Ciberseguridad, convergencia TI TO y gestión de activos

CIMGA 2023

Pilar Valderrama

Agenda

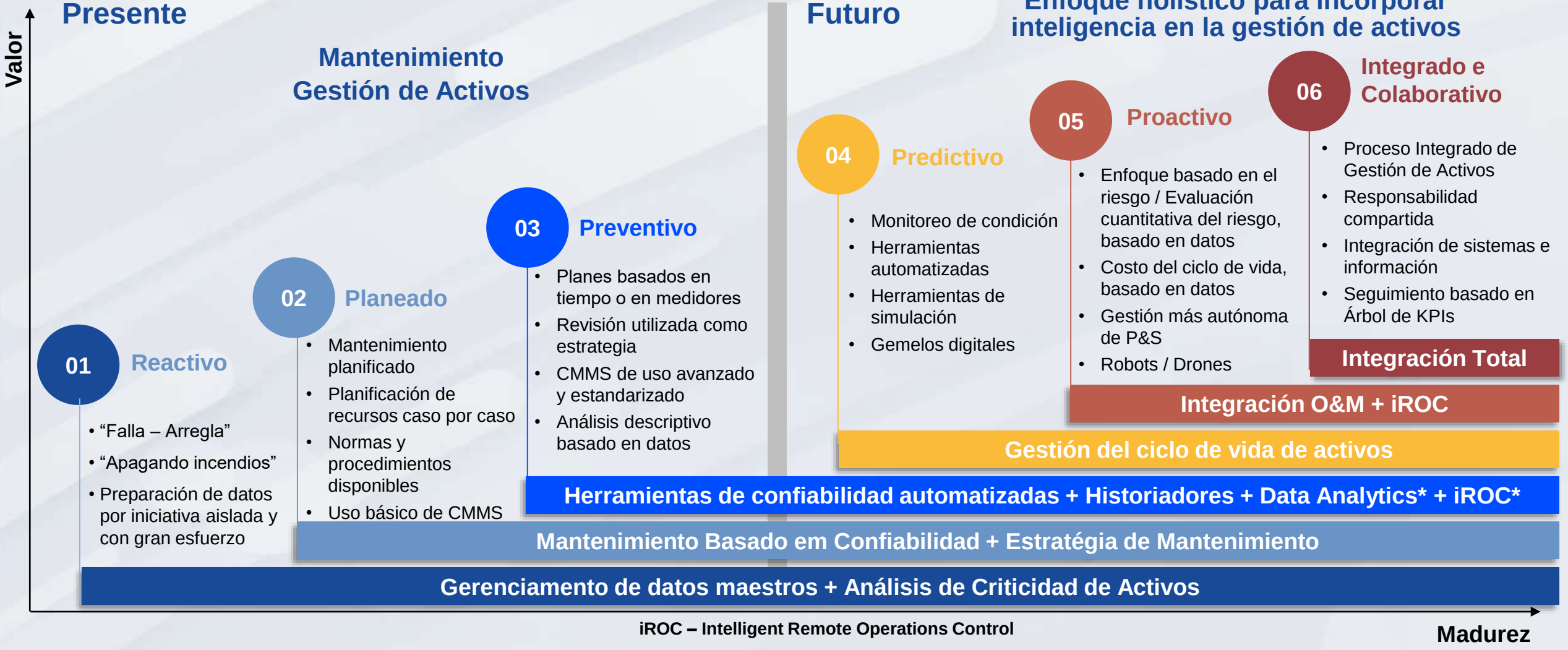
- Introducción
- Propósito
- Ciberseguridad
- IT / OT
- Convergencia
- Visión desde la Gestión de activos
- Conclusión

PILAR VALDERRAMA
Accenture Industry X
Pilar.valderrama@accenture.com

Casada, mamá de Verónika (7 años)
20 años de experiencia en Gestión de Activos y Mantenimiento
Fortuna de servir a diferentes industrias en Colombia, el Caribe, Australia y Latinoamérica

Estamos entrando en una era de Industria X, era de convergencia de tecnología de información y operación

Accenture Industry X


Presente
Futuro
Enfoque holístico para incorporar inteligencia en la gestión de activos
Mantenimiento Gestión de Activos
Valor
01 Reactivo
• "Falla – Arregla"
• "Apagando incendios"
• Preparación de datos por iniciativa aislada y con gran esfuerzo
02 Planeado
• Mantenimiento planificado
• Planificación de recursos caso por caso
• Normas y procedimientos disponibles
• Uso básico de CMMS
03 Preventivo
• Planes basados en tiempo o en medidores
• Revisión utilizada como estrategia
• CMMS de uso avanzado y estandarizado
• Análisis descriptivo basado en datos
04 Predictivo
• Monitoreo de condición
• Herramientas automatizadas
• Herramientas de simulación
• Gemelos digitales
05 Proactivo
• Enfoque basado en el riesgo / Evaluación cuantitativa del riesgo, basado en datos
• Costo del ciclo de vida, basado en datos
• Gestión más autónoma de P&S
• Robots / Drones
06 Integrado e Colaborativo
• Proceso Integrado de Gestión de Activos
• Responsabilidad compartida
• Integración de sistemas e información
• Seguimiento basado en Árbol de KPIs
Integración Total
Integración O&M + iROC
Gestión del ciclo de vida de activos
Herramientas de confiabilidad automatizadas + Historiadores + Data Analytics* + iROC*
Mantenimiento Basado em Confiabilidad + Estratégia de Mantenimiento
Gerenciamento de datos maestros + Análisis de Criticidad de Activos
iROC – Intelligent Remote Operations Control
Madurez

