Introducción a la Ciberseguridad

Teoría: Javier Díaz
jdiaz@unlp.edu.ar
Práctica: Soledad Gomez
Ulises Cabrera

Riesgos al Usar Cargadores USB Públicos

- **Juice Jacking**: instalación de malware o extracción de datos a través del puerto USB.
- Intercepción de información (contactos, credenciales, archivos personales).
- Instalación de perfiles o certificados falsos mediante conexión USB.
- Ataques a nivel de firmware o controladores del sistema.

Mitigación:

- Usar solo cargadores/cables propios o power banks.
- Emplear adaptadores 'USB data blocker' o modo 'solo carga'.
- Mantener el dispositivo bloqueado y actualizado.

Riesgos de Seguridad del Bluetooth

- **BlueSnarfing**: robo de contactos, mensajes o archivos.
- **BlueBugging**: control remoto parcial del teléfono (llamadas, mensajes AT).
- **BlueJacking**: envío de mensajes o archivos no solicitados.
- **BlueBorne**: ejecución remota de código sin emparejamiento.
- Rastreo por dirección MAC estática.

Mitigación:

- • Desactivar Bluetooth cuando no se use.
- • Evitar modo 'descubrible' permanente.
- • Actualizar OS y firmware regularmente.

vulnerabilidades rastreadores Bluetooth Tile

- No encriptan las transmisiones ni rotan la dirección MAC, exponiendo datos de ubicación: Esto permite que terceros (o la empresa) rastreen al usuario sin autorización.

https://www.eff.org/deeplinks/2025/10/tiles-lack-encryption-danger-users-everywhere

Riesgos para la Privacidad

- La política de privacidad contradice la falta de cifrado en las comunicaciones.
- El modo “anti-robo” impide que la víctima detecte el rastreador.
- La empresa Life360 podría acceder a los datos de ubicación sin protección.

RECOMENDACIONES

- Implementar cifrado extremo a extremo y rotación de direcciones MAC.
- Adoptar buenas prácticas de seguridad de Apple, Google y Samsung.
- Priorizar la privacidad del usuario sobre la funcionalidad del producto.

Buenas Prácticas de Seguridad - Apple

- Emparejamiento seguro con cifrado de clave pública (P-256).
- Cifrado de datos en reposo y en tránsito.
- Permisos Bluetooth explícitos por app.
- Alertas ante rastreadores desconocidos.
- Colaboración Apple–Google para detección de seguimiento no deseado.

Buenas Prácticas - Google / Android

- Modelo de seguridad con verificación de arranque y sandboxing.
- Permisos de acceso restringidos para Bluetooth y datos sensibles.
- Monitoreo de apps con Google Play Protect.
- Declaración de privacidad obligatoria en Google Play (Data Safety).
- • Actualizaciones y parches de seguridad frecuentes.

Buenas Prácticas - Samsung (Knox)

- Plataforma Samsung Knox: aislamiento de datos a nivel hardware y software.
- Cifrado avanzado para almacenamiento local y copias de seguridad.
- Detección de modificaciones no autorizadas.
- Control granular de permisos y funciones biométricas.
- Integración con políticas Android y gestión empresarial segura.

Colaboración Apple–Google: IETF DULT 2023

- Permite que iOS y Android detecten rastreadores Bluetooth desconocidos, sin importar el fabricante.
- Genera alertas automáticas cuando un dispositivo desconocido se mueve con el usuario.
- Compatible con iOS 17.5, Android 6.0+ y rastreadores Tile, Samsung, Chipolo, entre otros.
- Posibilita hacer sonar el rastreador para encontrarlo.
- Mejora la interoperabilidad y la protección contra el acoso mediante Bluetooth.

Bases de datos de Vulnerabilidades

CVE – Common Vulnerabilities and Exposures

- sistema estandarizado de identificación de vulnerabilidades, gestionado por MITRE Corporation con apoyo de la comunidad internacional.
- Cómo funciona: Cada vulnerabilidad recibe un identificador único del tipo CVE-AAAA-NNNN (ejemplo: CVE-2017-0144, asociado al ransomware WannaCry).
- Objetivo: Tener un lenguaje común para que investigadores, fabricantes y equipos de seguridad hablen de la misma vulnerabilidad sin ambigüedades.
- Limitaciones: CVE es solo un identificador y descripción básica, no incluye métricas de riesgo ni parches técnicos detallados. Referencia oficial: MITRE CVE
- https://www.cve.org/

