Más allá de la auditoría a sistemas de monitoreo Inteligentes

Ing. Jorge D Samayoa

CEO Plus Technologies

CLAIN 2023
XXVII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos

2023

XXVII CONGRESO LATINOAMERICANO
AUDITORÍA INTERNA
Y EVALUACIÓN DE RIESGOS
LA ANTIGUA GUATEMALA, GUATEMALA

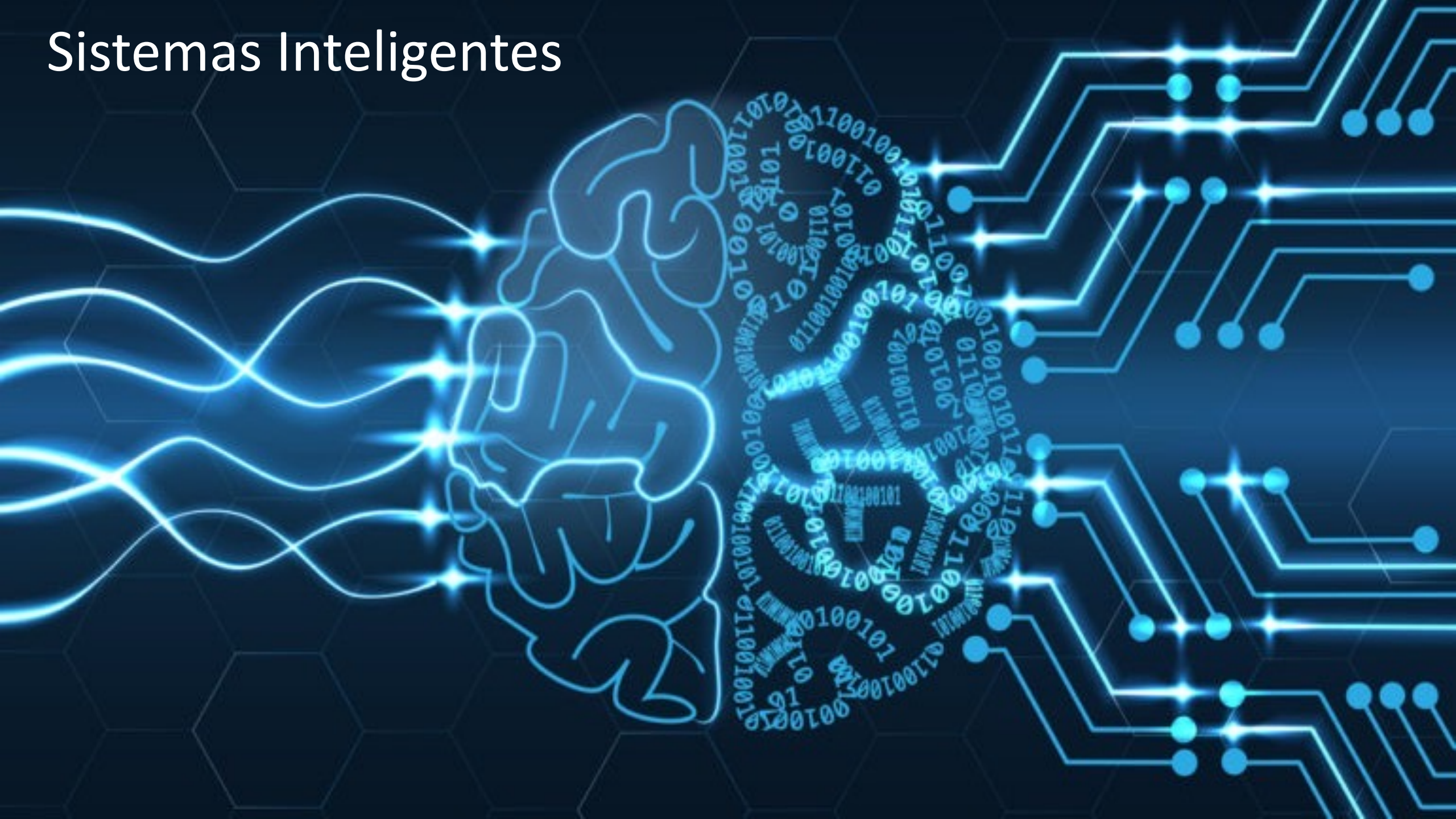
Agenda

- **Conceptos sobre sistemas de Monitoreo Inteligentes.**
- Auditoría a Sistemas de Monitoreo Inteligentes
- Más allá de la auditoría a Sistemas de Monitoreo Inteligente


FRAUDE

REAL-TIME MARKETING

Sistemas Inteligentes



Ciclo Sistema de Monitoreo Inteligente

Se realiza una operación

Sistemas Centrales

- Tiempo real
- Tiempo cercano al real
- Por lotes

Operaciones financieras
Y no financieras,
Consultas, Rechazos, operaciones administrativas, accesos

- Técnicas de AI &ML

Aprender

Análisis

Modelo de Detección
- Operaciones inusuales
- Fraudes o Errores
- Sospechosas AML
- Eventos relevantes
- Oportunidades
- Atrasos

Acciones

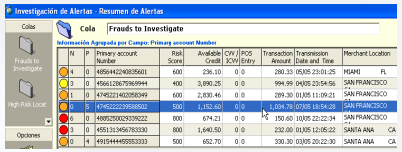
- Declinar
- Alertar a Visor
- Envío de mensajes
- Acciones automáticas

