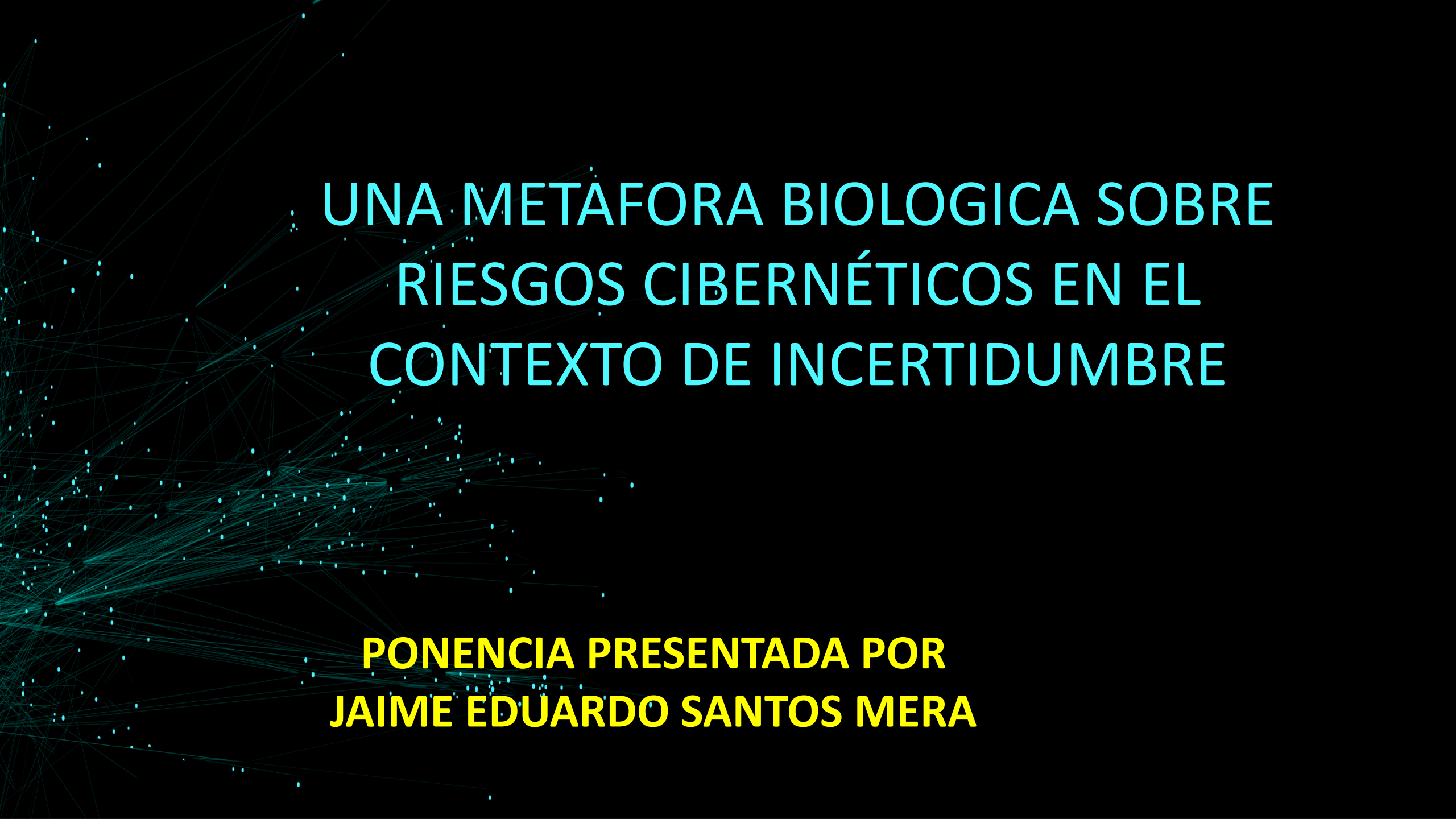




UNA METAFORA BIOLOGICA SOBRE RIESGOS CIBERNÉTICOS EN EL CONTEXTO DE INCERTIDUMBRE

**PONENCIA PRESENTADA POR
JAIME EDUARDO SANTOS MERA**

LA INCERTIDUMBRE ES LA CONSTANTE

DEBEMOS APRENDER A VIVIR CON ELLA

“UN CIBERATAQUE OCURRIRA”





