DIGITAL CX Forum

19 mayo 2020

Oscar Lazcano

Director General

Aslo

Consejos para migrar al trabajo remoto y operaciones en la nube, sin riesgos de seguridad

imt.

SEGURIDAD

PRODUCTIVIDAD

CONTROL

CONTINUIDAD

DESEMPEÑO

- SEGURIDAD
- CONTINUIDAD
- CONTROL
- PRODUCTIVIDAD
- DESEMPEÑO

ACTIVIDADES ESENCIALES

INSUMOS MÉDICOS

INSUMOS MÉDICOS

VENTAS

INSUMOS

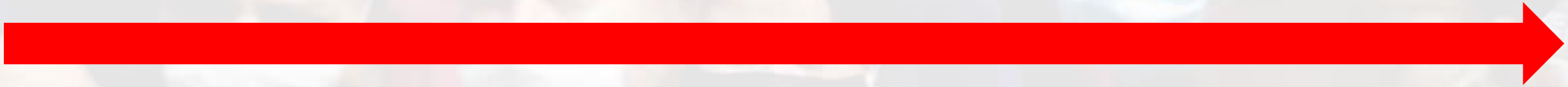
ATENCIÓN AL CLIENTE

EFICIENCIA

CALIDAD

RECURSOS PROPIOS

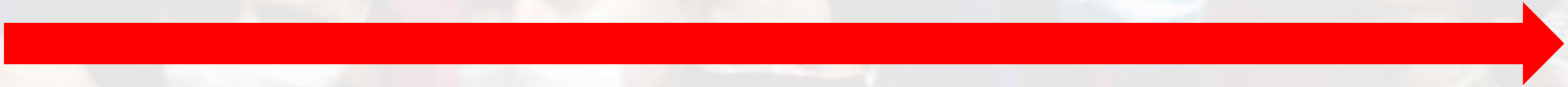
TECNOLOGÍA



INSUMOS MÉDICOS

CRM	VENTAS
ERP	INSUMOS
CONTACT CENTER	ATENCIÓN AL CLIENTE
OT / IoT	EFICIENCIA
COMPLIANCE	CALIDAD
ALL-AS-A-SERVICE	RECURSOS PROPIOS