Conclusión

- Descarte
- Confirmación
- Investigación
- Fraude

CLAIN 2023
XXVII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos

Gestión de Alertas



VISOR DE ALERTAS

CELULAR – SMS

VISOR MOVIL

E-MAIL

Telegram

Facebook Messenger

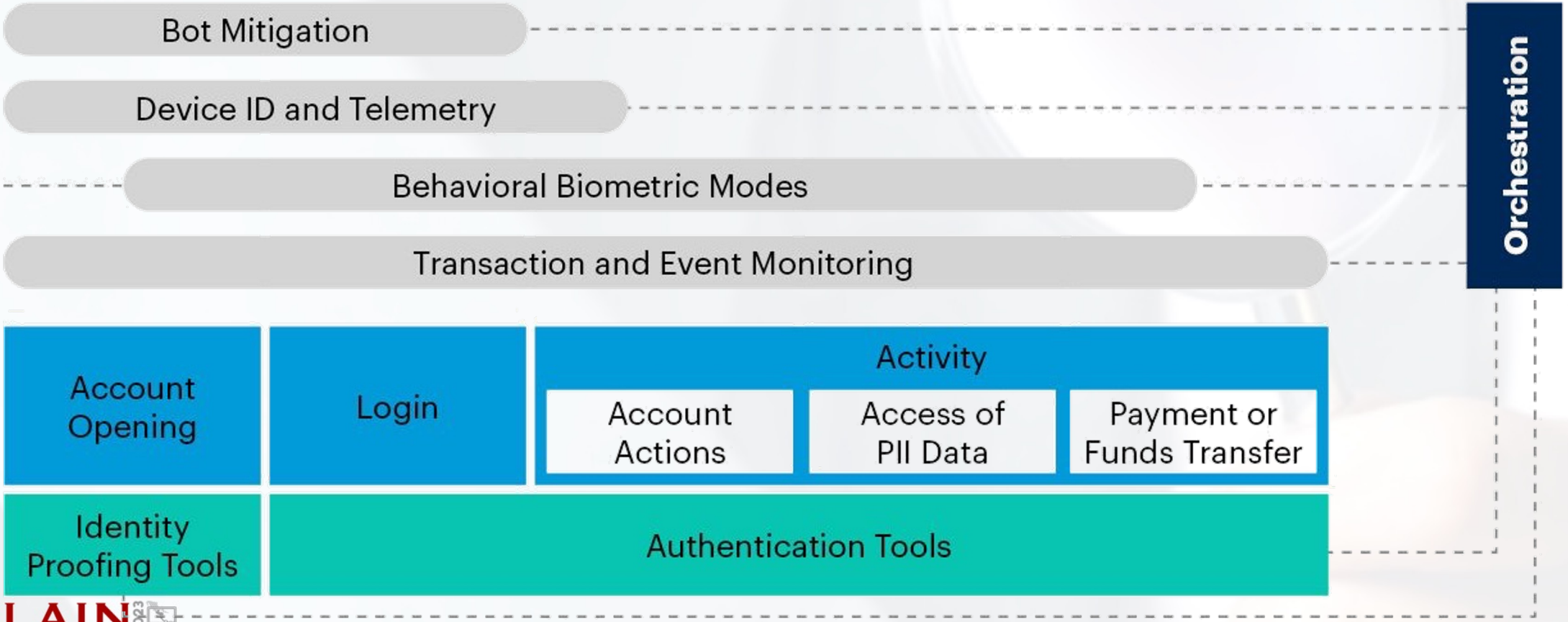
Whatsapp

CLAIN 2023
XXVII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos

Uso de la tecnología en el tiempo


REAL TIME

Span of OFD Capabilities Across a Typical Digital Customer Journey

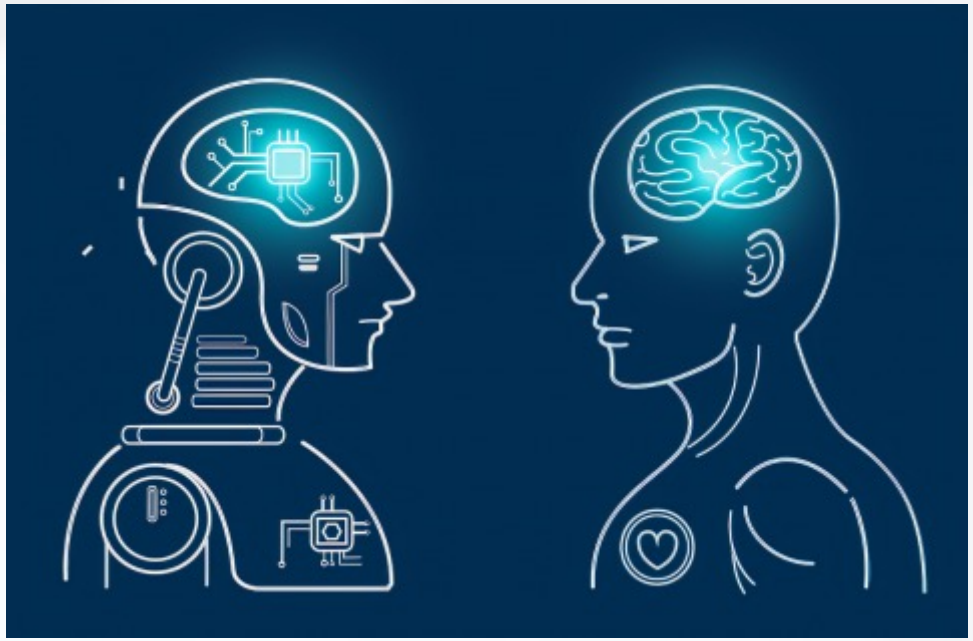


Source: Gartner

Resultados Prevención

Eficiencia Operativa

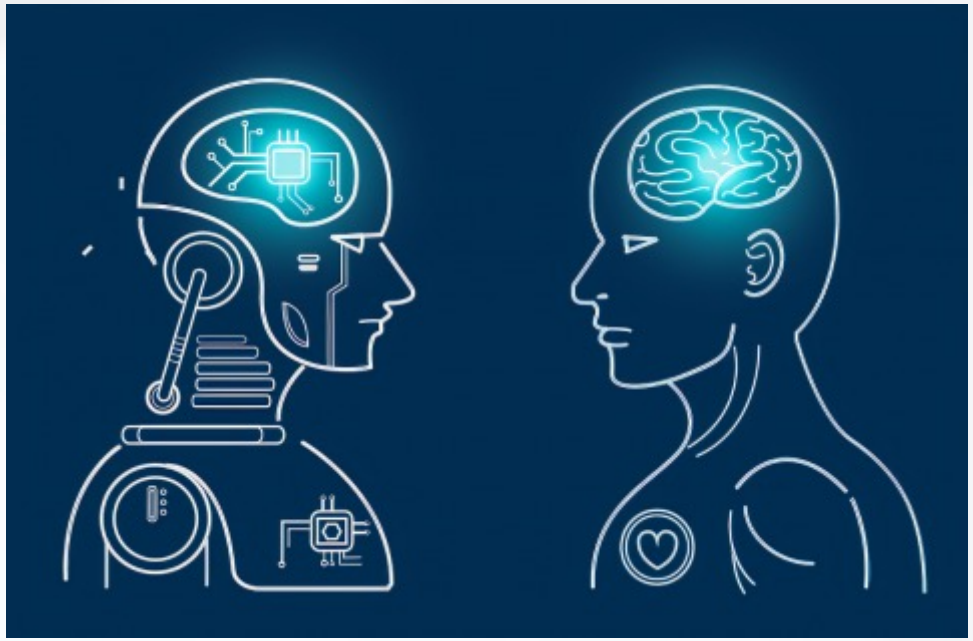
Experiencia del Cliente



Concepto de sistema experto

Un **sistema experto** es un sistema informático capaz de razonar y actuar al nivel de una persona experta en un campo o actividad en específico. Se caracteriza por igualar o superar las habilidades de un ser humano en un área de conocimiento en concreto.

Los sistemas expertos son un subconjunto de la inteligencia artificial y, como tal, es una de las tantas aplicaciones que pretende igualar o superar los conocimientos y habilidades de los humanos expertos.



- **Sistema experto basado en reglas:** Estos sistemas funcionan mediante el seguimiento de reglas, la comparativa de resultados y la aplicación de nuevas reglas utilizadas en contextos modificados.
- **Sistema experto basado en casos:** Consta en la solución de nuevos problemas basándose en soluciones de problemas pasados.