POR QUE UNA METAFORA BIOLOGICA

- TODOS LOS SERES VIVOS HACEMOS PARTE DE UN MICELIO QUE NOS PERMITE EVOLUCIONAR PARA SOBREVIVIR EN UN MUNDO DE INCERTIDUMBRE.
- EN CIENCIAS SOCIALES ACUDIMOS A CONCEPTOS DE LA BIOLOGIA PARA EXPLICAR FENOMENOS O PARA ORDENARLOS, COMO SON POR EJEMPLO ORGANIZACIONES Y VIRUS.

CARACTERISTICAS DE LOS HONGOS

COMUNICAN

TRANSFORMAN

Están en todas partes

Lo que vemos es menos de lo que NO vemos

RESILIENTES

Tienen distintas apariencias

ANTIFRAGILES



LA AUDITORIA GENERAL DE LA REPUBLICA ESTA EN LA RED DE CONOCIMIENTO DEL CONTROL FISCAL Y...

- TIENE LA OBLIGACION DE PRESERVAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE SU INFORMACION EN EL CIBERESPACIO.
- SU INFORMACION PUEDE SER ATACADA EN CUALQUIER MOMENTO.
- PUEDE SUFRIR DAÑOS EN SU INFRAESTRUCTURA TECNOLÓGICA Y EN SUS DATOS.
- TIENE COLABORADORES QUE PUEDEN SER ENGAÑADOS CON INGENIERIA SOCIAL.
- TIENE ANTECEDENTES DE OTRAS ENTIDADES PUBLICAS QUE HAN SIDO ATACADAS
- ¿TIENE UN PLAN DE ACTUACION Y RESILENCIA ANTE CIBERATAQUES?
-