Agenda

- Introducción
- Propósito
- Ciberseguridad
- Convergencia
- Visión desde la Gestión de activos
- Conclusión

Propósito

- Proporcionar una idea de la importancia de la ciberseguridad, la convergencia entre TI y TO en la Gestión de Activos.

- Visión estratégica de cómo apalancarse en el SGA para mitigar riesgos y apalancar la evolución digital.

Agenda

- Introducción
- Propósito
- Ciberseguridad
- Convergencia
- Visión desde la Gestión de activos
- Conclusión

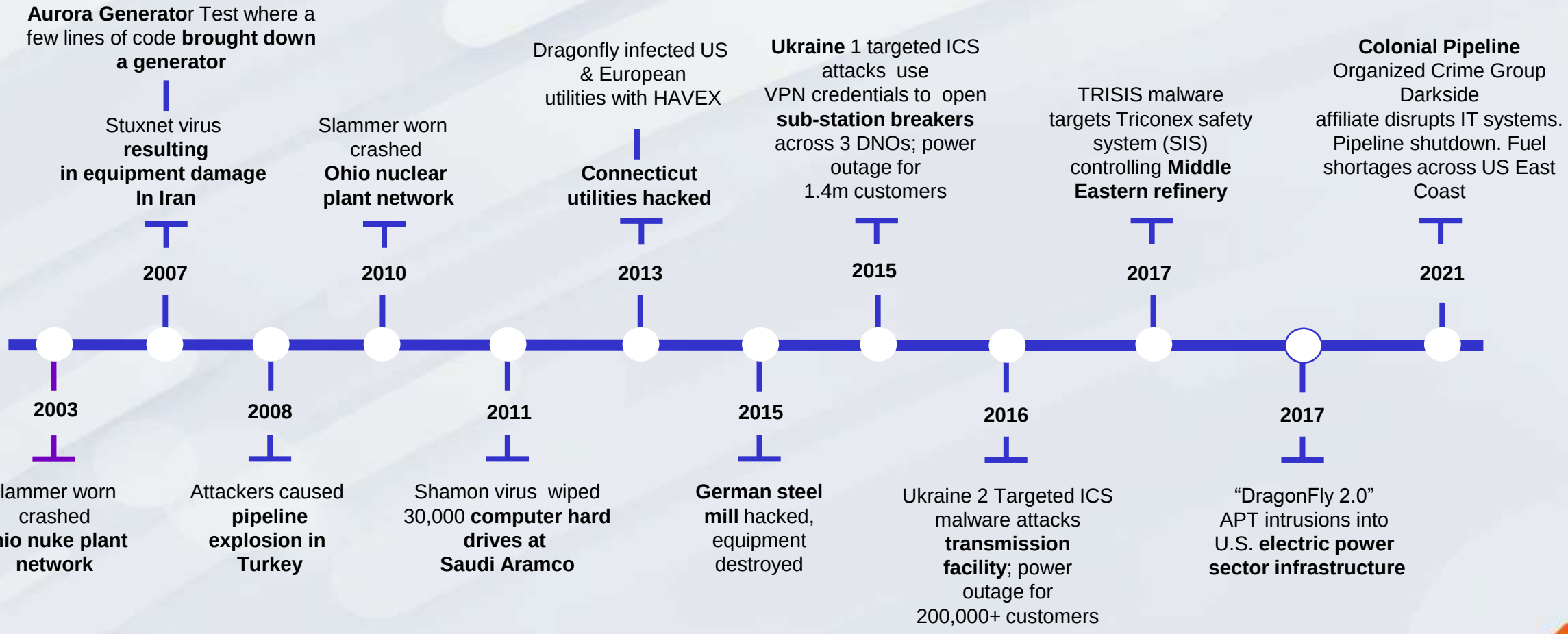
The ISA/IEC 62443-1-1

Ciberseguridad

- Proteger un sistema.
- Establecimiento y mantenimiento de medidas para proteger el sistema.
- Liberación de acceso no autorizado y de cambios, destrucción o pérdidas no autorizados o accidentales.
- Proteger para que no autorizados no pueden modificar el software y
- Proteger datos ni obtener acceso a las funciones del sistema
- Garantizar que esto no se niegue a personas y sistemas autorizados.
- **Prevenir de la penetración ilegal o no deseada o de la interferencia con el funcionamiento adecuado y previsto de un sistema de automatización y control industrial.**

Fuente: CCPS (Center for Chemical Process Safety). Managing Cybersecurity in the Process Industries (pp. 6-7). Wiley. Kindle Edition.

