

Cristian Camilo Perez

Emmanuel Rodriguez

Caso	Tipo de ataque o vulnerabilidad	Evidencias o síntomas	Herramienta o acción de mitigación
1	Phishing	Solicitud de datos sensibles; solicitud masiva a los empleados de la empresa.	Campañas de concienciación y formación; filtros anti-phishing en correo; reportar y bloquear remitentes sospechosos.
2	DDoS	La red está colapsada por solicitudes simultáneas; el tráfico proviene de múltiples IPs, indicando un ataque distribuido.	Rate limiting, reglas de firewall; bloquear IPs maliciosas, subnetting monitorizar y realizar análisis del tráfico.
3	compromiso de IoT (cámaras IP)	Las cámaras IP del edificio se reinician solas y transmiten a direcciones extrañas.	Aislar las cámaras (VLAN/segmentación); cambiar credenciales por defecto y aplicar contraseñas fuertes; actualizar firmware, monitorizar tráfico y logs; habilitar acceso de administración seguro (HTTPS/SSH) y usar VPN para la gestión remota.