UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Guía de Ciberataques

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Análisis Integral del Panorama de Ciberamenazas y Vulnerabilidades Operativas

Documento Original: Guía de Ciberataques - INCIBE / OSI (España) [cite: 1]

Dominio: Ciberseguridad y Gestión del Riesgo Tecnológico

1. Introducción y Propósito del Informe

El presente informe constituye un análisis técnico estructurado del documento oficial «Guía de ciberataques: Todo lo que debes saber a nivel usuario», publicado por el Instituto Nacional de Ciberseguridad de España (INCIBE) [cite: 1]. El objetivo esencial de este documento es traducir conceptos de seguridad digital compleja en un marco analítico de toma de decisiones estratégicas, evaluando la anatomía de los vectores de ataque contemporáneos, los riesgos asociados para la infraestructura de la información y la efectividad de las salvaguardas propuestas [cite: 1].

> **Visión del Especialista**
> *La ciberseguridad corporativa e individual ya no puede tratarse únicamente como un problema del departamento de TI; constituye un pilar central de la continuidad operativa y la resiliencia organizacional. El factor humano sigue siendo la frontera más crítica y el blanco predilecto de la ingeniería social moderna [cite: 1, 9].*

2. Taxonomía de los Vectores de Ataque

El documento de INCIBE clasifica las amenazas en cuatro categorías principales [cite: 1]. A continuación se detalla la mecánica operativa, el impacto de riesgo y las mitigaciones específicas para cada vector [cite: 1].

2.1. Compromiso de Credenciales y Contraseñas

A pesar del avance de los mecanismos de autenticación biométrica y tokens contextuales, la contraseña sigue siendo el punto primario de falla en la gestión de identidades [cite: 1, 4].

Ataques de Fuerza Bruta: Consiste en la generación combinatoria sistemática (ensayo y error) de claves de acceso [cite: 5]. El atacante utiliza algoritmos automatizados que prueban primero datos conocidos de la víctima (fechas, nombres) y luego permutaciones alfanuméricas complejas hasta vulnerar la autenticación [cite: 5].

Optimización de la fuerza bruta mediante el uso de listas predefinidas de palabras, términos comunes y combinaciones previamente filtradas en brechas de datos masivas [cite: 6]. Es altamente efectivo contra políticas de contraseñas laxas o repetitivas [cite: 4, 6].

Vulnerabilidades asociadas: Reutilización de credenciales en múltiples plataformas, uso de patrones predecibles (ej. Mayúscula + palabras de 4 letras + números/símbolos) y el almacenamiento plano o sin cifrado en navegadores [cite: 4]. Mitigación obligatoria: Implementación rígida de Autenticación Multifactor (MFA/2FA) y gestores corporativos de contraseñas [cite: 5, 6].

2.2. Ingeniería Social y Manipulación Humana

La ingeniería social explota la psicología humana (urgencia, autoridad, curiosidad) en lugar de las vulnerabilidades del software [cite: 7].

Phishing, Smishing y Vishing: Despliegue de comunicaciones fraudulentas mediante correo electrónico, SMS o llamadas de voz para suplantar a entidades de confianza (bancos, entidades públicas, soporte técnico) [cite: 8]. Su meta es capturar credenciales o desplegar cargas

maliciosas [cite: 8, 9]. El Spear Phishing ajusta este vector dirigiendo el ataque hacia individuos con acceso privilegiado mediante inteligencia previa [cite: 8].

Baiting (Cebo): Uso de incentivos físicos (memorias USB infectadas dejadas en instalaciones públicas o corporativas) o digitales (promociones falsas) que incitan a la víctima a ejecutar malware impulsada por la curiosidad o el beneficio percibido [cite: 10].

Shoulder Surfing: Observación visual directa no autorizada de credenciales o datos sensibles ingresados en dispositivos en espacios públicos o áreas no protegidas [cite: 11]. Mitigación: Uso de filtros de privacidad físicos e integración de gestores de credenciales [cite: 11].

Dumpster Diving: Recolección y análisis de documentación física desechada o componentes de almacenamiento no destruidos adecuadamente para extraer información confidencial empleada en fases posteriores del ataque [cite: 12]. Mitigación: Políticas strictas de destrucción documentaria (triturado) y borrado seguro de hardware [cite: 12].

2.3. Intercepción y Vulneración de Conexiones de Red

Los ataques a la capa de red buscan interceptar, alterar o redirigir el tráfico de datos entre el cliente y el servidor [cite: 15].

Redes Trampa (Rogue APs): Despliegue de Puntos de Acceso Wi-Fi falsos con SSIDs idénticos o similares a redes legítimas [cite: 16]. Permiten al atacante capturar datos no cifrados (HTTP) o realizar inyecciones de código [cite: 16]. Mitigación: Desactivar la conexión automática a Wi-Fi abiertas y utilizar túneles VPN cifrados [cite: 16].

Técnicas de Spoofing (Suplantación): Falsificación de identidades en diversos niveles de la capa OSI: IP Spoofing (falsificación de cabeceras IP para saltar controles ACL o lanzar ataques DDoS) [cite: 18], Web Spoofing (clonación de portales web para captura de credenciales) [cite: 19], Email Spoofing (falsificación de cabeceras de correo) [cite: 20] y DNS Spoofing (envenenamiento de tablas DNS para redirigir tráfico a sitios fraudulentos) [cite: 21].