LAS BRECHAS DE CIBERSEGURIDAD RESULTAN EN OPERACIONES INTERRUMPIDAS



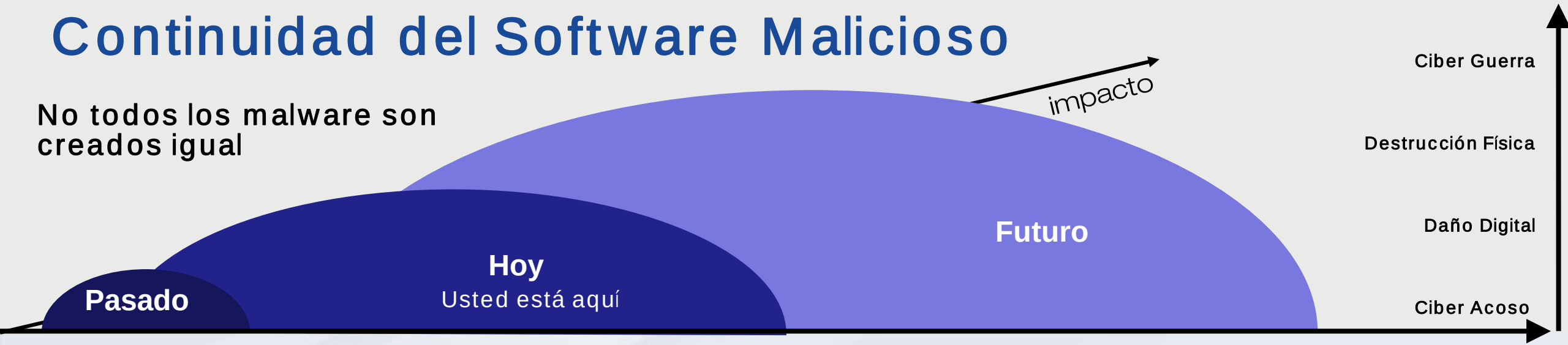
Colonial pipeline

- Durante el período del 7 al 12 de mayo, se suspendió el transporte de combustible a través del poliducto.
- La causa de esto fue un ataque cibernético que involucró al ransomware DarkSide.
- Colonial Pipeline entrega alrededor del 45% del combustible para la costa este, incluyendo
  - gasolina,
  - diesel,
  - combustible para aviones y
  - combustible utilizado por los militares.

Fuente: https://ics-cert.kaspersky.com/publications/reports/2021/05/21/darkchronicles-the-consequences-of-the-colonial-pipeline-attack/.

Continuidad del Software Malicioso

No todos los malware son creados igual



El Pasado:

El hackeo de la vieja escuela está muerto, porque se lo ha automatizado. La tendencia es el Malware.

Clases de malware:

Forma más baja

Automatizado, oportunista / no dirigido, auto-replicante, medianamente destructivo (como un resfriado común), software malicioso TONTO. Probablemente sin C2 (comando y control).

Forma media

Ransomware. El ransomware es el nuevo DoS; es la herramienta de menor denominador común. Un garrote moderno. Ni elegante, ni avanzado. Requiere C2. Mantiene a los activos DIGITALES como

Forma mas alta

Está aún por verse: ransomware con capacidad de destrucción física. Altamente automatizado, Dirigido por IA, altamente dirigido. Este retiene al PROCESO como rehén (por amenaza de daño físico).

Si el ransomware no es lo suficientemente aterrador, los atacantes avanzados pueden apuntar (y lo harán) a las variables del proceso industrial, no solo a la tecnología, es decir las entradas y salidas del los sistemas de control industrial (ICS) donde se manifiestan los daños y la destrucción.

Temperatura | Presión | Flujo | Nivel | Vibración | Tiempo/Frecuencia | Análisis | Movimiento (general) | Movimiento (control de mov.)

