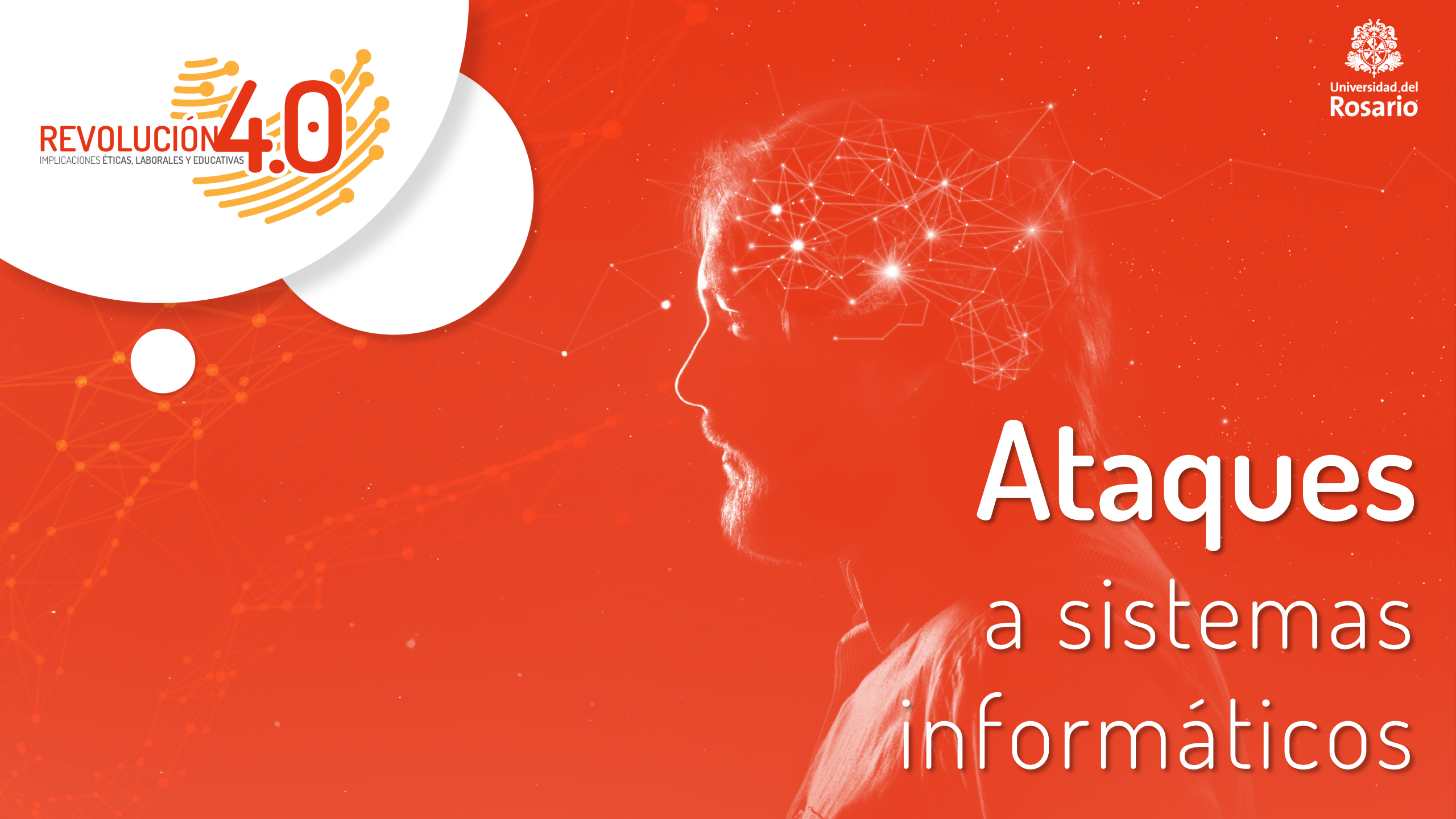
REVOLUCIÓN 4.0
IMPLICACIONES ÉTICAS, LABORALES Y EDUCATIVAS

Universidad del Rosario



Ataques a sistemas informáticos

Ataques a sistemas informáticos

El ciberespionaje

Una de las mayores preocupaciones para los gobiernos.