TECNOLOGÍA



TECNOLOGÍA

RIESGO

AHORRO

- CRM
- ERP
- CONTACT CENTER
- OT / IoT
- COMPLIANCE
- ALL-AS-A-SERVICE

RIESGO

DISCLAIMER

DESCARGO DE RESPONSABILIDAD


oscar@aslo.us


@ORLazcano


in/oscar-lazcano

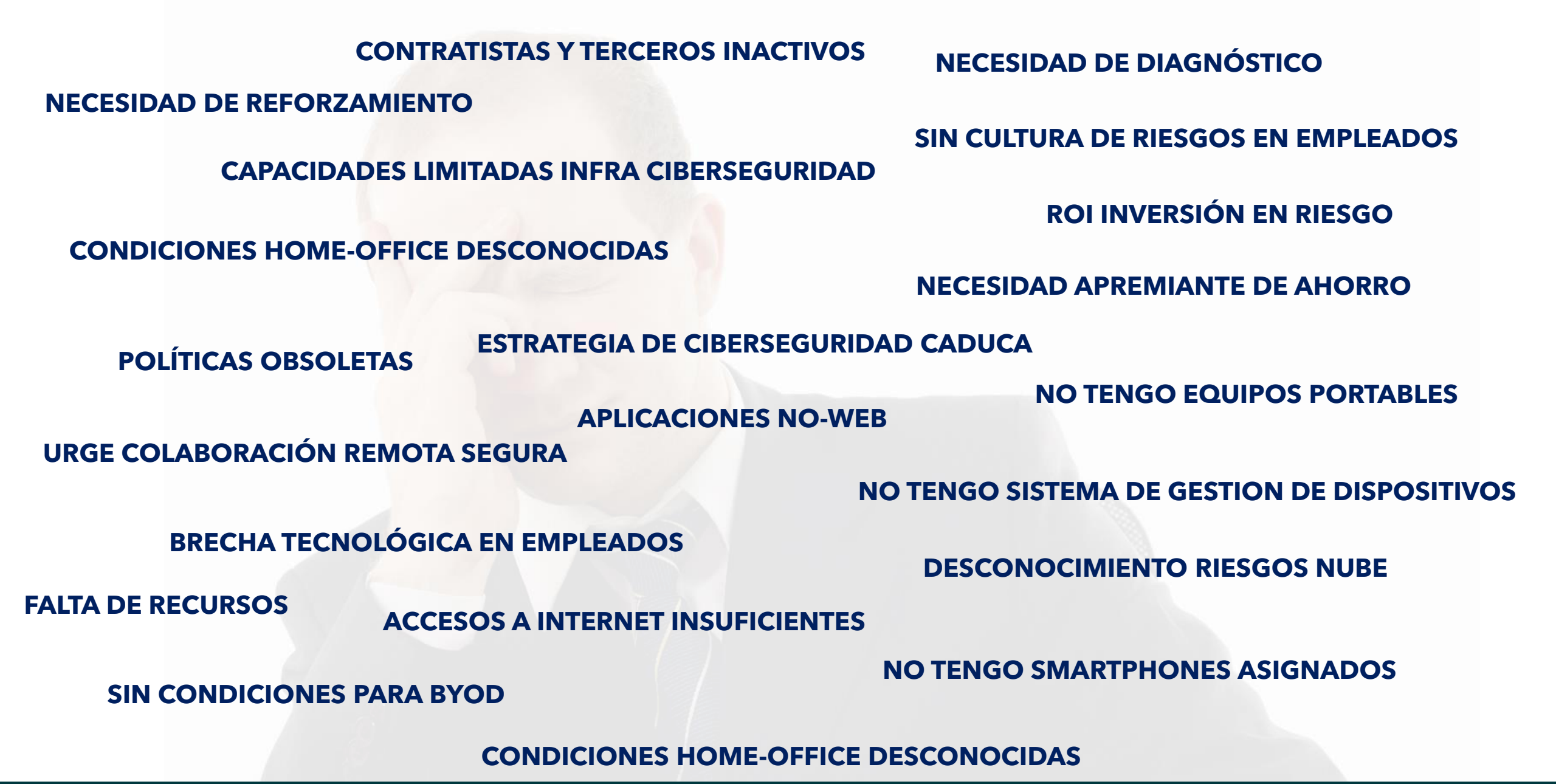

3316706563


oscar.lazcano

https://www.aslo.us/digitalCX

SEGURIDAD – COSTO – DESEMPEÑO

99.99% TIEMPO


CONTRATISTAS Y TERCEROS INACTIVOS
NECESIDAD DE DIAGNÓSTICO
NECESIDAD DE REFORZAMIENTO
SIN CULTURA DE RIESGOS EN EMPLEADOS
CAPACIDADES LIMITADAS INFRA CIBERSEGURIDAD
ROI INVERSIÓN EN RIESGO
CONDICIONES HOME-OFFICE DESCONOCIDAS
NECESIDAD APREMIANTE DE AHORRO
ESTRATEGIA DE CIBERSEGURIDAD CADUCA
POLÍTICAS OBSOLETAS
NO TENGO EQUIPOS PORTABLES
APLICACIONES NO-WEB
URGE COLABORACIÓN REMOTA SEGURA
NO TENGO SISTEMA DE GESTION DE DISPOSITIVOS
BRECHA TECNOLÓGICA EN EMPLEADOS
DESCONOCIMIENTO RIESGOS NUBE
FALTA DE RECURSOS
ACCESOS A INTERNET INSUFICIENTES
NO TENGO SMARTPHONES ASIGNADOS
SIN CONDICIONES PARA BYOD
CONDICIONES HOME-OFFICE DESCONOCIDAS

CADENA DE VALOR

DESCRIBIR LAS ACTIVIDADES DEL NEGOCIO
IDENTIFICAR Y CATEGORIZAR PROCESOS

(Entender y ubicar mejor el riesgo)

ENTENDER LA CADENA DE VALOR

PRIMER PASO PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

CLOUD

ACCESO VIA INTERNET A SERVICIOS, APLICACIONES E INFORMACIÓN QUE NO RESIDEN O SE EJECUTAN PRIMARIAMENTE EN DISPOSITIVOS LOCALES.

