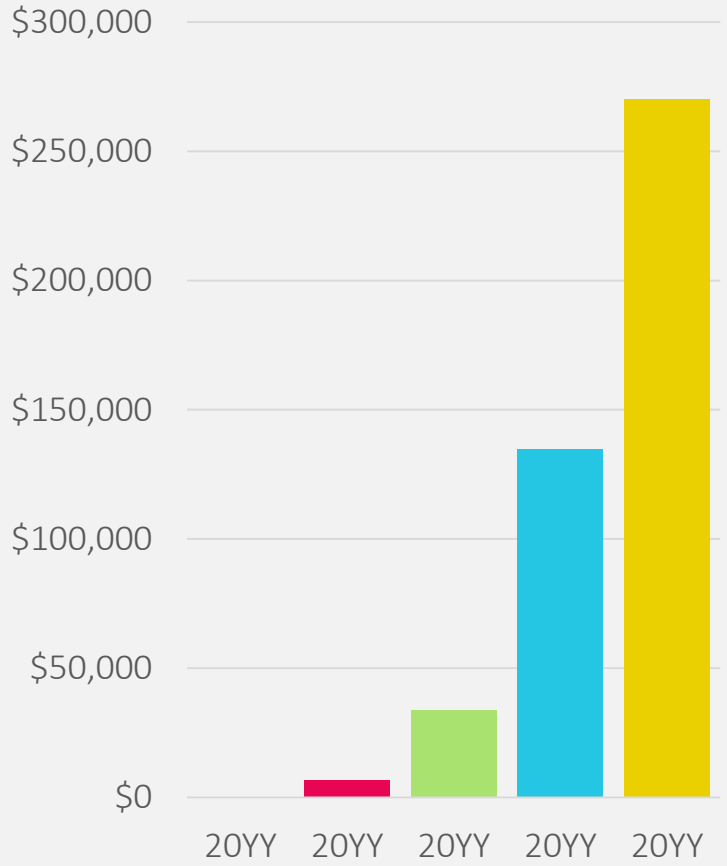
Herramientas

Forma de Abordar en riesgo de los procesos de Tecnología de la Información

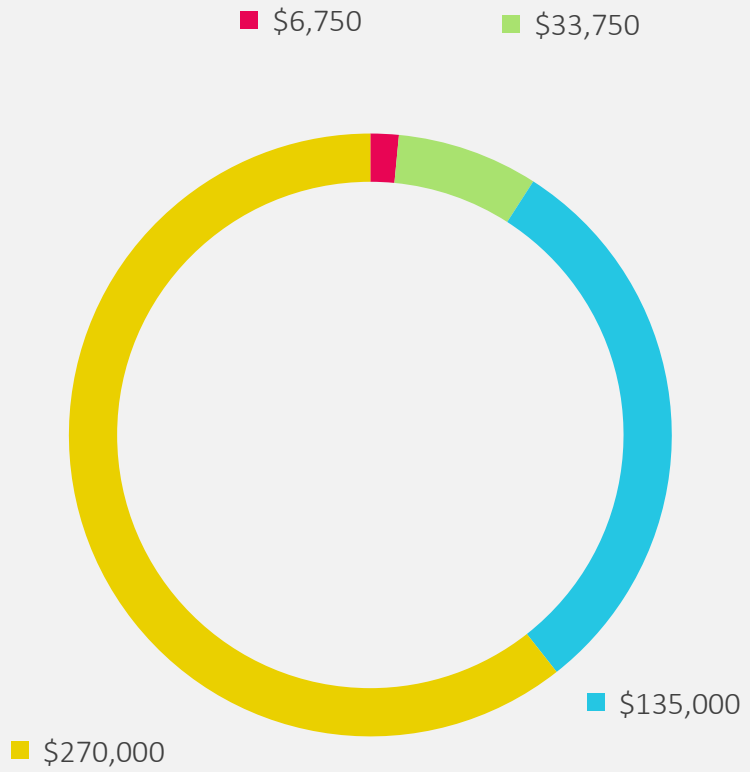
Análisis de Incidentes

Es importante dar seguimiento a la efectividad de los controles

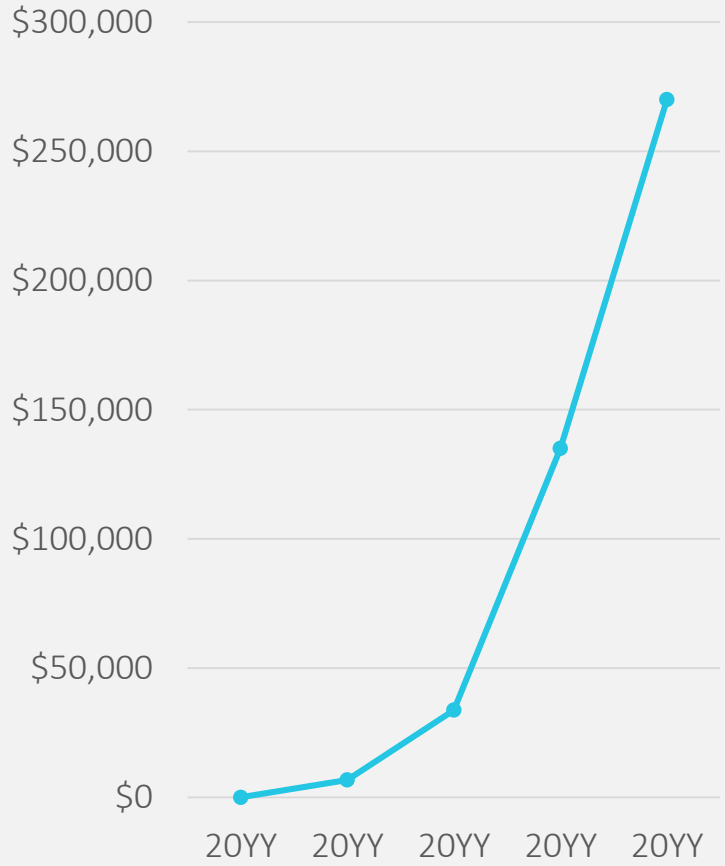
Costo Anual de Incidentes



Brechas de Seguridad



Inversión en Riesgo TI



Herramientas para Gestión de Riesgo TI

Marcos de Referencia

- COBIT – *Gobierno TI*
- ITIL – *Procesos TI*
- ISO 27000 – Serie – *Seguridad TI*
- BASILEA – *Cumplimiento*
- COSO - *Cumplimiento*
- TOGAF – *Arquitectura TI*
- ZACHMAN – *Arquitectura TI*
- NIST - *Ciberseguridad*
- OCTAVE – *Inventario de Activos*
- BIA – *Análisis de Vulnerabilidades*
- CMMI - *Diseño de Procesos*
- PCI-DSS – *Industria de Tarjetas*

