REGISTRO DE CURSO O TALLER

I. Datos generales:

Título:	**Cyber Threat Intelligence (Inteligencia de Amenazas)**						
Instructor o docente:	**TBD**						
Duración (en horas):	8 Horas						
Área:		Formación para la docencia		Formación para la gestión universitaria	**X**	Otra: Varias	
Modalidad de impartición:	**X**	Presencial		A distancia		Mixta	
Lugar y fecha	2 de Octubre de 2019, Universidad Autónoma de Nuevo León						

II. Descripción:

Destinatarios:

- Directivos y Tomadores de decisiones de TI
- Especialistas de Seguridad de la Información

Objetivo(s) o competencia(s):

En primer lugar, tenemos que responder a la pregunta: ¿Qué es la inteligencia de amenazas? La firma Gartner ha definido la inteligencia de amenazas como: "conocimiento basado en la evidencia, incluyendo el contexto, los mecanismos, los indicadores, las implicaciones y asesoramiento procesable, sobre una amenaza o un peligro existente o emergente a los activos que se pueden utilizar para tomar decisiones informadas con respecto a la respuesta del sujeto a la amenaza o peligro".

En su totalidad, pareciera una buena definición, pero ¿qué significa todo esto? ¿Cómo puede la inteligencia de amenazas beneficiarnos?

Metodología:
Exposición de la realidad de la ciberseguridad en México asi como los principales vectores de ataques, y la ventaja de conocer el comportamiento de estos para poder realizar acciones de mitigación.

Mecanismo y criterios de evaluación:
Mínimo 80% de asistencia y participación en las actividades del taller.

III. Temario:

Inteligencia de amenazas

Amenazas

-Intención

-Capacidad

-Oportunidad

Escenarios

Indicadores de Compromiso

Casos Reales

Aplicaciones

Conclusiones

IV. Bibliografía

V. Recursos y materiales requeridos

Pantalla, proyector, computadora, mesas de trabajo, rotafolios.