Alineándose hacia el FUTURO

Una misión: Resiliencia en todo el ecosistema

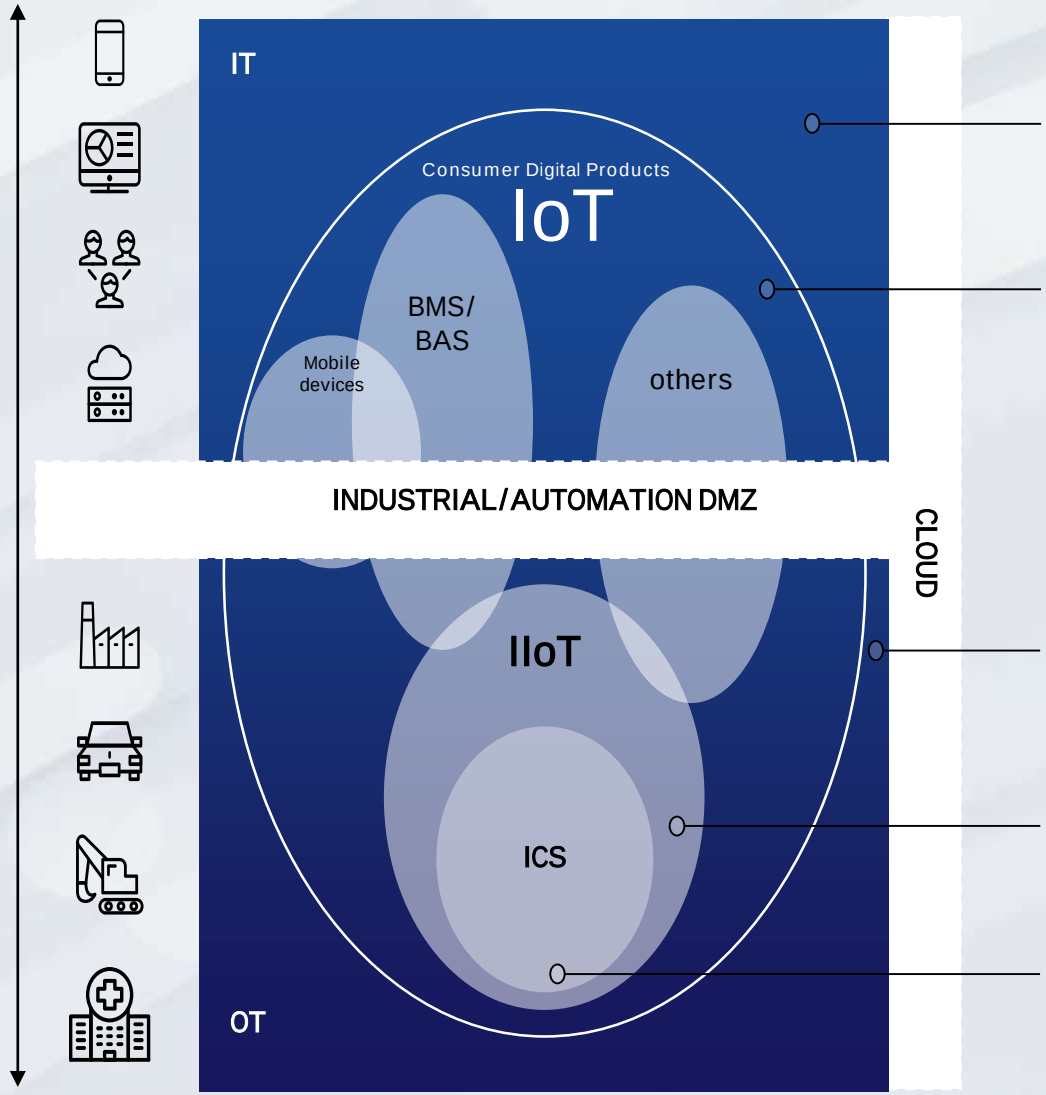
La tecnología importa. ***El riesgo importa.***

Diferentes elementos del negocio tienen diferentes impactos y criticidad cuando sufren disrupción.

Alineando los equipos, capacidades, y estructuras para contribuir con valor real al negocio y las operaciones

Agenda

- Introducción
- Propósito
- Ciberseguridad
- Convergencia
- Visión desde la Gestión de activos
- Conclusión



TECNOLOGÍA DE LA INFORMACIÓN

INTERNET DE LAS COSAS (IOT)

OPERATIONAL TECHNOLOGY (OT)

INDUSTRIAL INTERNET OF THINGS (IIOT)

INDUSTRIAL CONTROL SYSTEMS (ICS)

IT	OT
Confidencialidad	*Seguridad (Personas & Procesos)*
Integridad	*Disponibilidad*
Disponibilidad	*Integridad*
	Confidencialidad

"Para 2023, se asumirá que más del 50% de los CIO en empresas intensivas en activos tienen la responsabilidad del soporte de productos OT".

Cultura IT

Cambios constantes
Ciclo de vida de productos y sistemas corto
Conveniencia del usuario / cliente
Experiencia de usuario

Foco en la solución

Arquitectura / Marco TI
Endendimiento de requerimientos
Diseño/compra de lo mejor a mejor precio
Plan de actualizaciones, parches y soporte

El legado… opuesto a algo …Bueno

Foco en la solución

Seguridad y confiabilidad
Tolerancia a la falla
Consistencia
Longevidad
Determinístico

Foco en la solución

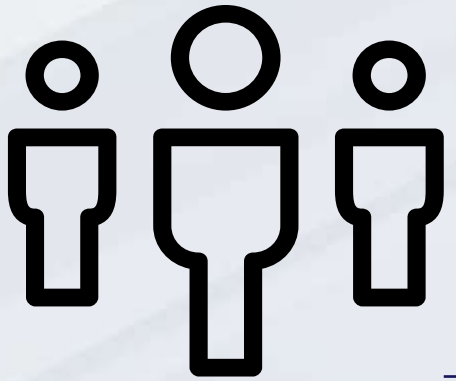
Falla segura
Prueba y error
Bloqueo
Estabilidad