Ataques a sistemas informáticos

La ciberdelincuencia

Aumenta en frecuencia, variedad y amplitud de ataques a cambio de una recompensa.

Ataques a sistemas informáticos

El ciberterrorismo

Como instrumento facilitador de sus actividades, o como objeto de su acción para la comisión de actividades terroristas.

Ataques a sistemas informáticos

El hacktivismo

Ataques dirigidos por grupos movidos por una determinada ideología y que tienden a atacar la seguridad de los sistemas y la información.

Ataques a sistemas informáticos

La ciberguerra

Operaciones militares y aquellas otras orientadas a negar, modificar, llevar a engaño o destruir las capacidades propias residentes en los sistemas de información y telecomunicaciones que afecten a la defensa nacional.

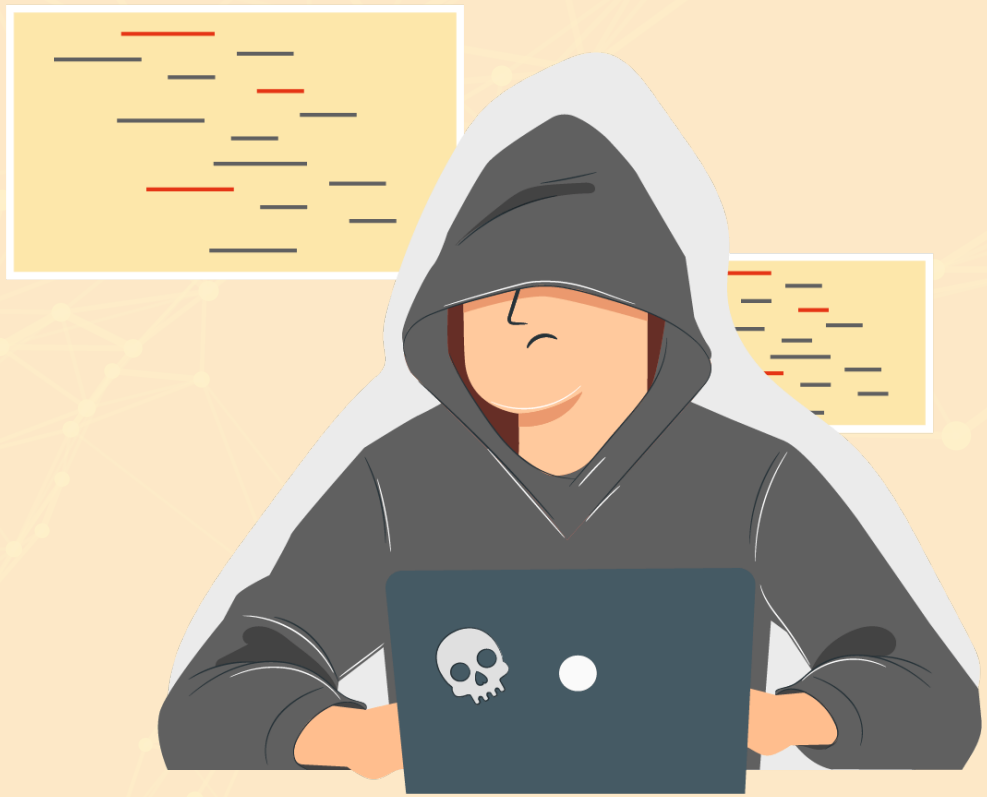
¿Cuáles son las recomendaciones frente a los ciberataques?

Defensa integrada

Las organizaciones demandan soluciones de seguridad integradas en lugar de puntuales, que permitan incluir la seguridad en todas partes y reforzarla en cualquier punto, desde el centro de datos (data center) hasta los terminales, las oficinas remotas y la nube (Cloud).

Servicios profesionales

La proliferación de amenazas avanzadas, dinámicas y persistentes, la creciente carencia de expertos en ciberseguridad y la fragmentación de la industria requiere que las organizaciones se apoyen en servicios profesionales efectivos.