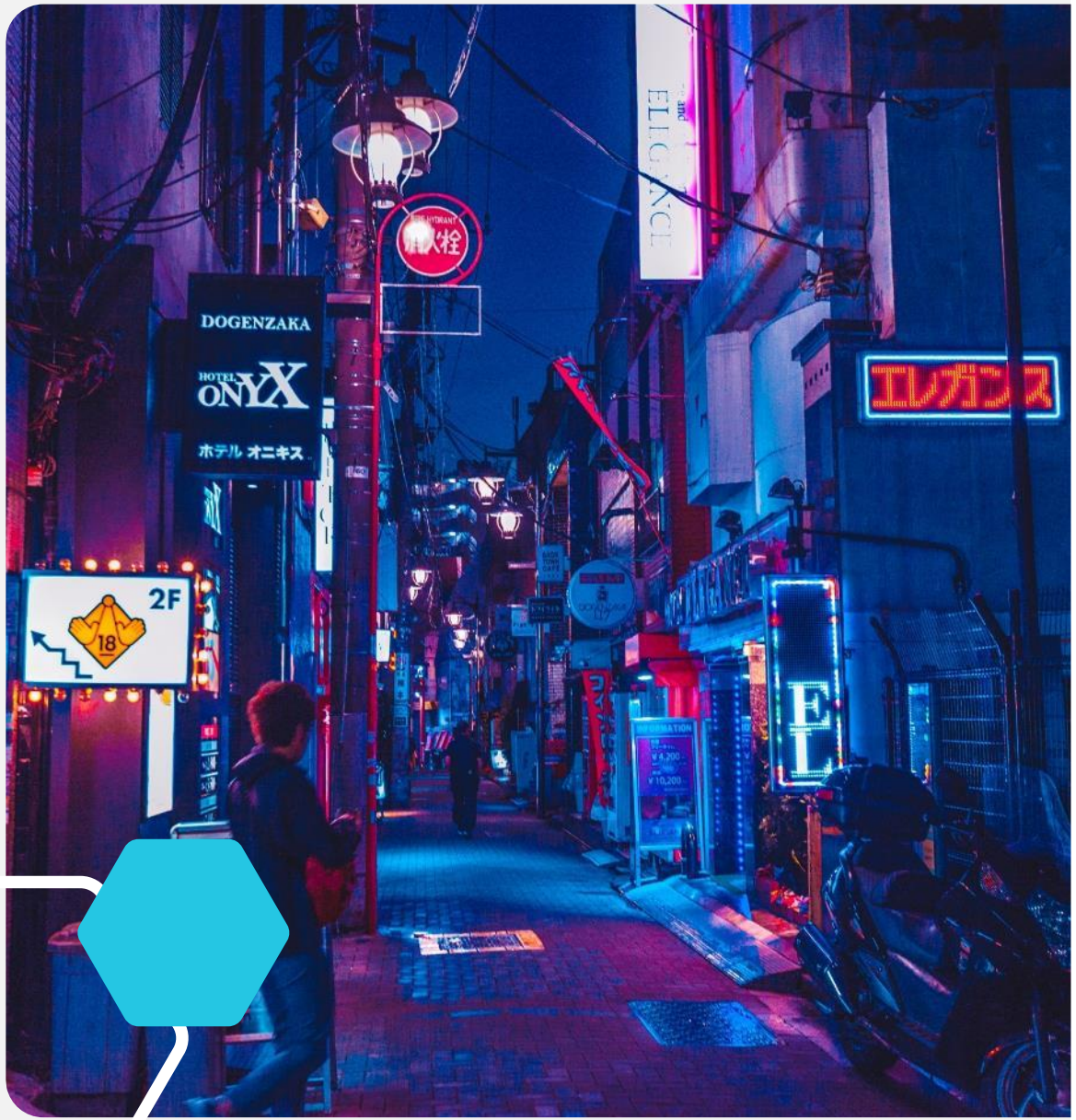
Legislation

Marco Regulatorio

También existe de forma local un régimen que exige cumplimiento

Legislación Especifica

- Ley de Protección de Datos
  - Habeas Data
- Ley Contra Delitos de Alta Tecnologia
- Ley Monetaria y Financiera
  - Reglamento de Riesgo Operacional
    - Riesgo Tecnológico
- Decreto 230-18 Estrategia Nacional de Ciberseguridad
  - Reglamento de Ciberseguridad
    - Instructivo



Estado Actual

Elaboración de Respuestas para Remitir

Guía de Autoevaluación

- Responsables - CISO / Riesgo
  - Postura de la Entidad
  - Acciones puntuales
  - Evidencias
  - Circular SIB -05/20
  - Portal - https://HEC.amf.gov.do

Recuerde

- Todos Somos responsables de la seguridad del Sistema Financiero
- Pero alguien debe ejecutar las tareas

Ningún rincón del Mundo es una Isla cuando esta interconectado

Gracias

Jose Cleto

+1 809 851 8809

josecleto@gmail.com

Linkedin: josecleto