ENTONCES LA “AGR” PODRIA
CONSIDERAR



1.-ESTABLECER UNA LINEA DE ACTUACION EN TRES SEGMENTOS

ANTES

CONFIANZA

DURANTE

MIEDO

DESPUÉS

RESILIENCIA

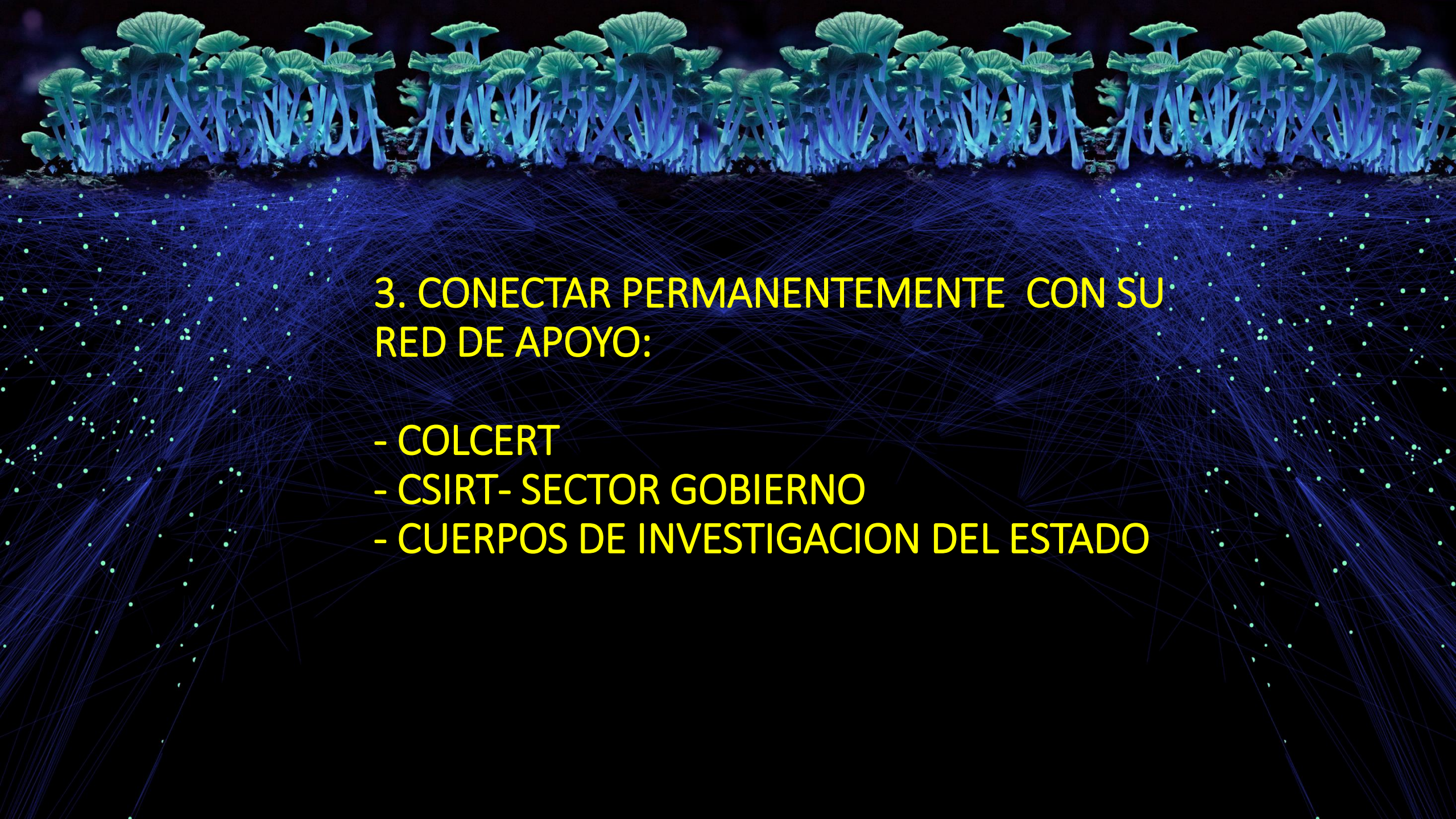
2. CONOCER SU TALENTO HUMANO



3 c

HV

BTSA



3. CONECTAR PERMANENTEMENTE CON SU RED DE APOYO:

- COLCERT
- CSIRT- SECTOR GOBIERNO
- CUERPOS DE INVESTIGACION DEL ESTADO



4. ESTABLECER SU PROTOCOLO DE GESTION DE INCIDENTES

- Activar el equipo de respuesta. (Líder y Vocero)
- Avisar a su red de apoyo. (CSIRT)
- Recibir y analizar información
- Definir el problema a solucionar
- Elaborar una lista de opciones para el problema
- Hacer una estrategia de soluciones
- Activar protocolo de gestión de medios y redes.
- Notificar a grupos de interés internos y externos
- Seguimiento hora a hora del problema
- Declarar paso a continuidad del negocio.



5. ESTABLECER SU PROTOCOLO DE CONTINUIDAD DEL SERVICIO

- Documentar el ataque con CSIRT.
- Informar a grupos de interés el resultado del informe forense.
- Listar lecciones aprendidas y compartirlas con su sector.
- Evaluar como opero el protocolo de incidentes y el CSIRT.



6. HACER ENTRENAMIENTO Y SIMULACION DE ATAQUES

- Simulacros.
- Ataques por terceros contratados



PONENCIA PRESENTADA ANTE LA AGR
POR:

JAIME EDUARDO SANTOS MERA

WWW.riesgosemergentesyconvergentes.com