CLOUD

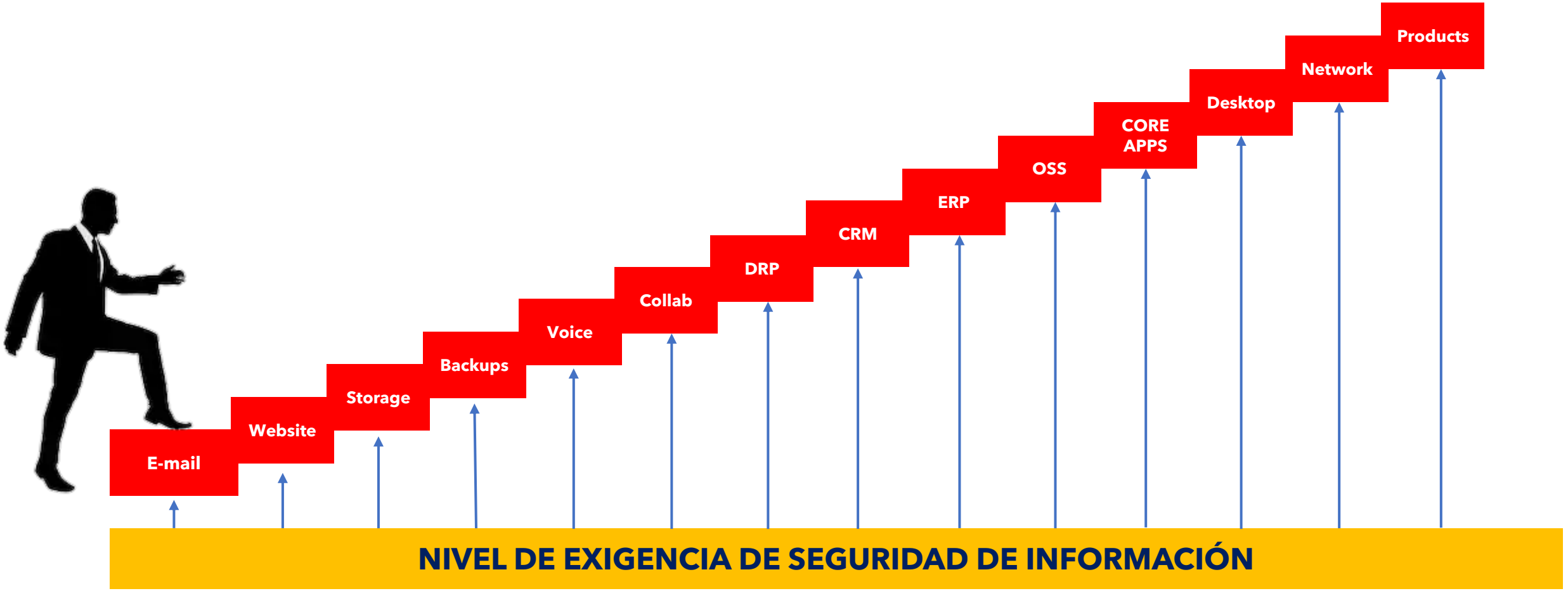
INFRAESTRUCTURA ELÁSTICA QUE PERMITE EL CONSUMO DE CONECTIVIDAD, CAPACIDAD DE PROCESAMIENTO Y ALMACENAMIENTO BAJO DEMANDA PARA EJECUTAR APLICACIONES Y ENTREGAR SERVICIOS.

CLOUD

MODELO DE NEGOCIO QUE PERMITE LA MONETIZACIÓN Y EL CONSUMO DE APLICACIONES "COMO SERVICIO" ELIMINANDO REQUERIMIENTOS DE INVERSIONES CAPEX Y HABILITANDO UN TCO MUCHO MAS BAJO PARA LAS EMPRESAS.

CLOUD

DE LA OPTIMIZACIÓN A LA TRANSFORMACIÓN



- Todos acuden a la oficina a trabajar
- Mayoría de equipos son de escritorio
- Aplicaciones Cliente-Servidor en LAN
- Aplicaciones no optimizadas para Web
- Telefonía TDM. No Softphones. No headsets.
- Seguridad Internet: Website + Filtrado de Contenido
- Ciberseguridad: Antivirus / UTM
- Sin políticas de trabajo remoto
- Innovación costosa y lenta