- **Sistema experto basado en redes bayesianas:** Son sistemas que poseen gráficos de variables conocidas y relaciones de dependencia entre ellas. El objetivo es determinar la probabilidad de aquellas variables que no se conocen.

¿Qué es Machine Learning?

Es el subcampo de las ciencias de la computación y una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas que permitan a las computadoras *aprender*. De forma más concreta, se trata de crear programas capaces de generalizar comportamientos a partir de una información de entrenamiento.

¿Por qué Machine Learning está de moda hoy día?

1) Porque hay datos

2) Capacidad de Cómputo

Los 4 problemas que resuelve el Machine Learning

Clasificación

ANN
DNN
Reglas Adaptivas
Arboles de decisión
Data Mining Online
Análisis Discriminante
Regresión Logística
Scoring Dinámico
Naive Bayes
Ensambles
XGBoost
lightGBM

Reducción de la dimensión

Análisis de Correspondencias
Análisis de Componentes Principales

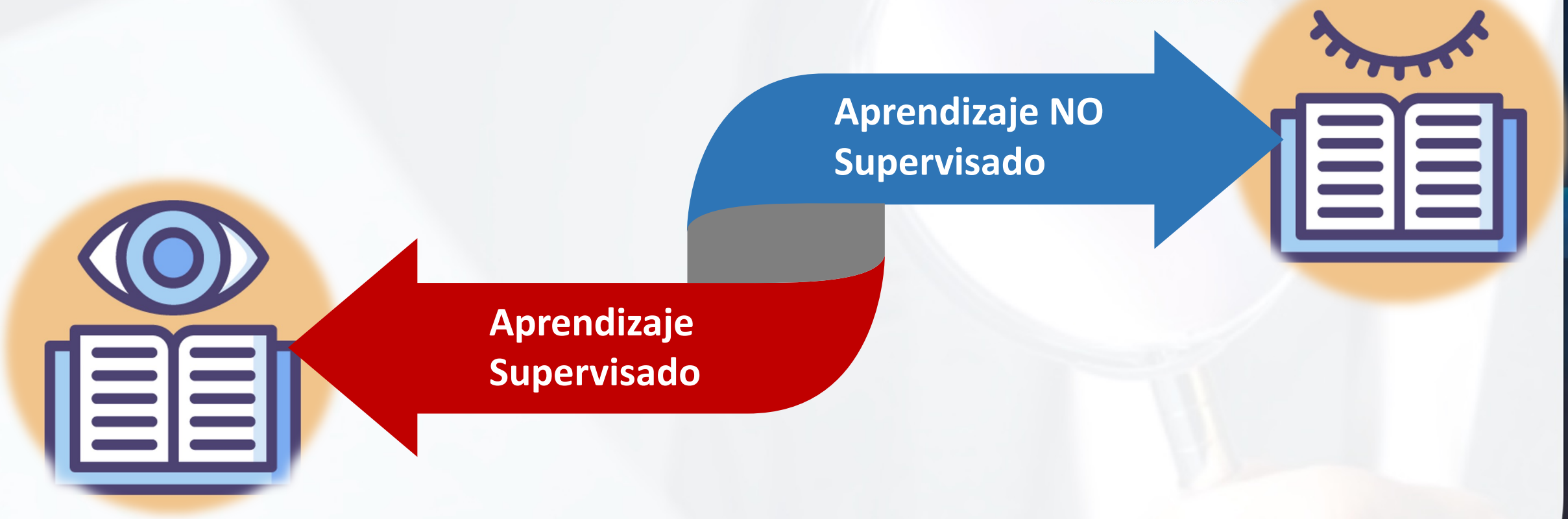
Predecir

Regresión Simple
Regresión Múltiple

Agrupación / Segmentación

K Medias
PAM
K Prototype
Reglas de Asociación

Machine Learning:



Modelo de Segmentación

La metodología **CRISP-DM** está diseñada para proporcionar la garantía de calidad de la implementación del modelo AML/PLD, combinando técnicas de minería de datos para este riesgo.

