

Pirámide de Maslow de la ciberseguridad

Referencia:

mswann@microsoft.com

[@MSwannMSFT](https://twitter.com/MSwannMSFT)

[linkedin.com/in/swannman](https://www.linkedin.com/in/swannman)

<https://github.com/swannman/ircapabilities>

**¿Cuánto
conoces de tu
organización?**

1.- Comenzamos leyendo de abajo hacia arriba, contestando a las preguntas que se muestran en la siguientes laminas.

2.- Si la respuesta a las preguntas es **NO, te ayudará a identificar las áreas de mejora de seguridad en tu organización.**



COLABORAR

ACTUAR

SEGUIMIENTO

CAZA DE AMENAZAS

COMPORTAMIENTO

AMENAZAS

CLASIFICACIÓN

DETECCIÓN

VISIBILIDAD

INVENTARIO

Auto realización

Reconocimiento

**Necesidades Básicas
de seguridad**

COLABORAR

¿Puede colaborar con socios de confianza para interrumpir las campañas adversarias?

ACTUAR

¿Puede implementar contramedidas comprobadas para desalojar y recuperar?

SEGUIMIENTO

Durante una intrusión, ¿puede observar la actividad de la amenaza en tiempo real?

CAZA DE AMENAZAS

¿Puedes detectar un adversario que ya está en tu entorno o ha comprometido tu infraestructura?

COMPORTAMIENTO

¿Puede detectar la actividad del adversario dentro de tu entorno?

AMENAZAS

¿Quiénes son tus adversarios? ¿Cuáles son sus capacidades?

CLASIFICACIÓN

¿Puede clasificar con precisión los resultados de detección?

DETECCIÓN

¿Puedes detectar actividad no autorizada?

VISIBILIDAD

¿Tiene visibilidad de sus activos?

INVENTARIO

¿Puedes nombrar los activos que estás defendiendo?

COLABORAR

ACTUAR

SEGUIMIENTO

CAZA DE AMENAZAS

COMPORTAMIENTO

AMENAZAS

CLASIFICACIÓN

DETECCIÓN

VISIBILIDAD

INVENTARIO

Mejorar no es opcional, esta es la capacidad de tu organización para mejorar respecto a las diversas áreas de oportunidad de seguridad como controles mal implementados por falta de valoración de activos o amenazas, o priorización de riesgos.

Esta es la capacidad de la organización para identificar amenazas, priorizarlas, y cazarlas cuando se presentan en cualquiera de nuestros activos.

Sino conocemos las amenazas, será como proteger de algo que no vemos.

Esta es la capacidad que tiene tu organización para la identificación, visibilidad y clasificación de tus activos con base en su criticidad.

Si no sabemos qué protegemos, estamos malgastando recursos valiosos.

Contacto

Email: alejandros@iciberseguridad.io

Tel – Whatsapp: +52 81 2587 2530

Monterrey, Nuevo León.

Tlalpan, CDMX

Contacto ante incidentes

csirt@iciberseguridad.io