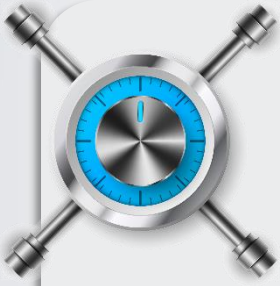
centro criptológico nacional

Zero Trust en redes corporativas



Es un modelo de seguridad de TI que requiere una verificación de identidad estricta para cada persona y dispositivo que intente acceder a los recursos de una red.

El modelo tradicional basado en el concepto de perímetro, donde se protege el acceso desde fuera y el usuario interno es de confianza, ya no es válido. La deslocalización de los datos en distintos centros de datos y nubes así como el acceso de terceros (proveedores e invitados) desde dentro y fuera de la red hace más difícil definir un perímetro.

"Nunca confiar, siempre verificar"

¿Por qué es tan importante la capa de acceso? Para implementar un modelo Zero Trust se debe tener visibilidad y control de la electrónica de red para después aplicar medidas de seguridad.

- Distribución de dispositivos con configuraciones por defecto.
- Incompleta visibilidad de la electrónica de red.
- Necesidad de procesos automáticos de auditoría de dispositivos.

Si un atacante accede a la red, tiene reinado libre sobre todo lo que hay dentro. Por lo tanto...

Deshabilite los protocolos de administración remota no cifrados que se utilizan en la infraestructura de red.

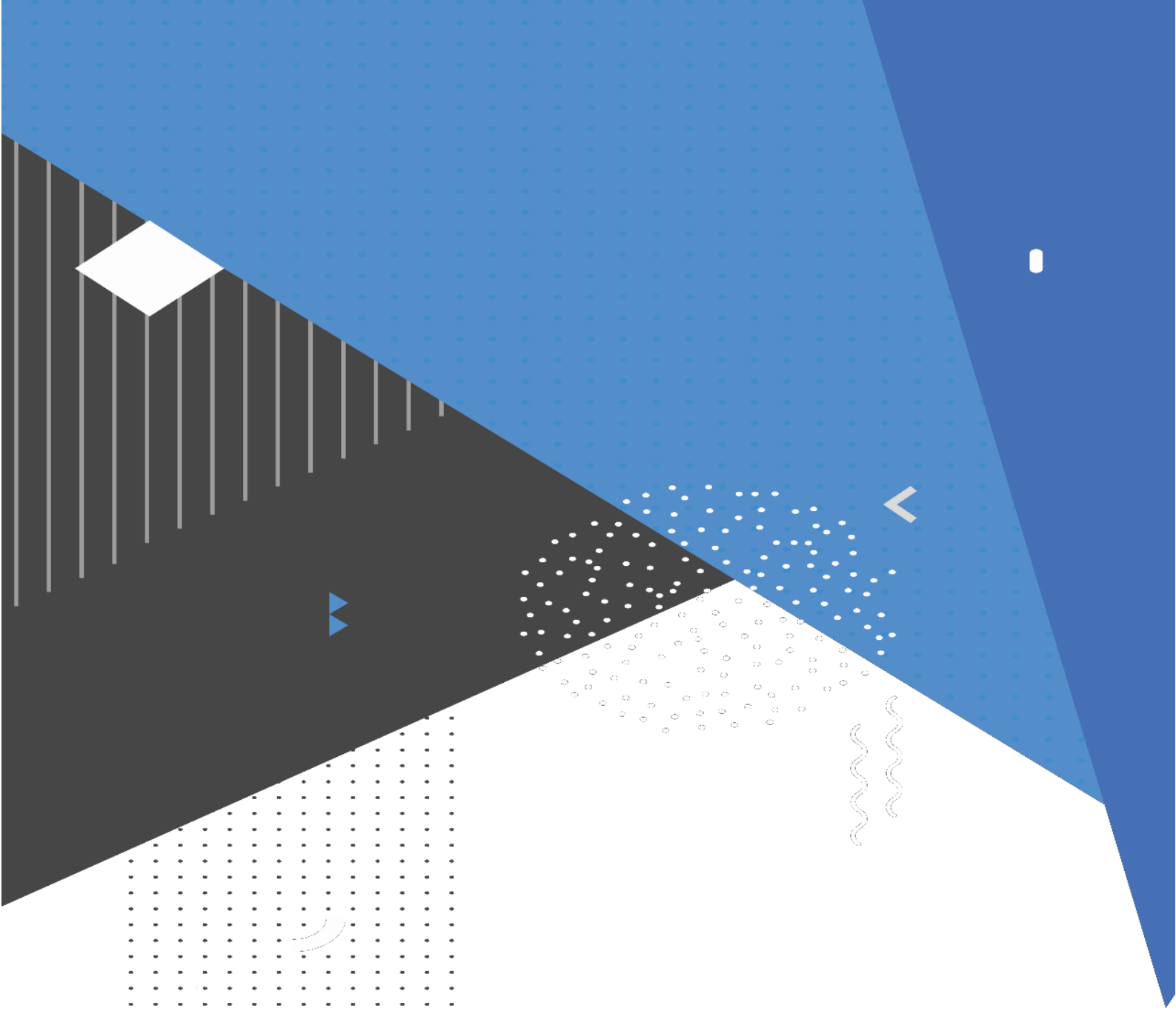
Desactive los servicios innecesarios.

Realice copias de seguridad de las configuraciones y almacénelas fuera de la red.

Una vez establecidas las medidas de seguridad, es importante **monitorizar y verificar continuamente las configuraciones** para asegurar que no ha habido cambios no deseados.

Base de un modelo Zero-Trust

- Conseguir visibilidad y contexto de cada dispositivo de red.
- Auditar los dispositivos según las guías del CCN-CERT y de manera continua para identificar cambios en las configuraciones.
- Corregir cambios o fallos de seguridad detectados en las auditorías.
- Establecer un proceso para monitorizar cualquier desviación.



centro criptológico nacional