Bases de datos de Vulnerabilidades

NVD – National Vulnerability Database

- **Qué es: Base de datos mantenida por el NIST (EE.UU.), basada en CVE.**
- **Cómo funciona: Amplía la información de los CVE agregando:**
  - **CVSS (Common Vulnerability Scoring System): puntaje de severidad (0 a 10).**
  - **CPE (Common Platform Enumeration): plataformas afectadas (sistema operativo, versión, fabricante).**
  - **CCE (Common Configuration Enumeration): configuraciones inseguras relacionadas.**
  - **Información de parches y enlaces a avisos de seguridad de proveedores.**
- **Ejemplo: El mismo WannaCry (CVE-2017-0144) figura en la NVD con un CVSS v3.0 = 8.1 (Alta severidad), detalles técnicos y enlaces a soluciones.**

https://nvd.nist.gov/

Relación entre CVE y NVD

CVE: “Etiqueta” universal para una vulnerabilidad.
NVD: Expansión técnica de esa etiqueta con puntajes, metadatos y referencias para gestión de riesgos.
Ejemplo práctico:

- **CVE-2021-44228 → Identificador de la vulnerabilidad de Log4Shell.**
- **NVD → Clasifica esa vulnerabilidad como CVSS 10.0 (Crítico), lista versiones afectadas de Log4j, enlaces a parches y guías de mitigación.**

Ciberataque a Costa Rica

- Primer ataque 17/4/22 a los servidores del Ministerio de Hacienda de Costa Rica, inutilizo la Administración Tributaria Virtual (ATV) y el Sistema de Información Aduanera (TICA). Dos días después, el sitio web del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones fue hackeado. Horas más tarde, Conti atacó un servidor de correo electrónico del Instituto Meteorológico Nacional robando la información contenida en el mismo. Pidieron 20Musd
- El Grupo Hive 31/5/22 ataco la Caja Costarricense de Seguro Social y obligo a cerrar todos sus sistemas críticos, Historia Única Digital de Salud y el Sistema Centralizado de Recaudación. Pidieron 5Musd.efectos hasta junio inclusive

https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)#:~:text=The%20Conti%20Group%2C%20which%20claimed,companies%20operating%20in%20Costa%20Rica

Incremento Ciberataques

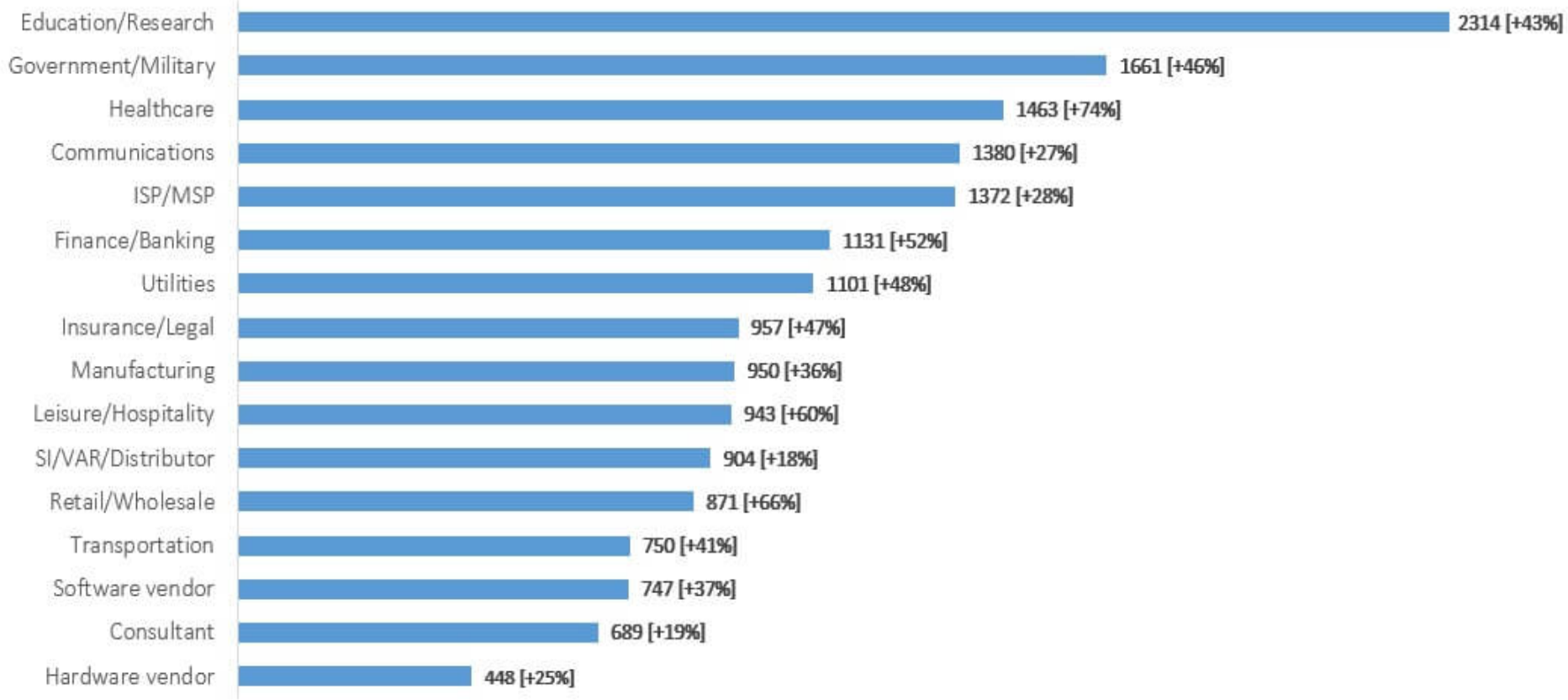
- **38%** es el porcentaje de incremento de los ciberataques en el año 2022 respecto del año anterior .
  https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/
- **30 %** aumento interanual de los ciberataques en el segundo trimestre de 2024, alcanzando 1636 ataques por organización por semana.
- Sectores más atacadas: Educación/Investigación (3.341 ataques por semana), Gobierno/Militar (2.084) y Salud (1.999).
- América Latina (+53%), África (+37%) y Europa (+35%) mostraron los mayores aumentos en ataques cibernéticos en el segundo trimestre de 2024, en comparación interanual.