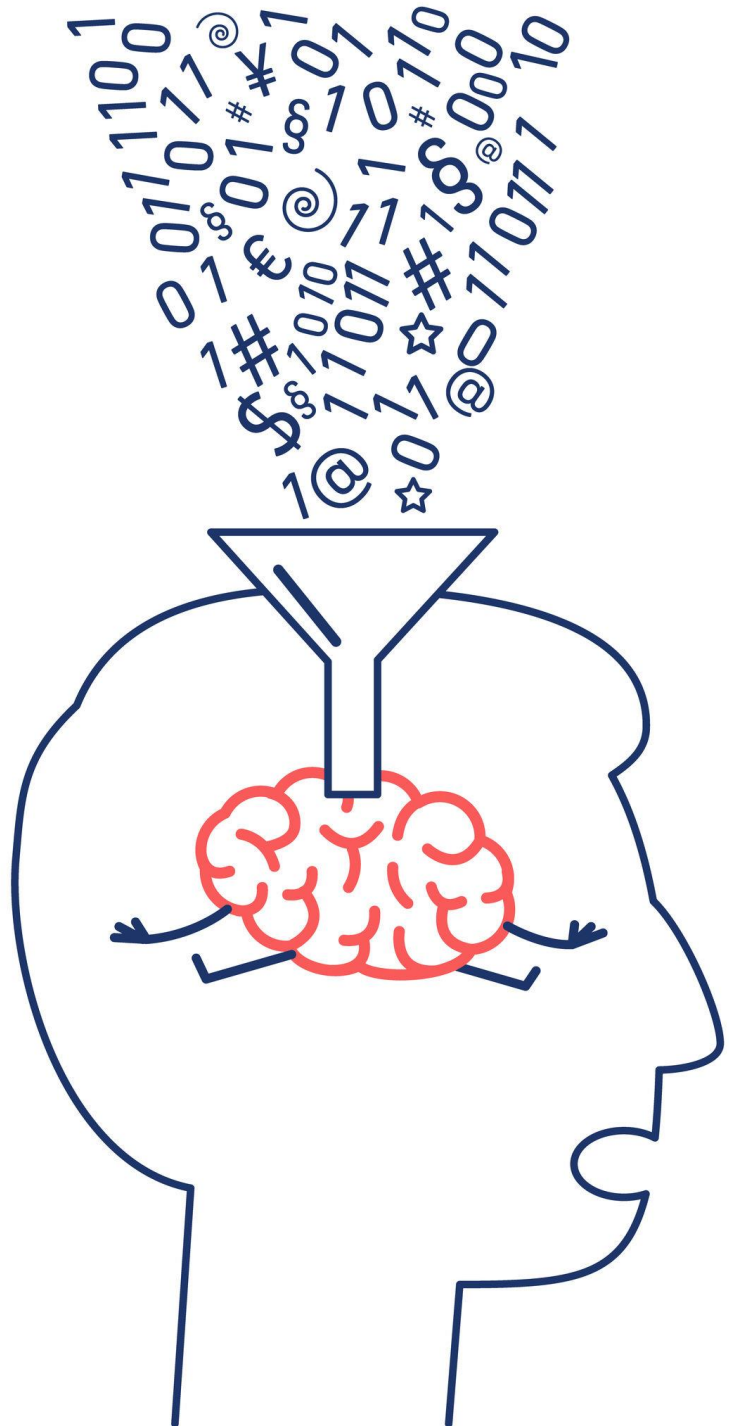
Empresas 100% On-Premise

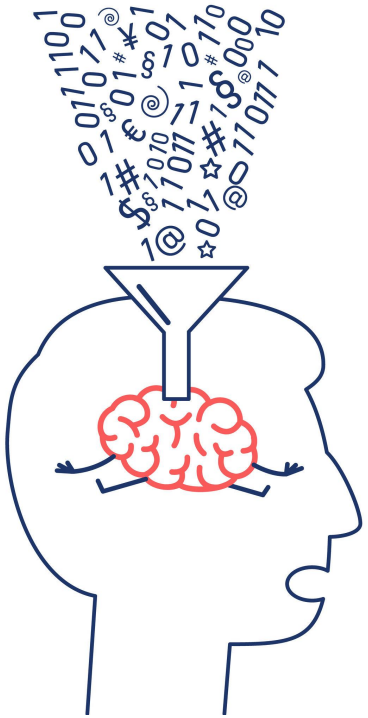
Empresas 100% CLOUD

- Sin dependencia del espacio físico para usar recursos.
- Estén en donde estén, acceden de la misma forma.
- Todos tienen equipo móvil y portable.
- Pueden medir uso del tiempo y productividad por usuario.
- Pueden identificar y frenar amenazas a datos, video y telefonía.
- Pueden comprobar identidad de usuarios y dispositivos.
- Segmentación de apps, red y recursos en nube.
- Demuestran cumplimiento de seguridad de información
- Ajustan su tamaño en función de las exigencias del mercado.
- Son ágiles para desplegar nuevos servicios al mejor costo.