Cambio… opuesto a algo …Bueno

Fuente: Garner 2022

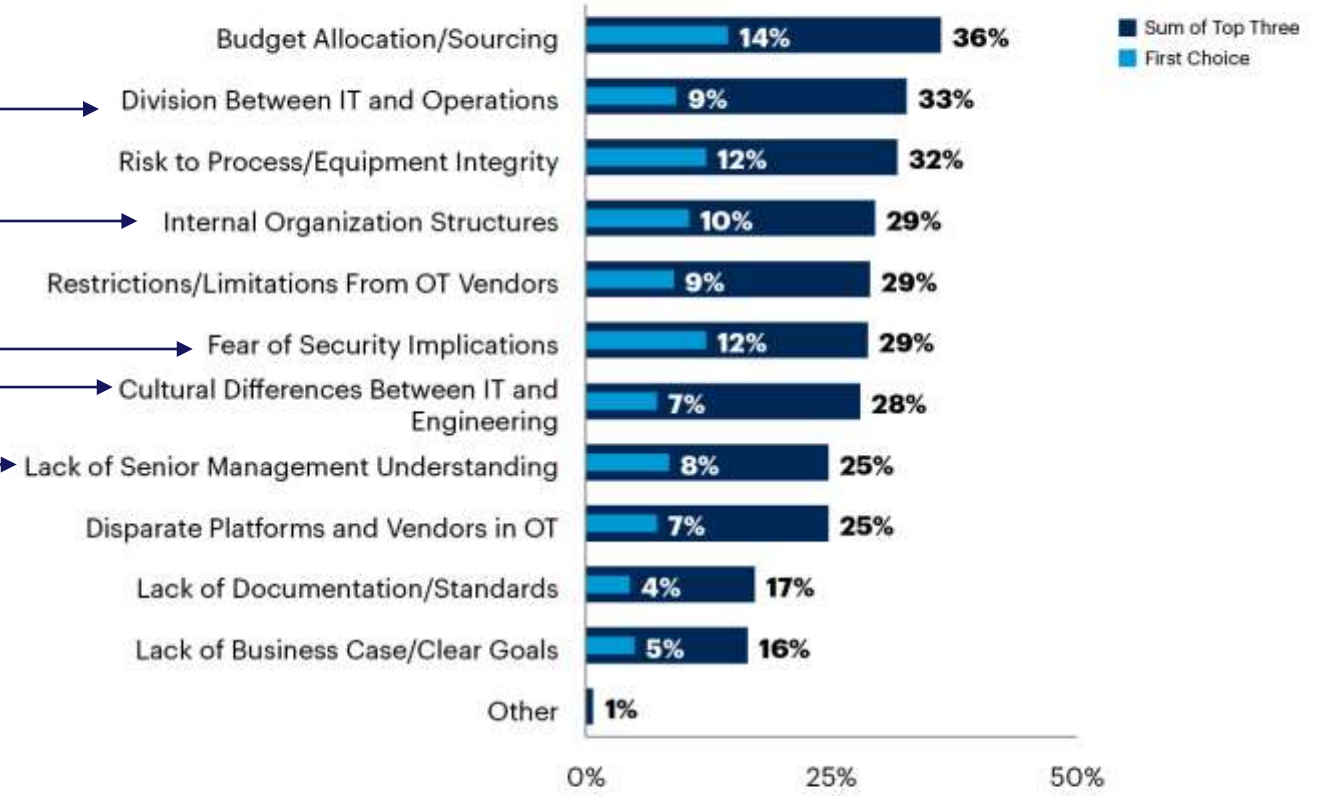
Agenda

- Introducción
- Propósito
- Ciberseguridad
- Convergencia
- Visión desde la Gestión de activos
- Conclusión



Obstacles and Challenges to IT/OT Alignment

Top 3 Rank Summary



n = 401; all respondents, excluding "don't know"

Q. Please rank in order of importance the top three challenges that your organization faces or is expected to face when aligning the management of IT systems with OT systems.

Source: 2021 Gartner IT OT Alignment and Integration Survey

754619_C

Gartner

1. Unión de culturas

Los estándares y métodos formales de ingeniería deben formar parte de un proceso de desarrollo dentro de TI.