Metodología CRISP-DM

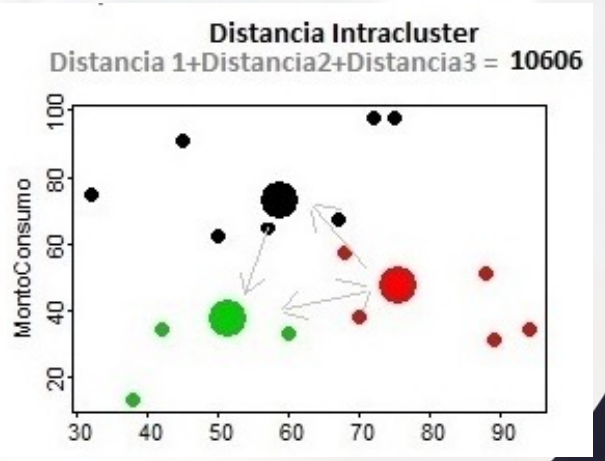
1. Comprensión del Negocio.
2. Comprensión de los Datos.
3. Preparación de los Datos.
4. Modelado
5. Evaluación
6. Despliegue

Modelos de análisis de conglomerados

K-Prototype

clustering | clustering

Ejemplo resultado cluster



CLAIN 2023
XXVII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos

XGBoost & ligthGBM

Evolución de los algoritmos basados en arboles de decisión

Simple Tree

Baja performance de clasificación. Se puede traducir a reglas

Bagging

Bootstrap con resample y clasificación por mayorías. Al cambiar la data salen árboles distintos y esto reduce la varianza del dataset. Se promedian las probabilidades. Al ser cientos de árboles los limites son mas suaves

Random Forest

Son árboles totalmente independientes y no correlacionados. Se generan árboles distintos con una selección random de variable, y reduce la varianza. Se pueden procesar en paralelo. Mejora a Bagging por la decorrelación de árboles. Pocos parámetros poco overfitting.

Boosting

Los árboles aprenden de sus sucesores y son secuenciales. Busca crear un nuevo dataset con los datos mal clasificados por el árbol anterior. Muchos parámetros y puede hacer overfitting