https://bit.ly/2yjZ0lE

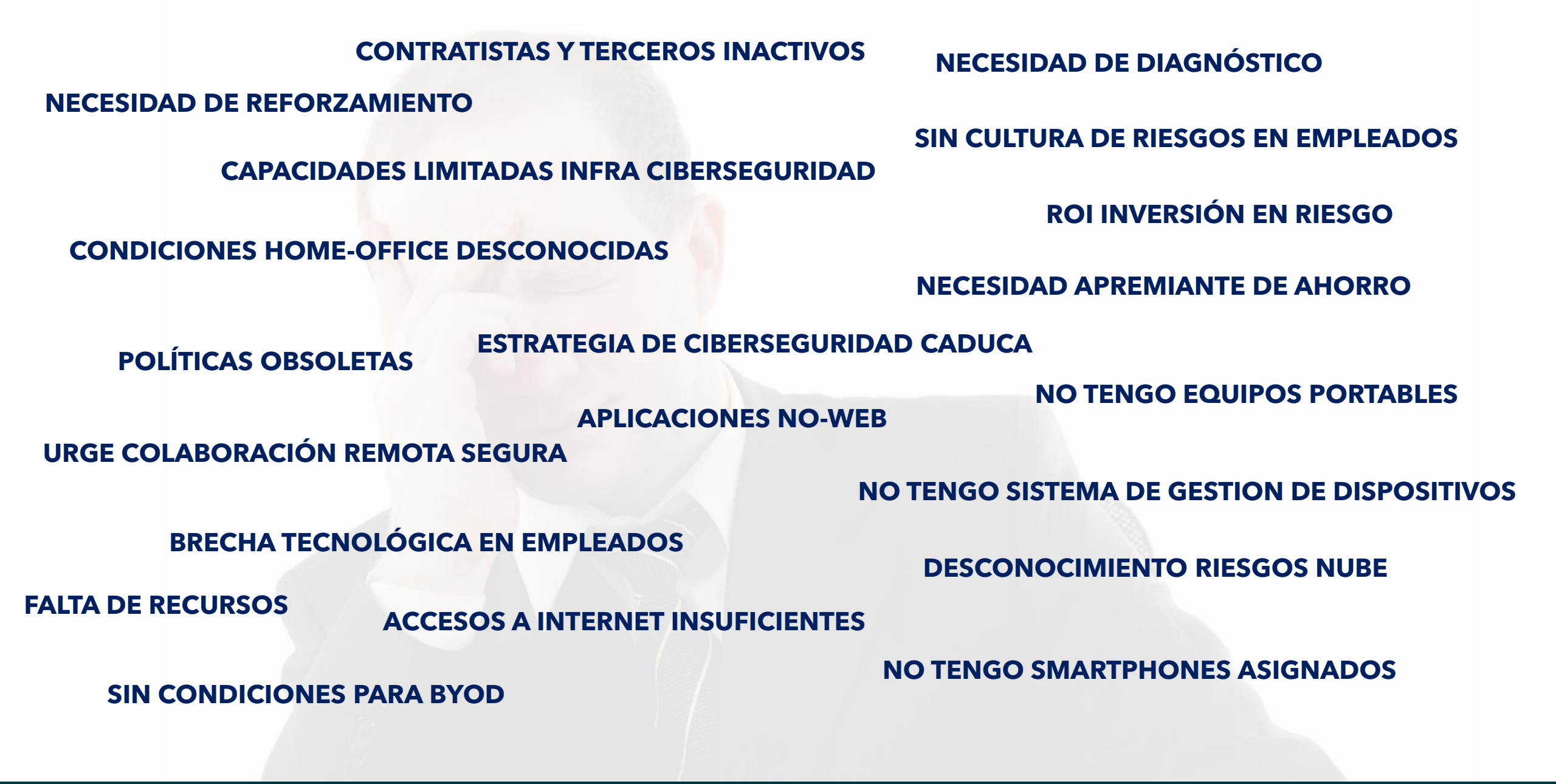
SIMPLIFICAR PARA ASEGURAR





30-60 Días

3 años


CONTRATISTAS Y TERCEROS INACTIVOS
NECESIDAD DE DIAGNÓSTICO
NECESIDAD DE REFORZAMIENTO
SIN CULTURA DE RIESGOS EN EMPLEADOS
CAPACIDADES LIMITADAS INFRA CIBERSEGURIDAD
ROI INVERSIÓN EN RIESGO
CONDICIONES HOME-OFFICE DESCONOCIDAS
NECESIDAD APREMIANTE DE AHORRO
ESTRATEGIA DE CIBERSEGURIDAD CADUCA
POLÍTICAS OBSOLETAS
NO TENGO EQUIPOS PORTABLES
APLICACIONES NO-WEB
URGE COLABORACIÓN REMOTA SEGURA
NO TENGO SISTEMA DE GESTION DE DISPOSITIVOS
BRECHA TECNOLÓGICA EN EMPLEADOS
DESCONOCIMIENTO RIESGOS NUBE
FALTA DE RECURSOS
ACCESOS A INTERNET INSUFICIENTES
NO TENGO SMARTPHONES ASIGNADOS
SIN CONDICIONES PARA BYOD

DEBILIDADES

- APLICACIONES NO-WEB
- ACCESOS A INTERNET INSUFICIENTES
- CAPACIDADES LIMITADAS INFRA CIBERSEGURIDAD
- BRECHA TECNOLÓGICA EN EMPLEADOS
- NO TENGO EQUIPOS PORTABLES
- NO TENGO SMARTPHONES ASIGNADOS
- NO TENGO SISTEMA DE GESTION DE DISPOSITIVOS
- POLÍTICAS OBSOLETAS
- NECESIDAD DE DIAGNÓSTICO
- FALTA DE RECURSOS

AMENAZAS

- CONTRATISTAS Y TERCEROS INACTIVOS
- CONDICIONES HOME-OFFICE DESCONOCIDAS
- DESCONOCIMIENTO RIESGOS NUBE
- NECESIDAD APREMIANTE DE AHORRO
- ESTRATEGIA DE CIBERSEGURIDAD CADUCA
- SIN CULTURA DE RIESGOS EN EMPLEADOS
- ROI INVERSIÓN EN RIESGO
- URGE COLABORACIÓN REMOTA SEGURA
- NECESIDAD DE REFORZAMIENTO
- SIN CONDICIONES PARA BYOD

REQUERIMIENTOS

Optimización de Aplicaciones y Sistemas

APLICACIONES NO-WEB

URGE COLABORACIÓN REMOTA SEGURA

Reforzamiento de Infraestructura de Red

ACCESOS A INTERNET INSUFICIENTES

ROI INVERSIÓN EN RIESGO

Adquisición y Control de Endpoints

NO TENGO EQUIPOS PORTABLES

NO TENGO SMARTPHONES ASIGNADOS

NO TENGO SISTEMA DE GESTION DE DISPOSITIVOS

Eficiencia

NECESIDAD APREMIANTE DE AHORRO

Reforzamiento de Infraestructura de Ciberseguridad

CAPACIDADES LIMITADAS INFRA CIBERSEGURIDAD

ESTRATEGIA DE CIBERSEGURIDAD CADUCA

CONDICIONES HOME-OFFICE DESCONOCIDAS

CONTRATISTAS Y TERCEROS INACTIVOS

NECESIDAD DE REFORZAMIENTO

Gobernanza y Cumplimiento

POLÍTICAS OBSOLETAS

NECESIDAD DE DIAGNÓSTICO

SIN CONDICIONES PARA BYOD

FALTA DE RECURSOS

Entrenamiento, Capacitación y Concientización

BRECHA TECNOLÓGICA EN EMPLEADOS

DESCONOCIMIENTO RIESGOS NUBE

SIN CULTURA DE RIESGOS EN EMPLEADOS

TECNOLOGÍA CLOUD

Reforzamiento de Infraestructura de Red

Routing & Switching

Software-defined WAN (SD-WAN)

