¿EQUIPOS DE CIBERSEGURIDAD

DESCUBRE SUS FUNCIONES Y ROLES

DESLIZA --- →

RED TEAM
ATRACANTE ÉTICO

BLUE TEAM
DEFENSORES

PURPLE TEAM
PUENTE ESTRATÉGICO

YELLOW TEAM
DESARROLLO SEGURO

GREEN TEAM
INTEGRACIÓN Y CONTINUIDAD

ORANGE TEAM
EDUCACIÓN Y CONCIENCIA

WHITE TEAM
ÁRBITROS

BLACK TEAM
SIMULACIÓN AVANZADA

PINK TEAM
HUMANISTAS

Ingrid Mora

Red Team

El atacante ético

- EQUIPO PRIMARIO -

Función:
Su misión es pensar como el enemigo.
Simular ataques para encontrar y explotar debilidades en los sistemas de la organización.
Mostrar qué tan vulnerable es tu organización antes que los ciberdelincuentes reales lo hagan.

Tareas:
Pruebas de penetración, ingeniería social y análisis de vulnerabilidades. Simulan ataques reales (phishing, explotación de vulnerabilidades, ingeniería social).

Ejemplo:
Descubren que un backup no es funcional ante un ataque de ransomware.

Ingrid Mora

Blue Team
Los defensores

- ¿EQUIPO ¿PRIMARIO -

Función:
Proteger la infraestructura y la información de la organización. Responden ante incidentes, aplican parches y fortalecen controles.

Tareas:
Monitoreo, análisis de vulnerabilidades, respuesta a incidentes y análisis forense.

Convierte los datos de los sistemas en acciones efectivas de defensa.

Ejemplo:
Detectan un ataque DDoS antes de que afecte la disponibilidad de un servicio crítico.

Ingrid Mora

Purple Team

El puente estratégico

- ¿EQUIPO ¿PRIMARIO -

Función:
Actuar como puente entre el Equipo Rojo y el Equipo Azul. Se aseguran de que los hallazgos del ataque (Rojo) sirvan para fortalecer las defensas (Azul).

Tareas:
Facilitar la comunicación y mejorar las defensas de forma continua.

Ejemplo:
Un hallazgo de Red Team se convierte en un playbook operativo para el SOC.

Ingrid Mora

Yellow Team

Desarrolladores seguros

- ¿EQUIPO ¿ESPECIALIZADO -

Función:
Desarrolladores seguros. Diseñadores y constructores. Se dedican a la creación y programación de herramientas, aplicaciones y sistemas seguros (DevSecOps). Evitan que vulnerabilidades lleguen a producción.

Tareas:
Desarrollo de software y aplicaciones con seguridad integrada (DevSecOps).

Dato:
Corregir un fallo en producción cuesta hasta 30 veces más que hacerlo en desarrollo.

Ingrid Mora

Green Team

Integración y continuidad

- ¿EQUIPO ¿ESPECIALIZADO -

Función:
Enfocados en la seguridad desde el inicio del desarrollo. Integran la seguridad en la arquitectura y el diseño de los sistemas. Vinculan desarrollo seguro (Yellow) y operaciones (Blue).

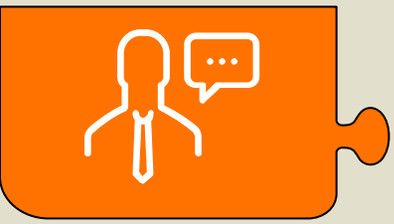
Tareas:
Revisión de código, análisis de vulnerabilidades y asesoramiento en las etapas tempranas de diseño.

Garantizan que la seguridad sea parte del día a día de la organización, no solo un proyecto aislado.

Ingrid Mora

Orange Team

Educación y concienciación



- ¿EQUIPO ¿ESPECIALIZADO -

Función:
Ayudar a los desarrolladores a mejorar sus habilidades en seguridad. Son el enlace entre el Equipo Rojo y los desarrolladores de software, entrenándolos para escribir código más seguro.

Tareas:
Capacitación, revisiones de código y asesoramiento en el desarrollo.

Generan campañas, simulaciones y entrenamientos para reducir riesgos humanos.

Ejemplo:
Campañas de phishing interno para enseñar a los empleados a detectar ataques reales.

Ingrid Mora

White Team

Los árbitros

- ¿EQUIPO ¿EMERGENTE -

Función:
Supervisar los ejercicios de seguridad, como las simulaciones de ataque del Equipo Rojo.

Establecen las reglas del juego, monitorean el progreso y se aseguran de que se cumplan las políticas. Supervisan ejercicios de Red vs Blue.

Tareas:
Planificación de ejercicios, supervisión de la simulación y evaluación de resultados.

Aseguran que las simulaciones se ejecuten bajo reglas definidas y que los aprendizajes sean medibles.

Ingrid Mora

Black Team

Simulación avanzada

- ¿EQUIPO ¿EMERGENTE -

Función:
Simular el rol de adversarios reales, sin ninguna restricción ética o legal.

Se utilizan en entornos controlados y con gran cuidado. Simulan ataques encubiertos extremos.

Tareas:
Ataques a gran escala sin restricciones.

Ayudan a poner a prueba la resiliencia de toda la organización.

Ingrid Mora

Pink Team
Humanistas

- ¿EQUIPO ¿EMERGENTE -

Función:
Se especializan en la ingeniería social, una de las mayores amenazas.

Su objetivo es identificar cómo el factor humano puede ser explotado y concienciar sobre estos riesgos.

Tareas:
Pruebas de ingeniería social, capacitación en conciencia de seguridad y análisis de la psicología humana en la seguridad.

Ingrid Mora

Resumen

No se trata solo de tener un Blue Team o un Red Team.

La madurez real se alcanza cuando cada color aporta su valor y todos trabajan como un ecosistema integrado:

- **Red:** Revela riesgos.
- **Blue:** Defiende.
- **Purple:** Conecta y enseña.
- **Yellow** y **Green:** Construyen seguridad desde el código hasta la operación.
- **Orange:** Educa.
- **White:** Asegura imparcialidad.
- **Black:** Desafía los límites.
- **Pink:** Trabaja con el factor humano.

"Si quieres proteger tu organización de verdad, asegúrate de que no falte ningún color en tu estrategia."

Ingrid Mora