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

ASOCIACION BANCARIA DE GUATEMALA

LightGBM

TensorFlow

RANDOM FOREST

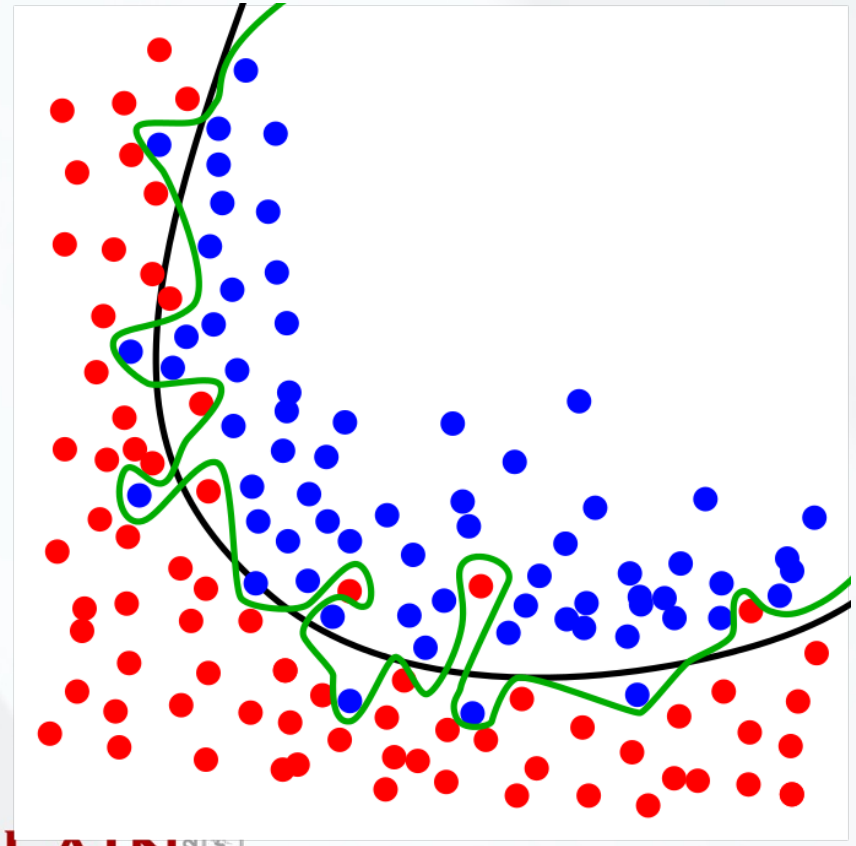
scikit learn

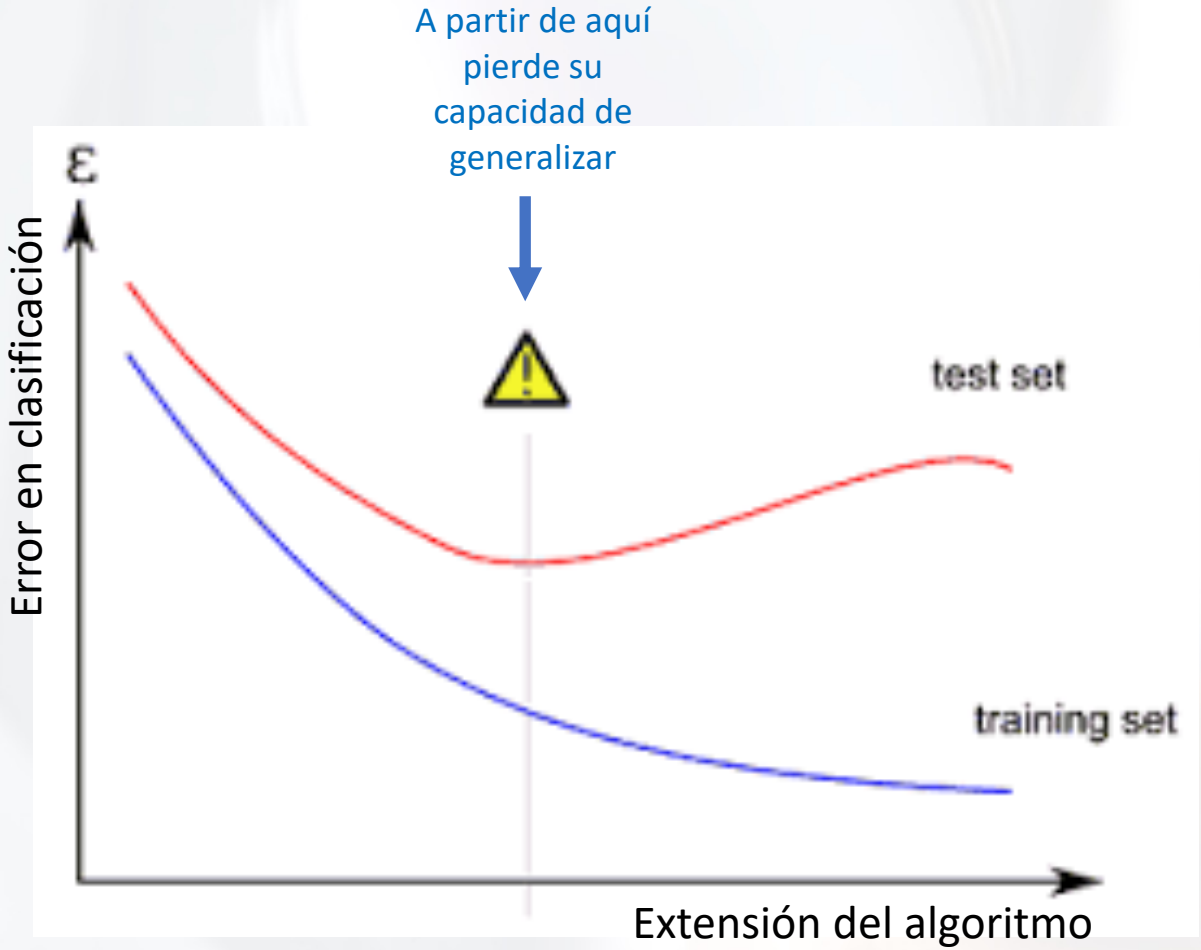
dmlc XGBoost

CLAIN 2023
XXVII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos

MATRIZ DE CONFUSION

Concepto de Overfitting & Underfitting

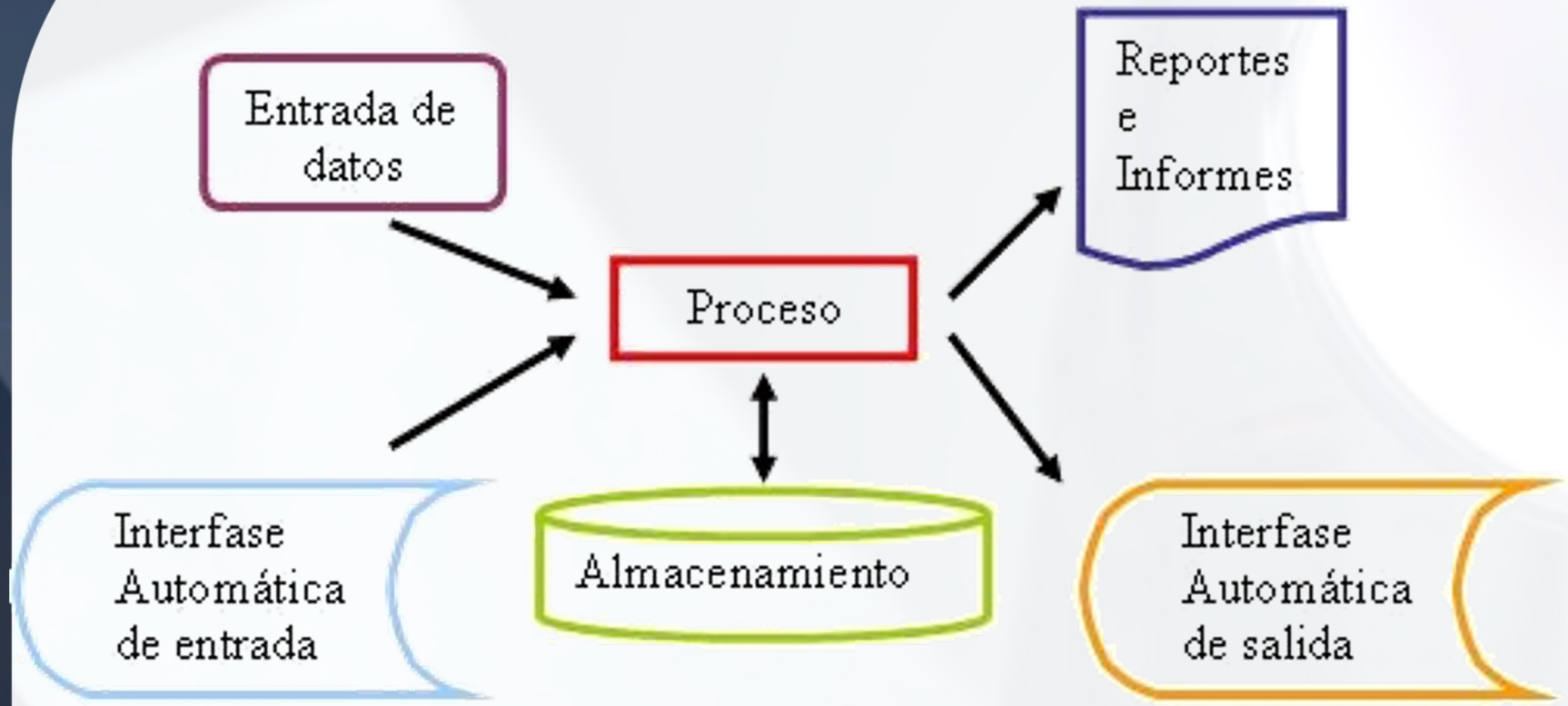




Agenda

- Conceptos sobre sistemas de Monitoreo Inteligentes.
- **Auditoría a Sistemas de Monitoreo Inteligentes**
- Más allá de la auditoría a Sistemas de Monitoreo Inteligente


