Coronado Noriega Jesús Olaf - 178991

Escenario	Servicios X.800 Comprometidos	Definición RFC 4949	Tipo de Amenaza	Medida de Control Recomendada
01 (LockBit)	Confidencialidad, Integridad, Disponibilidad	Multi-stage attack, Data breach	Externa (Cibercrimen)	Respaldos inmutables y EDR.
02 (Nube)	Control de acceso, Confidencialidad	Misconfiguration, Exposure	Interna (Error)	Auditoría CSPM y políticas IAM.
03 (Supply)	Integridad, Confidencialidad	Supply chain attack	Externa (Terceros)	Firmas digitales y análisis SBOM.
04 (Phishing)	Autenticación, Control de acceso	Credential compromise	Externa (Soc. Eng.)	MFA y concientización.
05 (Backups)	Disponibilidad, Integridad	Data destruction, Availability attack	Externa (Sabotaje)	Copias offline (3-2-1 rule).
06 (Insider)	Confidencialidad, Control de acceso	Insider threat	Interna (Maliciosa)	DLP y Mínimo Privilegio.
07 (Logs)	Integridad, No repudio	Audit trail violation	Mixta (Ocultamiento)	SIEM y Logs inalterables.
08 (Fallo)	Disponibilidad	Operational failure	Interna (Proceso)	Entornos de Staging y Rollback.
09 (Masq.)	Autenticación, Confidencialidad	Masquerade, Phishing	Externa (Suplantación)	DMARC y certificados SSL/TLS.
10 (Destr.)	Confidencialidad, Integridad, Disponibilidad	Destructive attack	Externa (Ataque total)	Respuesta a Incidentes (IRP).

Actividad 2

Materia: Seguridad Informatica