Optimización de Aplicaciones y Sistemas

Infrastructure-as-a-Service (IaaS)

Virtual Desktop Infrastructure (VDI)

Unified Communications As-a-Service (UCaaS)

Enterprise Mobility

Adquisición y Control de Endpoints

Mobile Device Management (MDM)

Endpoint Security

Mobile Security

Identity Management (IdP)

Eficiencia

Telecom Expense Management

Reforzamiento de Infraestructura de Ciberseguridad

Network Security

Web Security

Application Security

E-mail Security

Deception

User and Identity Behavior Analytics

Fraud Detection & Prevention

Artificial Intelligence

Software-defined Perimeter

Zero-trust

Entrenamiento, Capacitación y Concientización

E-learning

Gobernanza y Cumplimiento

Compliance Mapping

Data Loss Prevention (DLP)

Cyber Intelligence – Threat Hunting

Cloud Matrix

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: AWS, GCP, Azure, Azure AD, Office 365, SaaS.

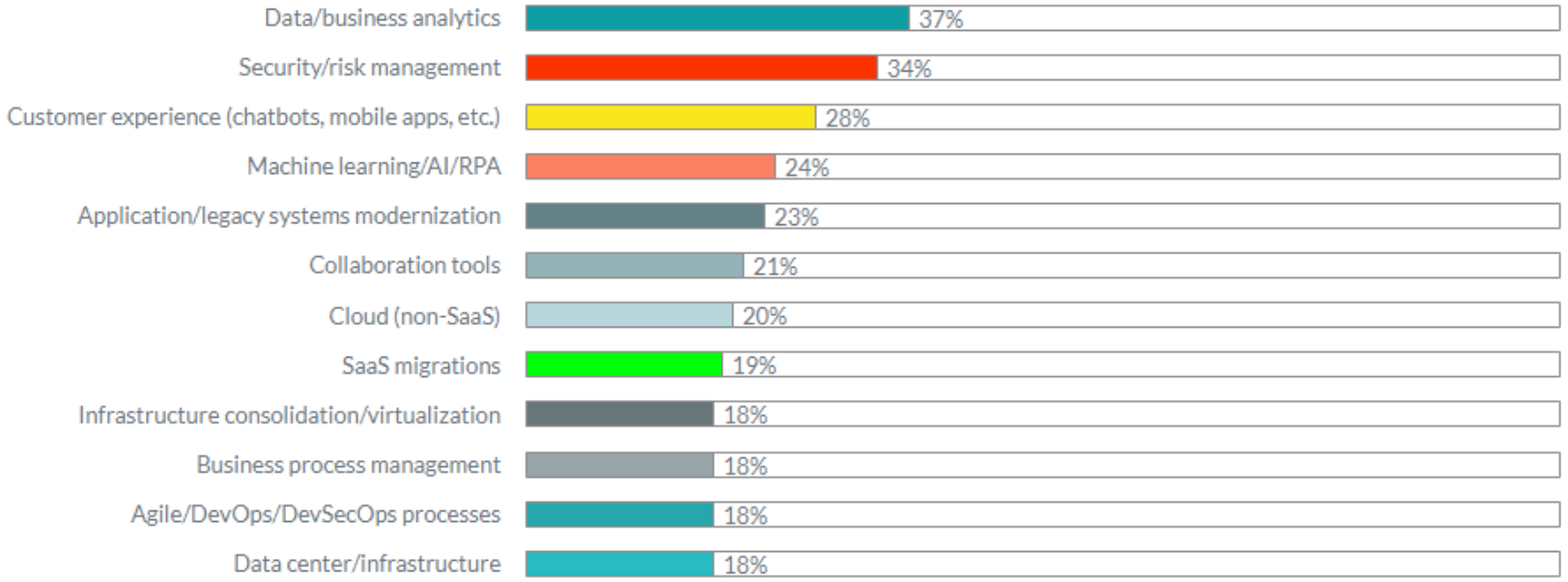
Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token	Network Share Discovery		Email Collection		
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie	Permission Groups Discovery				
					Remote System Discovery				
					System Information Discovery				
					System Network Connections Discovery				