PROHIBIDO
EL PASO



BITACORAS Y LOGS:

- ACCESOS
- CAMBIOS A ROLES Y PERMISOS
- CAMBIOS AL MODELO
- CONSULTA INFORMACION
- GESTION OPERATIVA
- PROCESOS DE CIERRE
- ERRORES

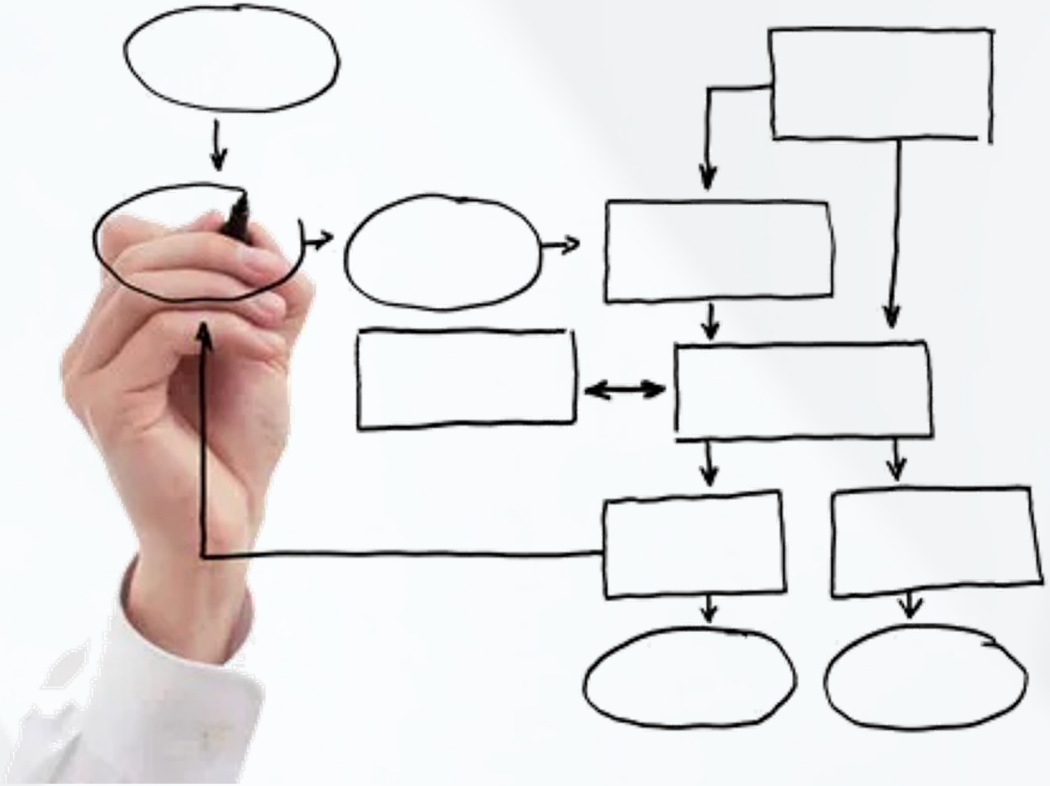
SEPARACION DE FUNCIONES EN LA ADMINISTRACION DE SEGURIDAD DEL SISTEMA

Segregación de Funciones

Es una de las principales actividades de control interno destinada a prevenir o reducir el riesgo de errores o irregularidades, y en especial el fraude interno en las organizaciones

Su función es la de asegurar que un individuo no pueda llevar a cabo todas las fases de una operación/transacción, desde su autorización, pasando por la custodia de activos y el mantenimiento de los registros maestros necesarios

PROCESOS CRITICOS EN UN SISTEMA DE MONITOREO INTELIGENTE



- DEFINICION DE POLITICAS
- CREACION DE USUARIOS Y DEFINICION DE ROLES
- MODIFICACIONES AL MODELO EXPERTO: REGLAS, UMBRALES, LIMITES, LISTAS BLANCAS, LISTAS NEGRAS, ETC.
- ENTRENAMIENTO Y PUESTA EN PRODUCCION DE MODELOS DE MACHINE LEARNING
- DETECCION DE OPERACIONES SOSPECHOSAS
- CONSULTAS A INFORMACION SENSITIVA
- CALIFICACION DE ALERTAS
- WORKFLOWS PARA INVESTIGACION DE CASOS SOSPECHOSOS
- ANALISIS DE CASOS NO DETECTADOS

INDICADORES CLAVE: KPI, KRI

- % DE ALERTAMIENTO
- RELACION FALSO POSITIVO
- % DE DETECCION
- INDICE DE TRX DECLINADAS
- % DE TRX CON TIME OUT
- % DE TRX DE FRAUDE LUEGO DE 1ª ALERTA
- INACTIVIDAD: NO HAY TRX, NO HAY ALERTAS
- DESBORDE DE ALERTAMIENTO
- CAMBIOS EN LAS TENDENCIAS

