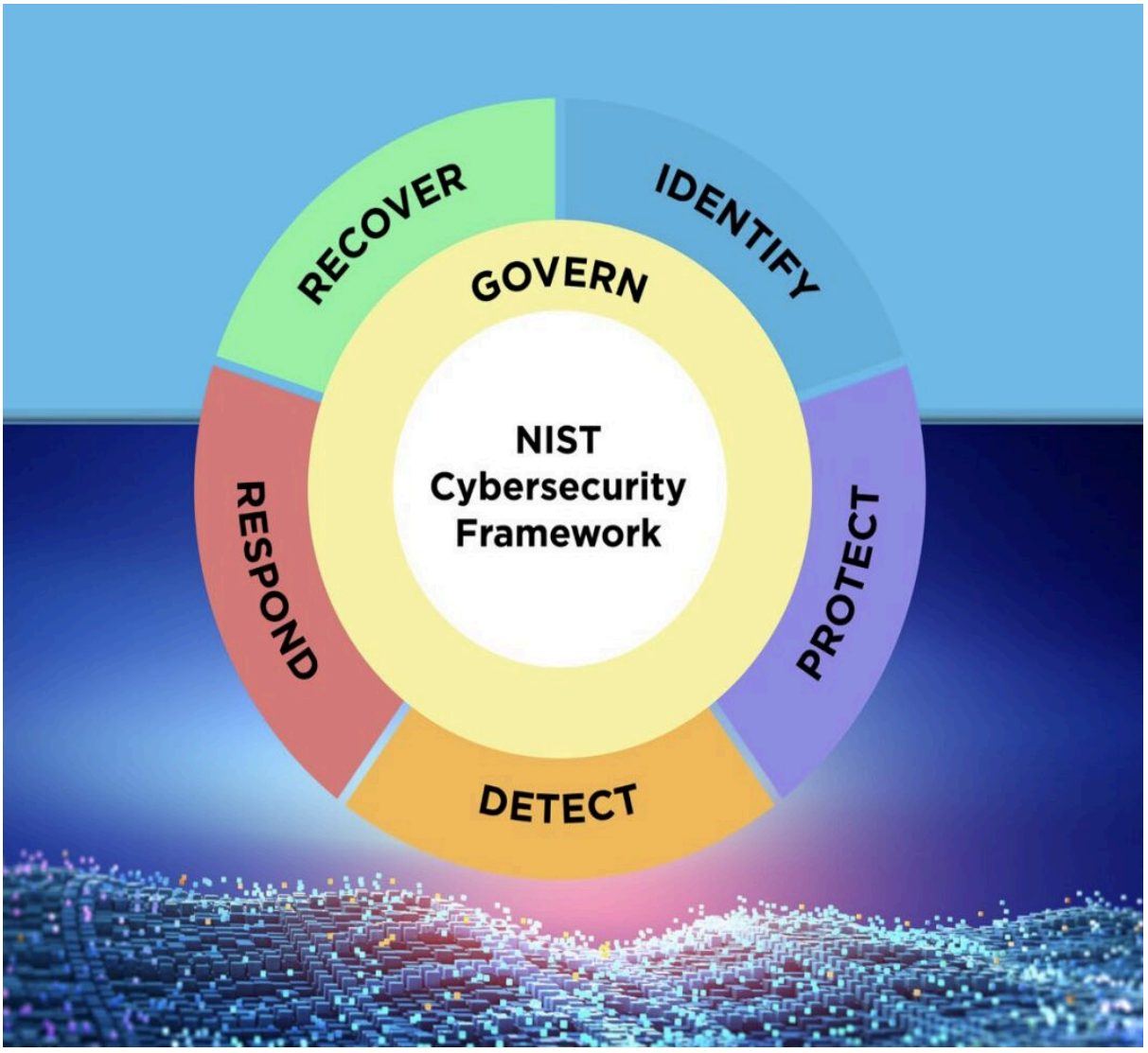
Daniel Hernandez
Curso de Ciberseguridad
2025

Introducción

A continuación aplicaremos las políticas del marco de Ciberseguridad del **NIST** que consiste en Identificar, Proteger, Detectar, Responder y Recuperar, las cuales ayudaran a la compañía a tener un plan organizado al momento de que la empresa sea vulnerada.



Identificación

Archivos Vulnerados: Servidor de Archivos, Bases de Datos de Clientes y sistemas de copias de seguridad.

Factores débiles: Faltas de segmentación en la red, ya que es una de las razones por las cuales el ransomware se movió bastante rápido. También falta de monitoreo y de alarma continuo ya que esto facilitó la intrusión en la empresa. Por último sería falta de conocimiento de los trabajadores ya que esta fue una de las causas por la que se infesto la compañía.

Protección

Segmentación en la Red: Implementar un firewall interno para así de esta manera apartar los archivos críticos como Bases de datos, copias de seguridad.

Capacitación a trabajadores: Implementar programas didácticos y de conocimientos sobre ransomware/phishing o simulacros dentro la empresa para que así mismo los trabajadores sepan cómo actuar en estos casos.

EDR/XDR: Endpoints y servidores con protección antivirus/anti ransomware avanzada y muy importante que cuente con proceso de detección y respuesta.

Detección

SIEM: Recopilación centralizada y correlación de logs de servidores, firewalls, endpoints, etc, para identificar patrones irregulares.

Monitoreo de Red (EDR): Detección de comportamiento irregular en la empresa y en los servidores.

Honeypots: Sistemas de anzuelo y detección para los usuarios maliciosos y así reconocer el ataque de manera temprana.

Respuesta

Aislamiento Inmediato: Desconectar los afectados de la red, ya sea físicamente o lógicamente.

Límites del Virus: Saber directamente qué sistemas han sido comprometidos y hasta donde se han llegado a cifrar los datos.

Análisis forense: Esto ayudaría a identificar el paso a paso del virus y lo que ha llegado a dañar.

Por último sería eliminar el ransomware y cualquier puerta trasera.

Recuperación

Recuperación de Datos: Restaurar todos los datos y sistemas afectados desde copias de seguridad verificadas.

Reconstrucción de sistemas: Reconstruir los sistemas críticos "desde cero" con configuraciones seguras y parches actualizados para garantizar que no quede ningún rastro del ransomware.

Verificación y Pruebas: Probar muchas veces los sistemas y datos restaurados para asegurar su funcionalidad e integridad antes de volver a ponerlos en producción. Este método lo podremos usar con la ayuda de Máquinas virtuales.