

# Proyecto: MOCASI (Modelo de Clasificación de Amenaza Cibernética)

Empresa: INABVE

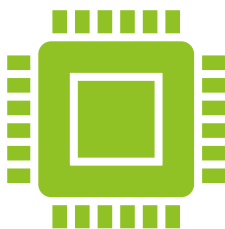
Equipo : Juan  
Laug y Henry  
Ramírez

# OBJETIVO

Presentar los resultados y viabilidad del  
Modelo MOCACI.



# CONTEXTO DEL PROBLEMA



La Institución presenta un aumento constante de eventos y ataques cibernéticos, pero su proceso de detección y análisis es manual, reactivo y depende únicamente de alertas aisladas de firewall y servicios externos.



Se busca automatizar la clasificación y priorización de amenazas para evitar la revisión manual de grandes volúmenes de eventos y mejorar la capacidad de respuesta ante incidentes críticos.

# DESCRIPCION DE LOS DATOS



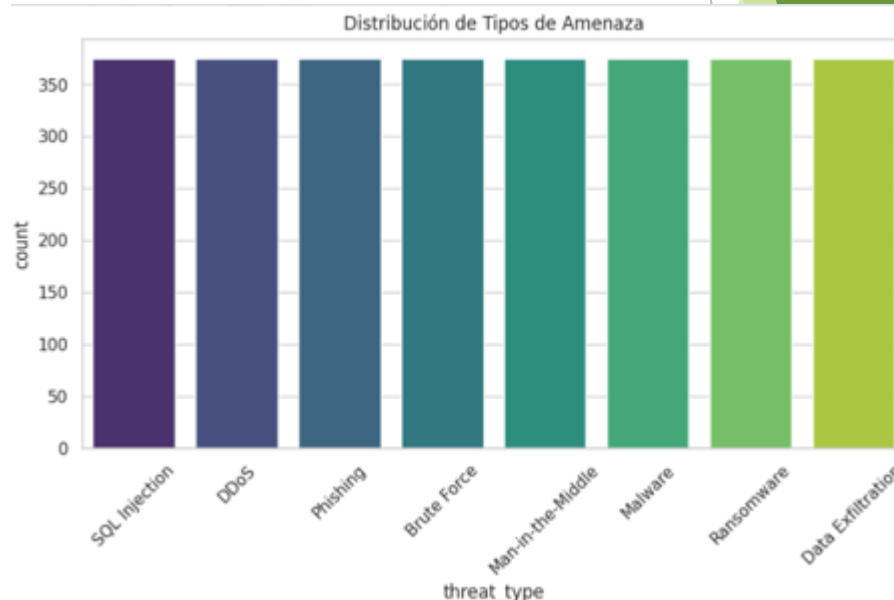
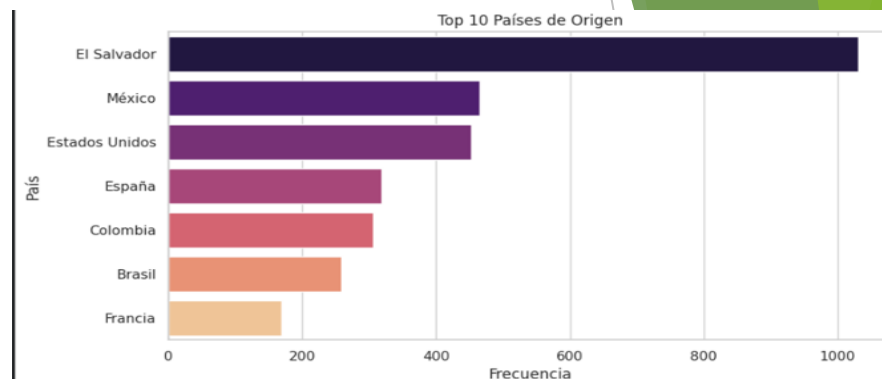
Fuente de los datos:  
registros institucionales  
de seguridad digital.



Cantidad: 3,000  
registros con 16  
características



Tipo: Direcciones IP,  
país de origen,  
protocolos, puertos,  
tamaños de paquetes,  
acciones de firewall,  
tipo de ataques.



# METODOLOGIA



Modelo empleado:  
modelo de  
clasificación.



Validación del Modelo:  
división de datos en 2  
grupos: a) entrenar el  
modelo y b) probarlo en  
escenario no vistos.



Métricas: MOCACI  
acierta 85 de cada 100  
predicciones.

Matriz de Confusión

9	12	6	7	10	7	17
11	12	11	6	1	13	15
8	12	3	14	11	10	9
11	11	9	9	12	9	10
8	10	9	10	11	10	9
4	11	11	9	11	8	12
6	13	9	7	5	12	13
10	9	9	12	10	12	7
1	2	3	4	5	6	7
Predicciones						

Matriz de Correlación

port	1	-0.017	-0.0064	-0.023	0.034	-0.013	0.035	0.022
_size	-0.017	1	-0.0064	0.017	0.026	0.0041	-0.024	-0.016
_sec	-0.0064	-0.0064	1	0.024	-0.0071	-0.015	0.016	0.014
:tion	-0.023	0.017	0.024	1	-0.0024	0.013	-0.014	0.02
_flag	0.034	0.026	-0.0071	-0.0024	1	-0.019	0.00013	-0.0095
cted	-0.013	0.0041	-0.015	0.013	-0.019	1	0.027	-0.022
ar_id	0.035	-0.024	0.016	-0.014	0.00013	0.027	1	0.0051
:e_id	0.022	-0.016	0.014	0.02	-0.0095	-0.022	0.0051	1
port	packet_size	duration_sec	vpn_connection	cloudflare_flag	endpoint_detected	user_id	device_id	

# RESULTADOS

ASPECTO	SITUACION ACTUAL	CON MOCACI
Detección	Reactiva, Manual	Automatizada
Prioridad	Subjetiva	Basada en patrones
Tiempo de Análisis	Alto(horas)	Reducido (min. Seg)

- ▶ El modelo es capaz de clasificar automáticamente los eventos de red según su tipo de amenaza.
- ▶ Ahorro de tiempo operativo.
- ▶ Mayor productividad.
- ▶ Reduce lo riesgos

## ► Valor esperado

	VALORES
Cantidad de analistas	2
Horas por Analista por mes (\$)	160
Costo de hora (\$)	12
Ahorro estimado (%)	0.5
Costo promedio por reduccion de incidente (\$)	2000
incidentes evitados (anual)	1
Costo del proyecto (\$)	10000
Cálculos	VALORES
Ahorro anual (\$)	23040
Ahorro anual por reduccion de incidentes (\$)	2000
Ahorro total anual(\$)	25040
ROI (%)	150.4

Un ROI de 150.4% significa que el proyecto no solo recupera el 100% de lo invertido, sino que además genera un 50.4% mas adicional.

# RECOMENDACIONES

- Integrar el modelo MOCACI en 1 a 3 meses.

IMPLEMENTACION MODELO MOCASI	DURACION ESTIMADA
DESARROLLO DE API O MICROSERVICIO	4 SEM
CONSTRUCCION DE DASHBOARD OPERATIVO	2 SEM
INTEGRACION CON HERRAMIENTAS EXISTENTES	3 SEM
MEJORA CONTINUA	CONTINUO



# CONCLUSIONES

- ▶ La institución enfrenta amenazas constantes, por lo que la automatización es necesaria.
- ▶ Los resultados del proyecto no solo son técnicos, si no estratégicos.
- ▶ Se recomienda integrar el modelo dentro del flujo de monitoreo y crea un dashboard operativo para evaluar su desempeño en tiempo real.