AUDITORIA DE SISTEMAS

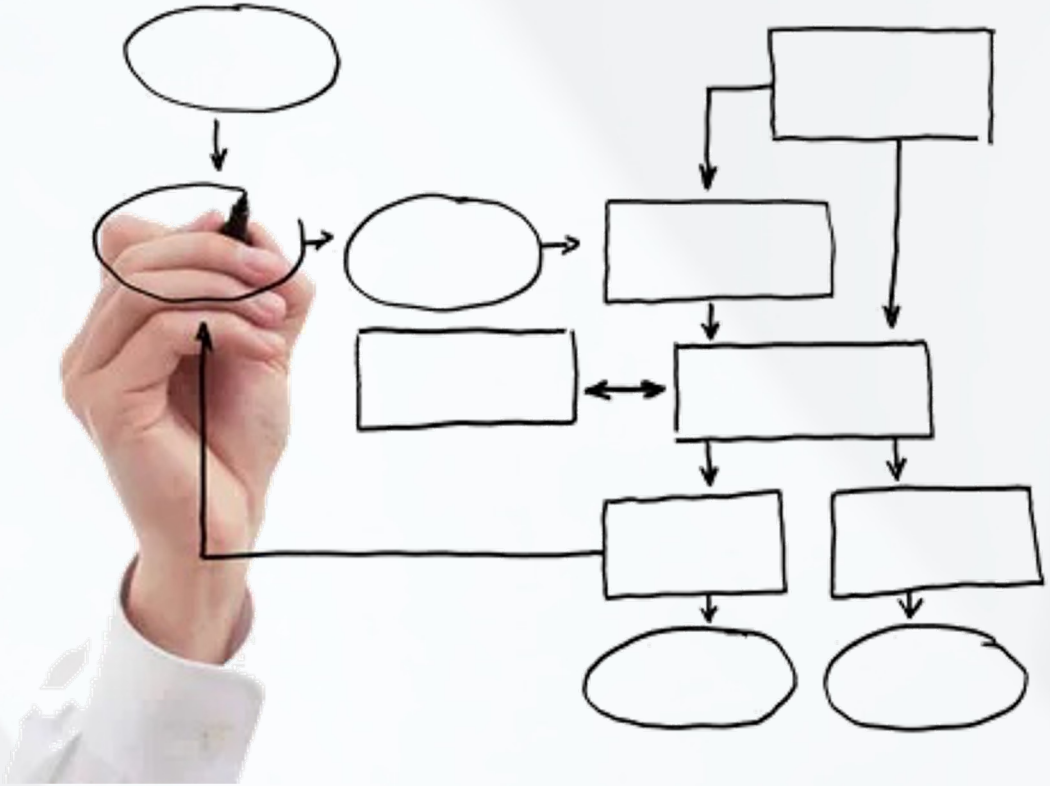
- INTEGRIDAD
- CUMPLIMIENTO NORMAS PCI, ISO 27000, ETC.
- CALIDAD DE DATOS
- CAMBIOS A PROGRAMAS EN AMBIENTE PRODUCTIVO
- BAJADA Y SUBIDA DE SERVICIOS
- ERRORES Y WARNINGS EN EL APLICATIVO
- ACCESOS FUERA DE HORARIO
- LOGINS FALLIDOS
- USUARIOS INACTIVOS
- FUNCIONALIDAD NO UTILIZADA

Agenda

- Conceptos sobre sistemas de Monitoreo Inteligentes.
- Auditoría a Sistemas de Monitoreo Inteligentes
- **Más allá de la auditoría a Sistemas de Monitoreo Inteligente**

CONOZCA SU SISTEMA DE MONITOREO INTELIGENTE

PROCESOS CRITICOS EN UN SISTEMA DE MONITOREO INTELIGENTE



- DEFINICION DE POLITICAS
- CREACION DE USUARIOS Y DEFINICION DE ROLES
- MODIFICACIONES AL MODELO EXPERTO: REGLAS, UMBRALES, LIMITES, LISTAS BLANCAS, LISTAS NEGRAS, ETC.
- ENTRENAMIENTO Y PUESTA EN PRODUCCION DE MODELOS DE MACHINE LEARNING
- DETECCION DE OPERACIONES SOSPECHOSAS
- CONSULTAS A INFORMACION SENSITIVA
- CALIFICACION DE ALERTAS
- WORKFLOWS PARA INVESTIGACION DE CASOS SOSPECHOSOS
- ANALISIS DE CASOS NO DETECTADOS

PROCESOS CRITICOS EN UN SISTEMA DE MONITOREO INTELIGENTE

- DEFINICION DE POLITICAS
- CREACION DE USUARIOS Y DEFINICION DE ROLES
- MODIFICACIONES AL MODELO EXPERTO: REGLAS, UMBRALES, LIMITES, LISTAS BLANCAS, LISTAS NEGRAS, ETC.
- ENTRENAMIENTO Y PUESTA EN PRODUCCION DE MODELOS DE MACHINE LEARNING
- DETECCION DE OPERACIONES SOSPECHOSAS
- CONSULTAS A INFORMACION SENSITIVA
- CALIFICACION DE ALERTAS
- WORKFLOWS PARA INVESTIGACION DE CASOS SOSPECHOSOS
- ANALISIS DE CASOS NO DETECTADOS

- Alerta en la creación de Super Usuario
- Alerta al modificar una regla al modelo
- Alerta al modificar umbral crítico
- Alerta al agregar Item a lista Blanca - Verde
- Alerta al tener N casos no detectados en un periodo de tiempo
- Alerta al vencimiento de N alertas
- Alerta al vencimiento de casos de investigación
- Alerta al cambiar el modelo ML