Ataques a Cookies de Sesión: Captura (Cookie Hijacking) o alteración (Cookie Poisoning) de la información de sesión almacenada en navegadores debido a la falta de cifrado en el tránsito (protocolos HTTP) [cite: 22, 23].

Ataques DDoS: Ataque por Denegación de Servicio Distribuido en el que una botnet de equipos comprometidos satura los recursos de un servidor mediante peticiones masivas para inhabilitar su disponibilidad [cite: 24]. Mitigación: Balanceo de carga, limitación de tasa (rate limiting) y Firewalls con detección anómala [cite: 25].

Inyección SQL (SQLi): Inyección de sentencias SQL maliciosas en campos de entrada de aplicaciones web no validados [cite: 26]. Permite a los atacantes leer, modificar o destruir bases de datos completas [cite: 26]. Mitigación: Consultas preparadas (Prepared Statements) y sanitización estricta de entradas a nivel de desarrollo [cite: 26].

Man-in-the-Middle (MitM) y Sniffing: Posicionamiento del atacante en el flujo de comunicación entre dos extremos para interceptar, auditar o modificar el intercambio de datos en tiempo real [cite: 28]. Complementado con herramientas de Sniffing (captura pasiva de paquetes) [cite: 29].

2.4. Amenazas por Software Malicioso (Malware)

El malware abarca programas desarrollados con la finalidad explícita de ejecutar acciones dañinas en los sistemas informáticos [cite: 30].

Virus y Gusanos: Software autorreplicante que altera o corrompe archivos del sistema [cite: 31]. Se propaga adjunto a ejecutables legítimos o soportes extraíbles [cite: 31].

Spyware y Adware: Software diseñado para recolectar actividades del usuario, capturar pantallas, conversaciones o grabaciones de audio/video sin autorización [cite: 33]. El Adware se enfoca en la saturación publicitaria no deseada [cite: 32].

Troyanos y Variantes Especializadas: Malware camuflado como aplicaciones legítimas [cite: 34]. Incluye subclases especializadas: Backdoors (puertas traseras de acceso remoto) [cite: 35], Keyloggers

(registro de pulsaciones de teclado) [cite: 36] y Stealers (extracción masiva de credenciales y cookies del sistema) [cite: 37].

Ransomware: Una de las amenazas de mayor impacto financiero e institucional [cite: 38]. Cifra los datos clave del sistema objetivo y exige el pago de un rescate económico a cambio de la clave de descifrado [cite: 38]. Mitigación: Copias de seguridad fuera de línea (air-gapped) y aislamiento de redes [cite: 38, 45].

Rootkits: Conjunto de herramientas que otorgan acceso administrativo persistente y oculto al sistema, escondiendo archivos y procesos a las herramientas de seguridad convencionales [cite: 40].

Criptojacking: Uso no autorizado del procesamiento de CPU/GPU del sistema víctima para el minado de criptomonedas, degradando el hardware y saturando el consumo energético [cite: 43].

3. Matriz Estratégica de Protección y Buenas Prácticas

Frente a este ecosistema multipartito de amenazas, la guía de INCIBE plantea un Decálogo de Buenas Prácticas que constituye una arquitectura de defensa en profundidad [cite: 1, 45]. A continuación se sintetizan las salvaguardas operativas indispensables:

Dominio de Control	Salvaguarda Recomendada (INCIBE)	Impacto / Riesgo Mitigado
Gestión de Identidades	Uso de contraseñas complejas, gestores dedicated y MFA activo en todo servicio [cite: 5, 45].	Elimina el 99% de ataques por Fuerza Bruta y Diccionario [cite: 5, 6].
Seguridad de Endpoints	Antivirus EDR actualizado, parches del SO al día y	Detiene la ejecución de Ransomware, Troyanos y Rootkits

	auditoría de permisos de Apps [cite: 44, 45].	[cite: 38, 40, 45].
Seguridad en Redes	Uso estricto de HTTPS/VPN, desactivación de Auto-Wi-Fi y filtrado en routers [cite: 16, 18, 45].	Previene MitM, Sniffing, Rogue APs y Spoofing de tráfico [cite: 16, 18, 28].
Cultura y Concienciación	Verificación de remitentes, análisis de URLs y escepticismo ante incentivos [cite: 9, 45].	Neutraliza Phishing, Smishing, Vishing y Baiting [cite: 8, 10, 45].
Resiliencia de Datos	Ejecución de respaldos periódicos (3-2-1) y destrucción física/digital segura [cite: 12, 45].	Mitiga el impacto de secuestro de datos por Ransomware y Dumpster Diving [cite: 12, 38, 45].

4. Conclusiones y Recomendaciones de Gestión

1. Integración de la Ciberseguridad en la Cultura Organizacional: Como destaca INCIBE, hasta el 95% de los incidentes de seguridad digital tienen su origen en fallas o descuidos humanos [cite: 9, 10]. La implementación de un programa de concienciación continuo es de carácter imperativo [cite: 9].

2. Mínimo Privilegio y Autenticación Fuerte: Las empresas y usuarios deben erradicar la reutilización de claves y adoptar arquitecturas de Confianza Cero (Zero Trust) impulsadas por la autenticación multifactor [cite: 4, 5, 45].

3. Mantenimiento y Gestión de Vulnerabilidades: La actualización oportuna de sistemas operativos, navegadores y firmware de red es la medida defensiva con mayor retorno de inversión técnica para cerrar brechas explotadas por gusanos y botnets [cite: 25, 39, 41].