ISO 55000

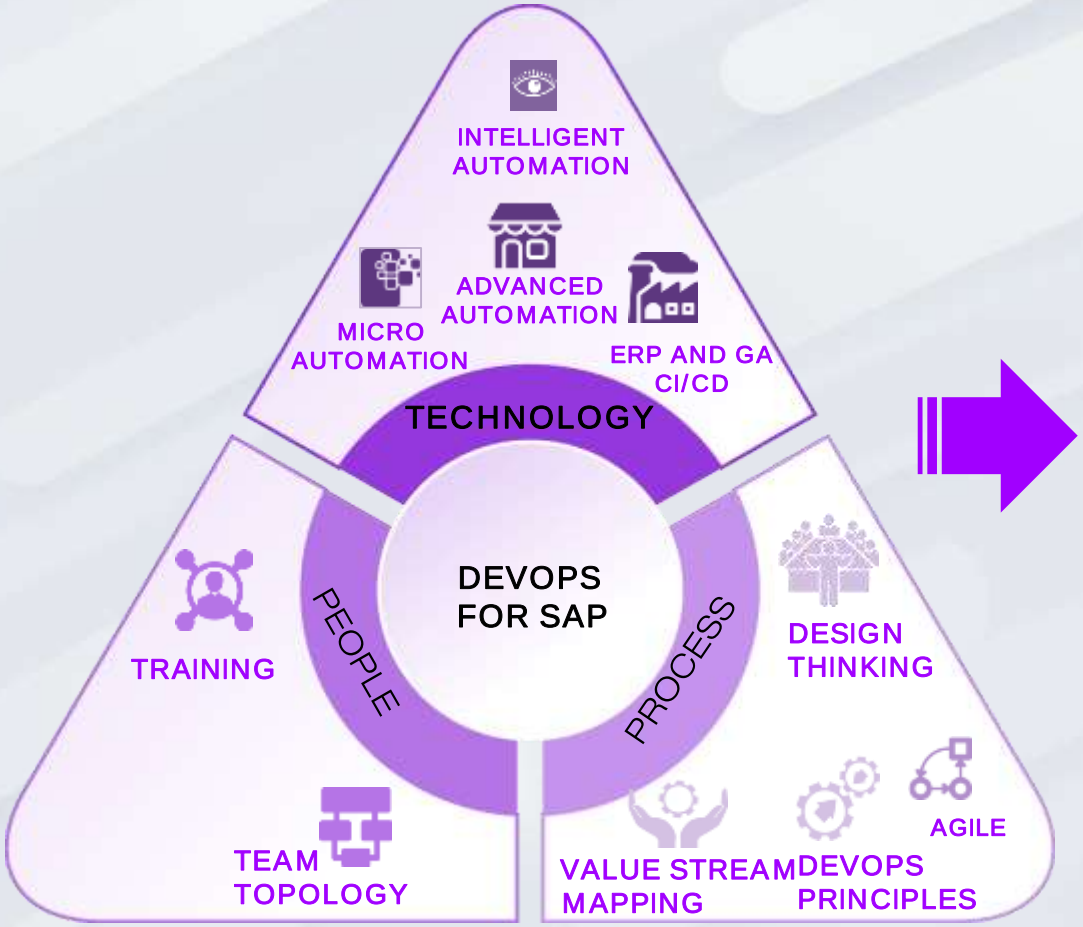
Los estándares y métodos formales de TI deben formar parte de un proceso de desarrollo dentro de TO.

DevOps

Gestión de activos

Actividad coordinada de una organización para obtener **valor a través de sus activos**