Beneficiarios múltiples del sistema de Monitoreo inteligente

Usos múltiples del sistema de Monitoreo inteligente

Control Interno
Auditoría

Comercial

Tesorería

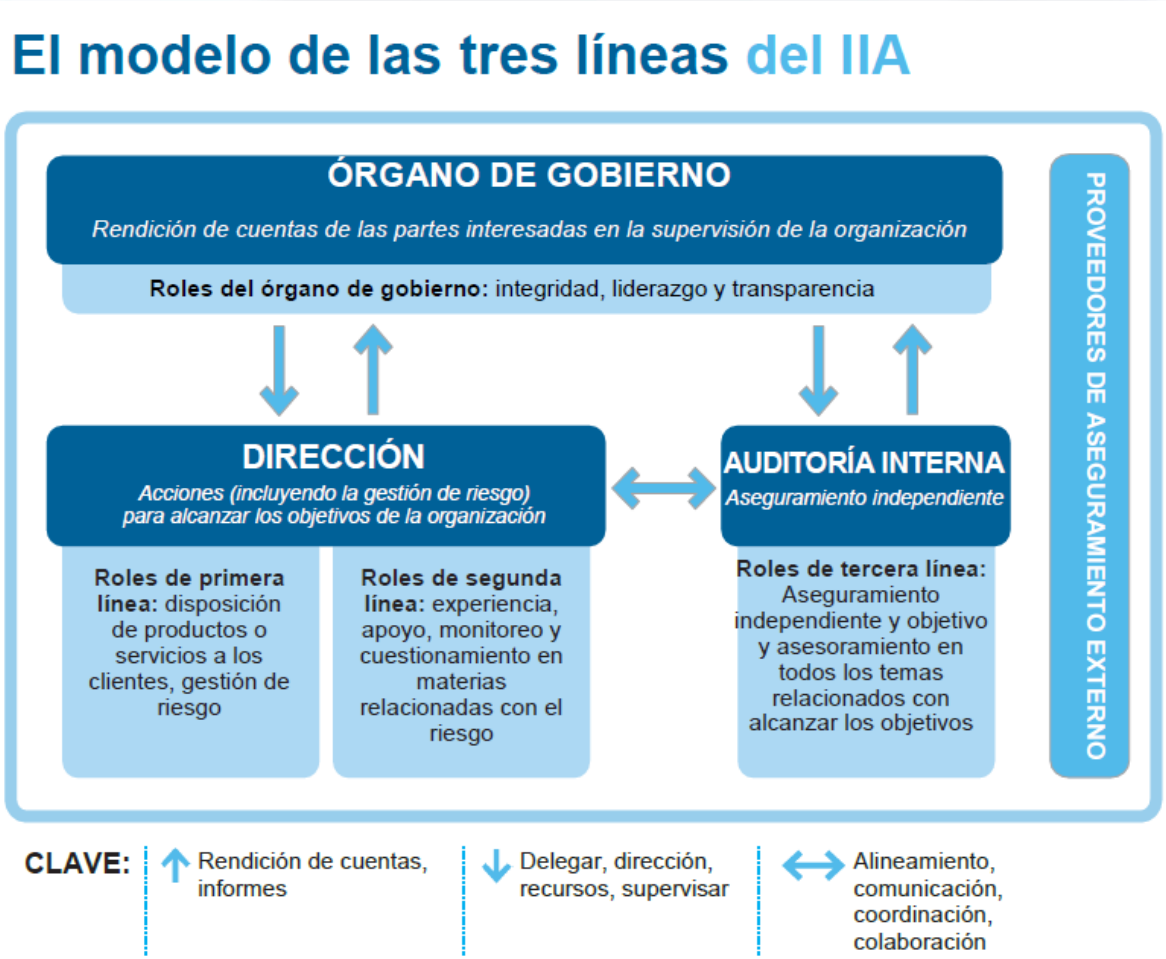
Una Transacción en una Sucursal

Cumplimiento

Prevención
Fraude

Recursos
Humanos

RECOMIENDE REFORZAR CONTROLES de la PRIMERA LINEA

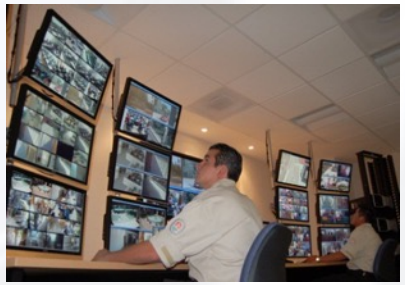


EJEMPLOS

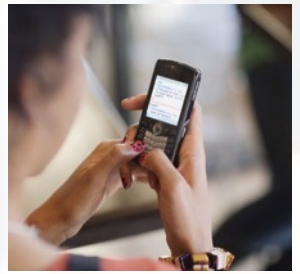
- OPERACIONES FUERA DE HORARIO
- CONTROL DE AUTORIZACIONES
- POSIBLE ROBO DE CONTRASEÑA DE SUPERVISOR
- OPERACIONES DE ALTA CUANTIA
- DESVIACIONES SOBRE PROCEDIMIENTOS
- CAMBIOS EN TENDENCIAS
- DIFERENCIAS Y DESCUADRES DE INFORMACION
- ERRORES Y ATRASOS REPETITIVOS
- NIVEL DE RIESGO ACUMULADO
- DATA DE MALA CALIDAD
- CONSULTAS Y POSIBLE FUGA DE INFORMACION

Descentralice el Manejo de Alertas:

- Centralizadas:
  - ✓ Unidad de Monitoreo
  - ✓ Call Center
  - ✓ Unidad de Prevención de Fraude
  - ✓ Auditoría
  - ✓ Seguridad



- Des-centralizadas:
  - ✓ Gerencia de Sucursales
  - ✓ Mismo Empleado
  - ✓ Usuario Final (cliente)



UTILICE EL SISTEMA DE MONITOREO PARA REALIZAR UNA AUDITORIA CONTINUA

Genere un factor disuasivo

Aproveche la data en estos sistemas de Monitoreo

Recomendaciones:

- ❑ Conozca su sistema de monitoreo inteligente
- ❑ Utilice el mismo sistema de monitoreo inteligente para generar alertas oportunas para Auditoria
- ❑ Aproveche el sistema de monitoreo inteligente para más beneficiarios y distintos usos
- ❑ Recomiende reforza los controles de la primera línea de defensa con controles y alertas adicionales proporcionadas por el sistema de monitoreo inteligente
- ❑ Explore la posibilidad de utilizar el sistema de Monitoreo inteligente para hacer una auditoria continua creando un factor disuasivo
- ❑ Aproveche la data valiosa acumulada

Gracias

- Ing. Jorge D Samayoa
- CEO Plus Technologies

jdsamayoa@plusti.com