Marco regulatorio global de ciberseguridad

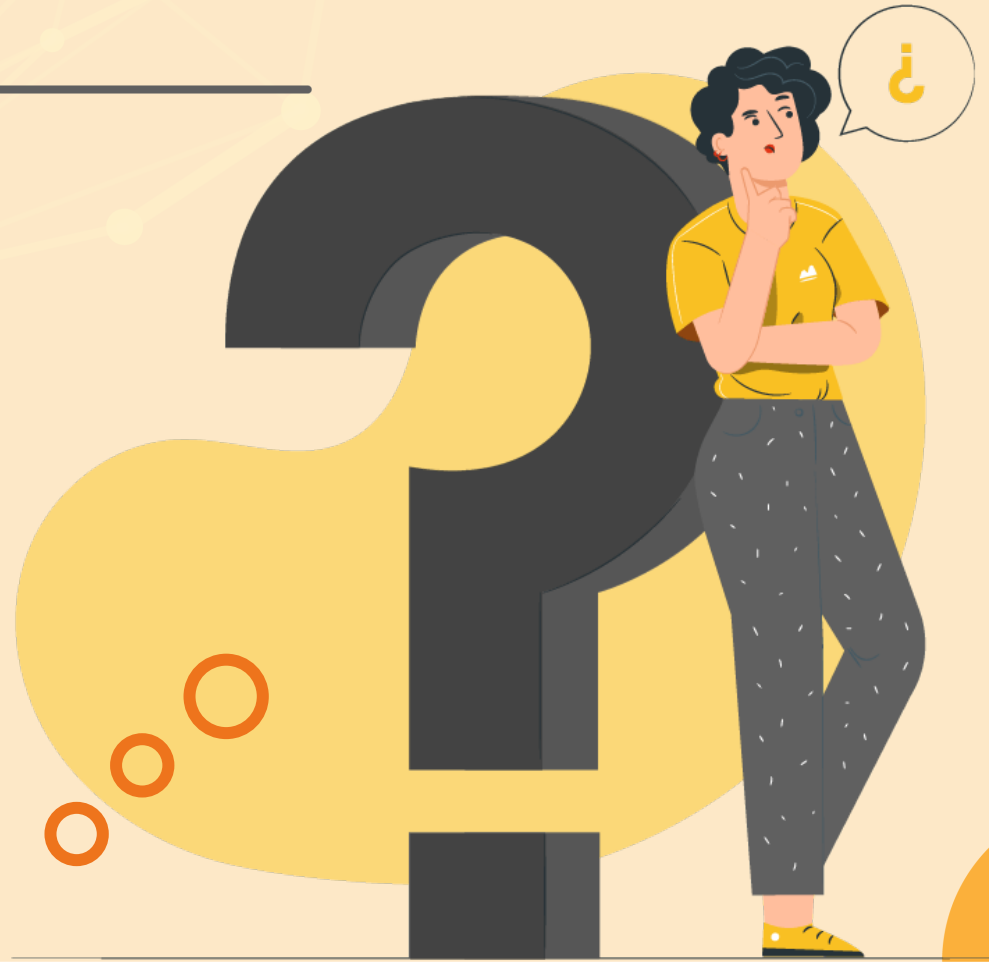
Es necesario establecer un marco regulatorio global y cohesionado en el que participen múltiples Gobiernos y empresas para evitar problemas jurisdiccionales a la hora de hacer frente a las ciberamenazas, resolver los problemas geopolíticos y sostener el crecimiento económico.

Proveedores contrastados

Para que un proveedor tecnológico pueda considerarse contrastado y fiable debe integrar la seguridad desde el principio, en todas sus soluciones y a través de todo su ciclo de vida, desde el proceso de desarrollo y test hasta la cadena de suministro y soporte.

¿Cuál es el decálogo de la ciberseguridad?

1. Analizar los riesgos.
2. Los responsables de seguridad.
3. Seguridad en el proyecto de trabajo.
4. La protección de la información.
5. Movilidad con seguridad.
6. Protección antimalware.
7. Actualización y parcheo.
8. La seguridad de la red.
9. Monitorización.
10. Seguridad gestionada.



Referencias

Joyanes. L. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). Cuadernos de estrategia, N.º. 185, 19-64. https://dialnet.unirioja.es/servlet/articulo?codigo=6115620