DevOps

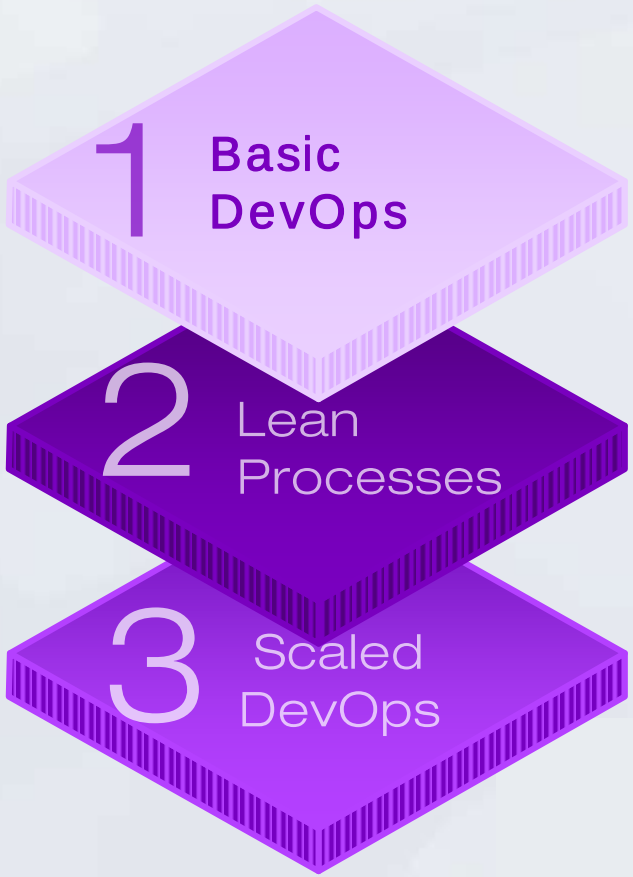


ÁREAS DE HABILITACIÓN

Demuestre el ROI temprano con microautomatizaciones

Lograr una agilidad mínima viable

Escale con orquestación inteligente e integrada



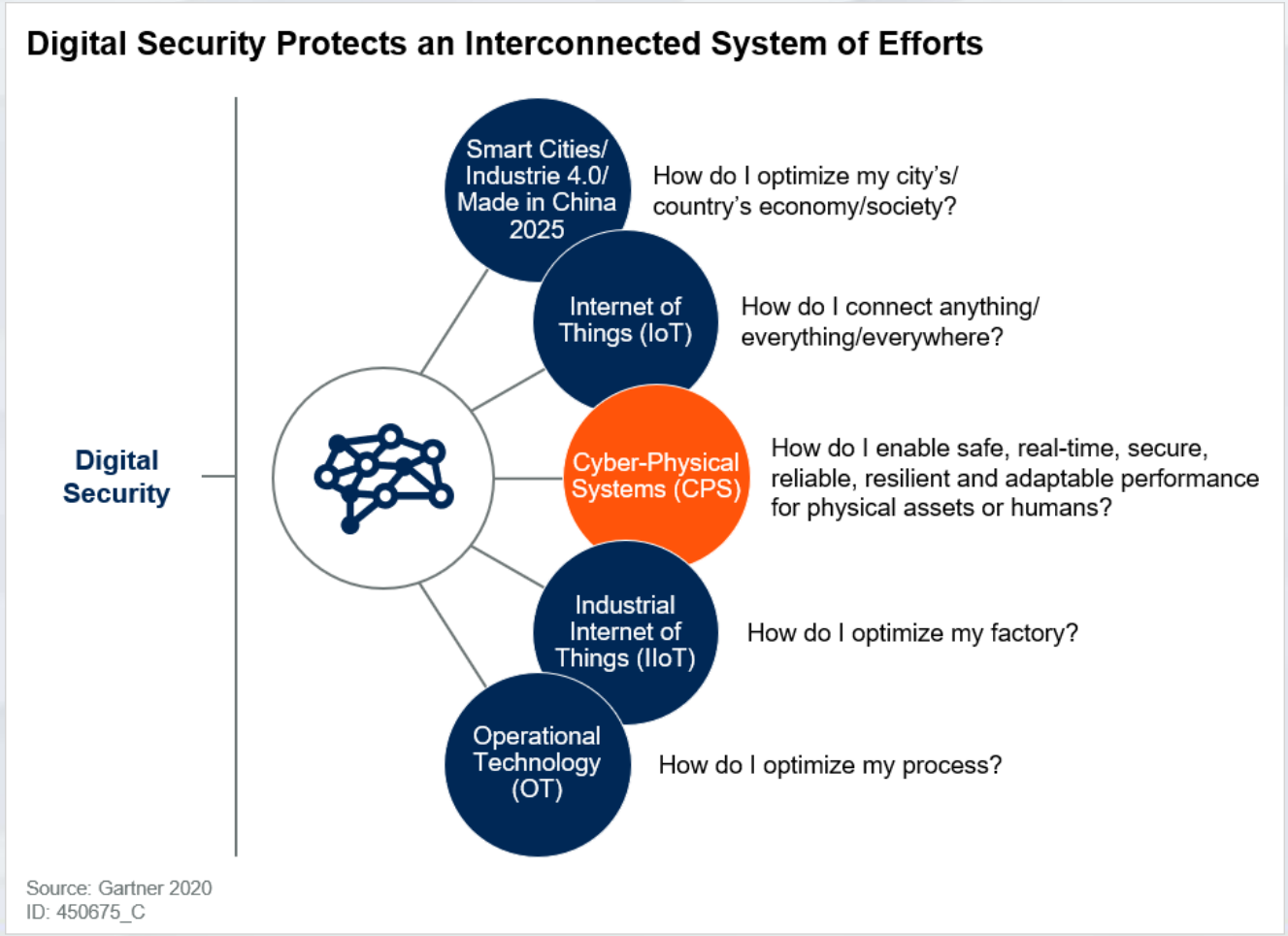
ENFOQUE DE IMPLEMENTACIÓN

2. Análisis del riesgo

Seguridad de Procesos	Ciberseguridad
Process Hazard Analysis (PHA)/Hazard and Operability Study (HAZOP)	Cybersecurity HAZOP
Checklist (e.g., facility siting)	Checklists de ciberseguridad
Failure Modes and Effectis Analysis	FMEA de ciberseguridad
Bow tie	Bow tie de ciberseguridad
Layer of protection Analysis (LOPA)	Semi-cuantitativa verificación de nivel de seguridad
Analisis de riesgo cuantitativos (QRA)	Analisis de riesgo cuantitativos (QRA)

Los CIO podrían comenzar a ver los valores de ingeniería de una actitud de aversión al riesgo y seguridad primero como útiles, no como inflexibles y un obstáculo.

