

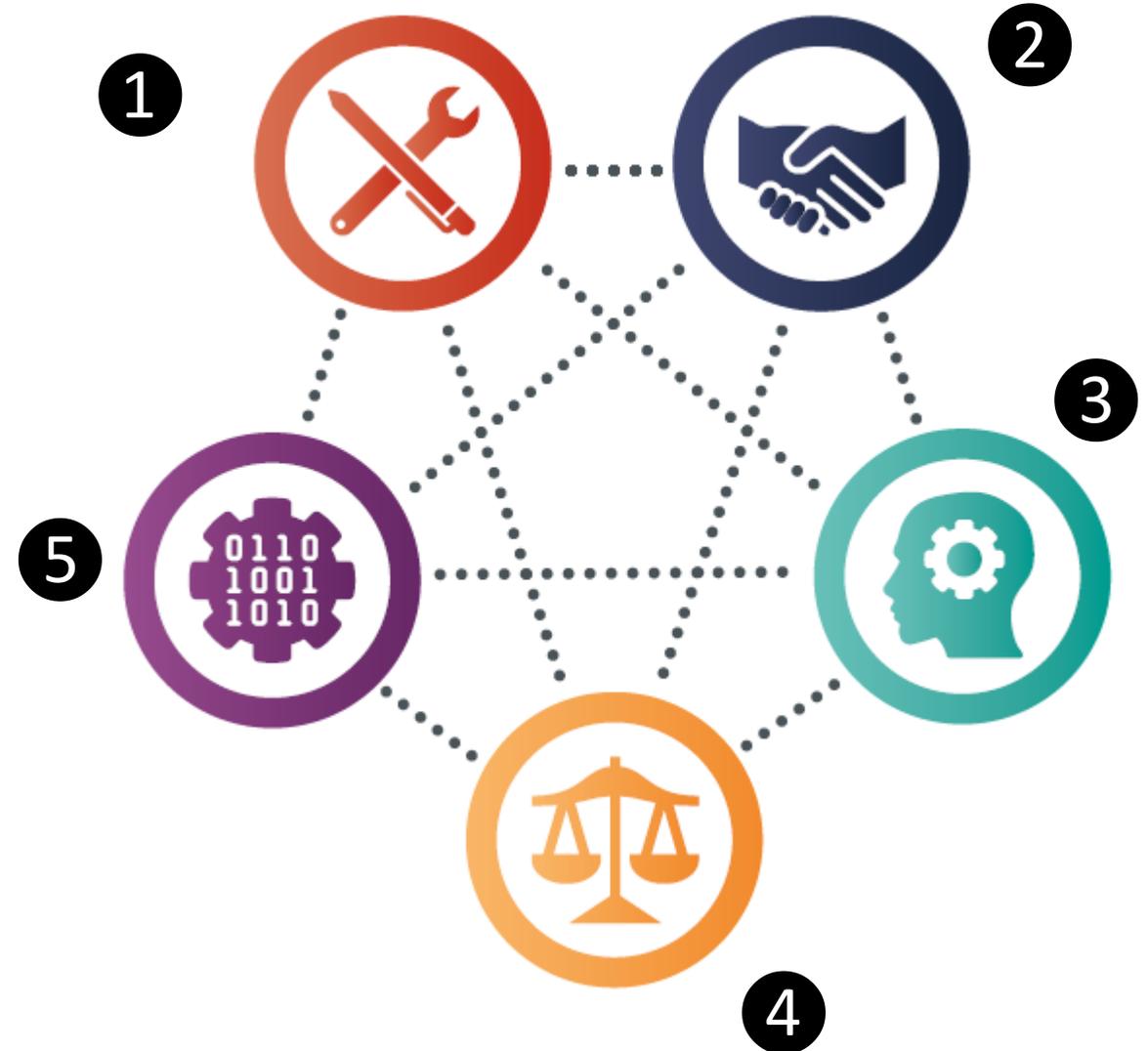


Panel Sesión 4: “Evolución de las amenazas. ¿Cómo responder? - Proyecciones en la Región - Cooperación público-privada”

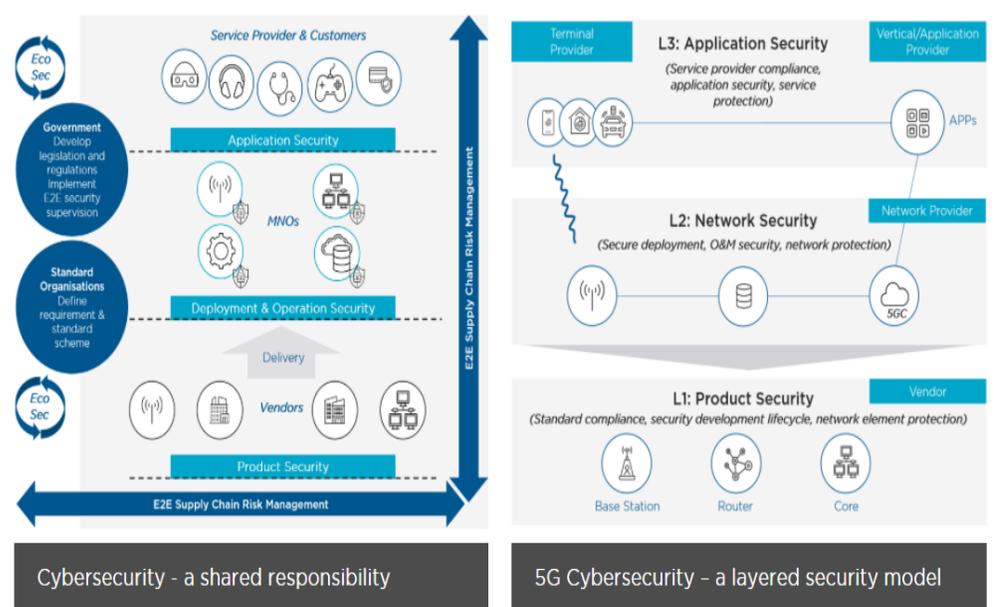
Un Modelo de Madurez en la Ciberseguridad en 5 dimensiones:

Pueden constituir la capacidad nacional para ser efectivo en la practica de Ciberseguridad:

- 1 Desarrollar una **Política y Estrategia** de Ciberseguridad;
- 2 Fomentar una **Cultura en la Sociedad** de ciberseguridad;
- 3 Desarrollar **Conocimientos y Capacidades** en ciberseguridad;
- 4 Adecuar los **Marcos Legales y Regulatorios** para que sean efectivos;
- 5 Control de Riesgos a través de **Estándares y Tecnologías**.



Base de Conocimiento de Ciberseguridad de la GSMA, establece una responsabilidad compartida que involucra a las partes interesadas clave en un modelo de 3 capas



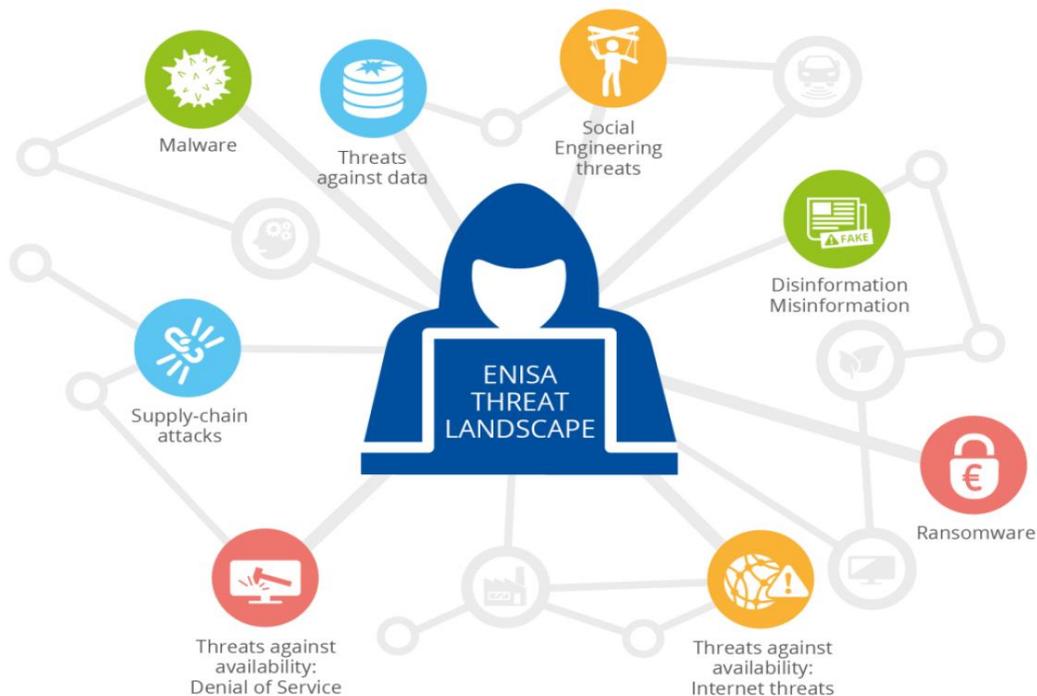
Capas de Seguridad:

- Las Aplicaciones** (Desarrolladores y Proveedores de Servicios)
- La Red** (comúnmente gestionada por Operadores)
- El/los Producto(s)** (seguridad de origen por Fabricantes)

Medidas de seguridad coordinadas y verificables basadas en estándares comunes.

Sistema de **Afianzamiento** de la **Ciberseguridad**
Cada parte de Huawei, y cada persona, está incrustada en la estrategia, control y gobernanza





1. Ransomware
2. Malware
3. Amenazas Ingeniería Social
4. Amenazas contra los datos
5. Amenazas contra la Disponibilidad:
 - Denegación de Servicio
 - Internet threats
6. Desinformación (intencional y sin darse cuenta)
7. Ataques a la Cadena de Suministro

Basicos de como Proteger tu Empresa y Negocio



Control de Acceso

Ponga controles en BD con información sensible. Limite el acceso a la necesidad de saber y solo por la cantidad de tiempo que el usuario necesita para hacer un trabajo.



Usar autenticación multi-factor

Esto hace que los proveedores tomen medidas adicionales además de iniciar sesión con una contraseña para acceder a su red, como un código temporal en un teléfono inteligente o una clave que es insertado en una computadora.



Poner seguridad en la Red

Requerir contraseñas seguras: al menos 12 caracteres con una combinación de números, símbolos y tanto en mayúsculas como en minúsculas. Nunca reutilice las contraseñas, no las comparta y limitar el número de intentos fallidos de inicio de sesión.



Salvagarde los datos y privacidad

Utilice una **cifrado segura y bien configurada**. Esto protege la información sensible como es transferido y almacenado.

- Email
- Dispositivos móviles
- Pagina Web Corporativa
- Redes Sociales y medios
- e-Commerce
- Online banking
- Politicas de Oficina de Traer su propio dispositivo
- Gestion de Redes
- Respaldos y acceso remoto







THANK YOU