https://attack.mitre.org/matrices/enterprise/cloud/

IT BUDGETING

DE LA OPTIMIZACIÓN A LA TRANSFORMACIÓN

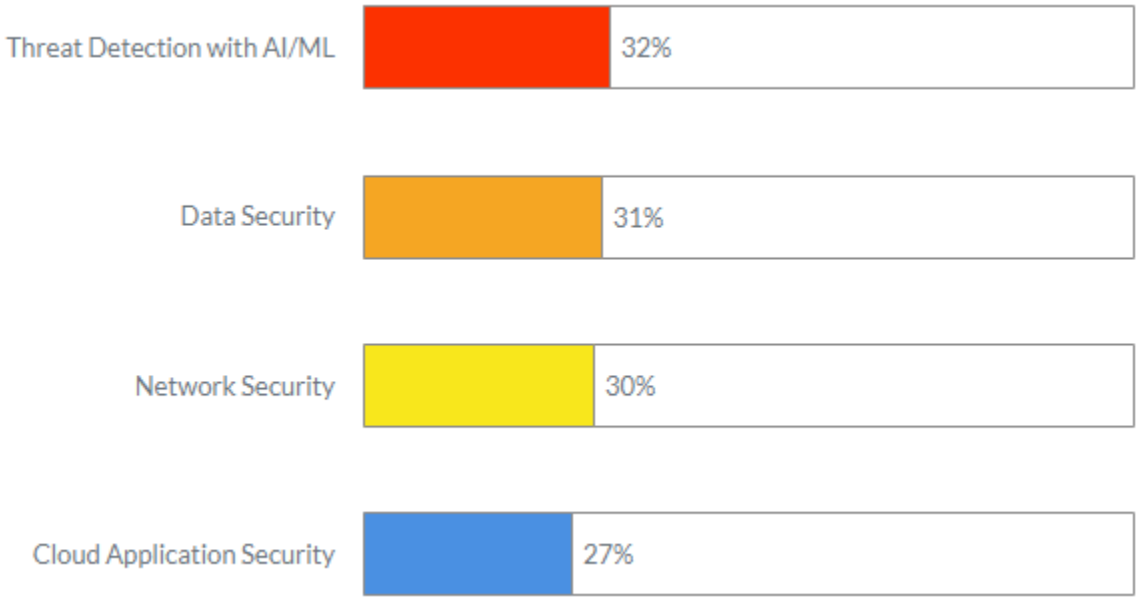


- ✓ **CUSTOMER ENGAGEMENT**
- ✓ **EMPLOYEE ENGAGEMENT**
- ✓ **CYBERSECURITY**

CIO **https://bit.ly/3bPjAYx**

SECURITY BUDGETING

DE LA OPTIMIZACIÓN A LA TRANSFORMACIÓN



- ✓ **Robo de Identidad de Usuarios / Dispositivos**
- ✓ **Hackeos / ej. Ransomware**
- ✓ **Concientización y Entrenamiento**
- ✓ **Multas y mala reputación**