3. Confiabilidad / Integridad



Los CIO deben ver la seguridad del sistema ciberfísico como un requisito de seguridad física y confiabilidad, así como una necesidad de integridad del software

4. Gobernabilidad

PEGA

- Claro
- Foco en activos
- Foco en el negocio

Comité Estratégico

Integrantes

- CIO
- CFO
- VP Ingeniería
- VP Producción
- Gerente de Mtto / TO
- Gerente de HSE
- Gerente de RH

Actividades

- Alineación de la estrategia organizacional
- Decisión del presupuesto
- Priorización de las iniciativas para la TO
- Seguimiento a los KPI estratégicos
- **Soportado** por un comité técnico – ejecución de proyectos

Agenda

- Introducción
- Propósito
- Ciberseguridad
- Convergencia
- Visión desde la Gestión de activos
- Conclusión

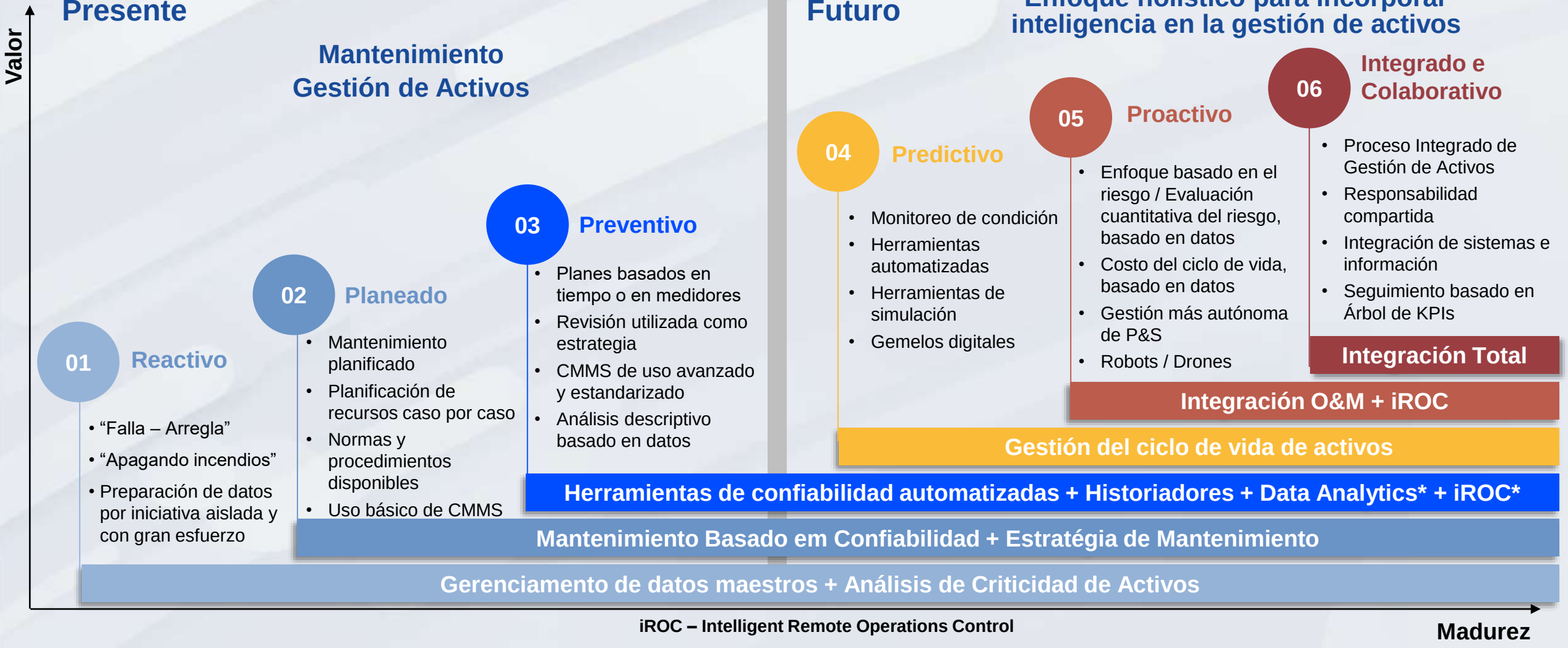

5. Liderazgo
5.1 Liderazgo y compromiso
5.2 Política
5.3 Roles, responsabilidades y autoridades
6. Planificación
6.1 Acciones para abordar riesgos y oportunidades
6.2 Objetivos y planificación
7. Soporte
7.1 Recursos
7.2 Competencia
7.3 Conciencia
7.4 Comunicación
7.5 Requerimientos de información
7.6 Información documentada
8. Operación
8.1 Planeación y control operacional
8.2 Manejo del cambio
8.3 Tercerización
9. Evaluación de desempeño
9.1 Monitoreo, medición, análisis y evaluación
9.2 Auditoría interna
9.3 Revisión por la dirección
10. Mejoramiento
10.1 No conformidades y acciones correctivas
10.2 Acciones preventivas
10.3 Mejora continua
4. Contexto de la Organización
4.1 Contexto
4.2 Partes interesadas
4.3 Alcance del sistema
4.4 Sistema de gestión de activos

Presente

Mantenimiento Gestión de Activos

Futuro

Enfoque holístico para incorporar inteligencia en la gestión de activos



COLABORACIÓN


CONFIANZA

GRACIAS

PILAR VALDERRAMA
Accenture Industry X
Pilar.valderrama@accenture.com
+57 317-639-7441