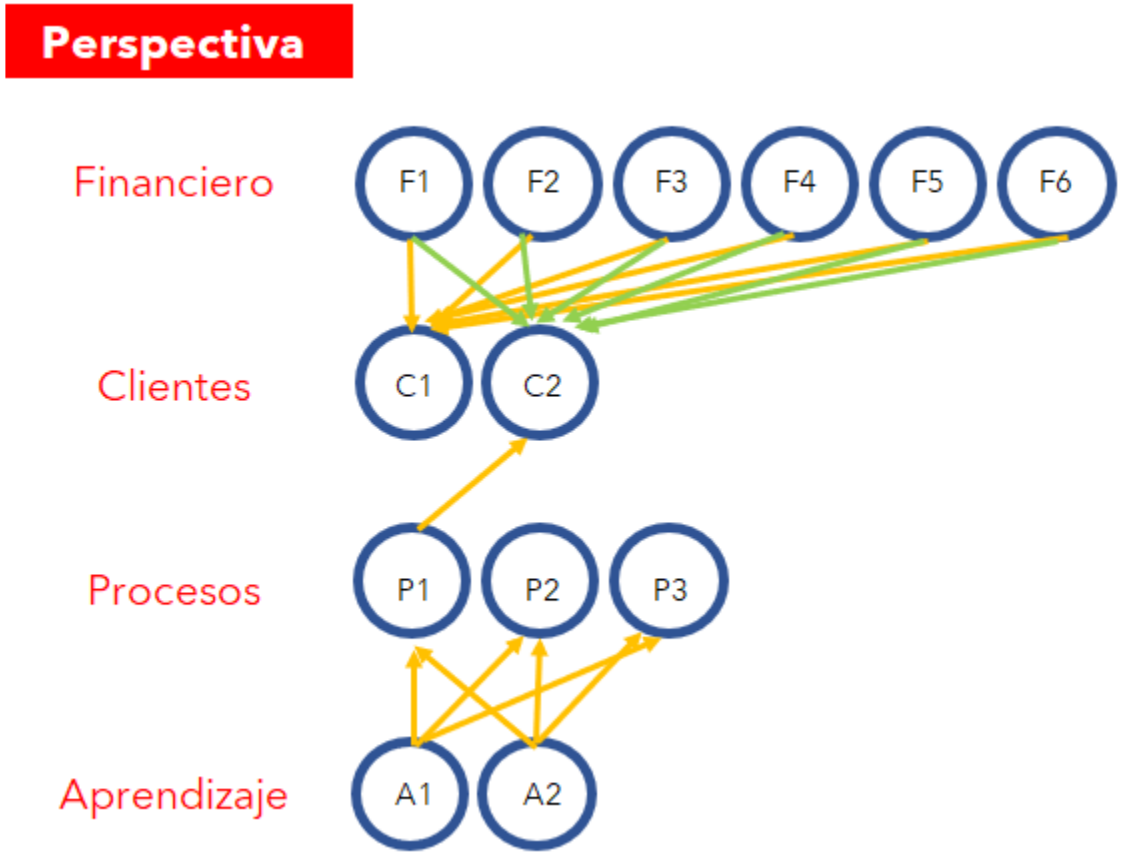
CSO **https://bit.ly/2TkIOYK**

RECOMENDACIONES

DE LA OPTIMIZACIÓN A LA TRANSFORMACIÓN

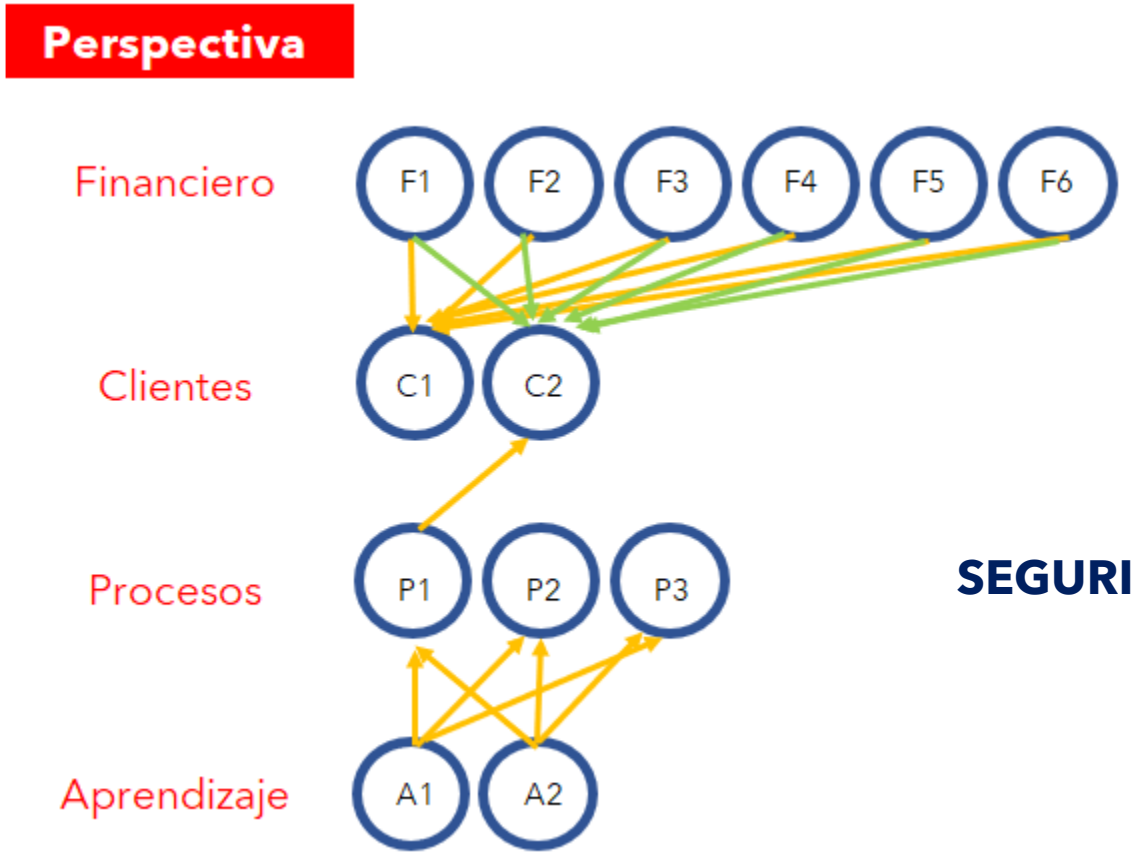
RECOMENDACIONES

DE LA OPTIMIZACIÓN A LA TRANSFORMACIÓN



RECOMENDACIONES

DE LA OPTIMIZACIÓN A LA TRANSFORMACIÓN



RENTABILIDAD / PREVENCIÓN PÉRDIDAS

CONFIANZA / PROTECCIÓN REPUTACIÓN

SEGURIDAD / DESEMPEÑO / CONTINUIDAD / DISPONIBILIDAD

CUMPLIMIENTO / CULTURA / CONCIENTIZACIÓN

DIGITAL CX Forum

ASLO INFORMATION TECHNOLOGIES

GRACIAS.