Instituciones educativas europeas son el sector con más ciberataques: superan a Instituciones militares

- Estudio de Check Point realizado por su división de Inteligencia de Amenazas, ha analizado los ciberataques y amenazas recibidas en distintos sectores, desde enero a julio de 2023.
- En concreto, según los datos recabados, cada organización enmarcada en el sector de la educación o de la investigación ha recibido **una media de 2.256 ciberataques semanales** durante la primera mitad de 2023, mientras que el sector militar desciende la cifra a una media semanal de 1.759 ataques por organización. (11% de incremento)

- *https://tekiosmag.com/2023/09/08/instituciones-educativas-europeas-son-el-sector-con-mas-ciberataques-superan-al-militar/*

Avg. Weekly Cyber Attacks per Organinzation by Sector in 2022 showing all sectors suffer double-digit increase comapred to 2021



Mas de la mitad de las IES víctimas de ataques de *Ransomware* pagaron para recuperar datos

- Encuesta a más de 200 IES en 14 países.
- **63%,** utilizaron backups para restaurar sus datos, mientras que **56%** pagó el rescate.
- Las IES que utilizaron sus sistemas de respaldo de datos tuvieron menores costos de recuperacion **$980,000 libras esterlinas,** respecto de los que pagaron rescate **$1.3 million de libras esterlinas**.

- *https://www.highereddive.com/news/higher-education-ransomware-paid-ransom-college/689929/*

Noticias de Ciberataques Argentina

- Hackearon el INTA y piden un rescate de u$s 2 millones: hay 7000 afectados

https://www.cronista.com/infotechnology/actualidad/hackearon-al-inta-y-piden-un-rescate-de-us-2-millones-hay-7000-afectados/

- Por un hackeo, el INTA no puede utilizar sus radares meteorológicos en pleno temporal

https://www.infobae.com/economia/campo/2023/05/24/por-un-hackeo-el-inta-no-puede-utilizar-sus-radares-meteorologicos-en-pleno-temporal/

- Hackeo al INTA: Argentina lidera el ranking de ciberataques en la región. Un **promedio de 2.052 ataques semanales.**

https://news.agrofy.com.ar/noticia/204770/hackeo-inta-argentina-lidera-ranking-ciberataques-region

Incremento Ciberataques

- Ataque de ransomware a CONICET 20 abril del 2022, efectos mas de un mes

https://www.perfil.com/noticias/modo-fontevecchia/un-hackeo-anonimo-sigue-afectando-al-conicet-modof.phtml

- Ataque a la UBA desde 15/12/2023 con impacto hasta febrero

https://www.unvime.edu.ar/la-uba-sufrio-un-ciberataque-de-ransomware-docentes-y-alumnos-no-pueden-acceder-a-los-sistemas/

- La Argentina registró más de 262 millones de intentos de ciberataques durante el primer trimestre del 2024

*h*ttps://www.forbesargentina.com/innovacion/ciberataques-argentina-registraron-262-millones-intentos-intrusion-primer-trimestre-n53913

Ejercitar respuestas a Incidentes Ciberseguridad

- 287 días: Promedio de tiempo para detectar y contener un incidente de seguridad

https://venturebeat.com/security/report-average-time-to-detect-and-contain-a-breach-is-287-days

- Ejercicios para personal Directivo
  - Decisiones al máximo nivel
  - Perspectiva Legal
  - Perspectiva Económica Financiera
  - Perspectiva Comunicaciones

Impactos de un Ciberataque

- Impacto Económico Financiero
  - Directo
  - Indirecto
- Impacto en Imagen y Prestigio
  - Servicios directos
  - Redes sociales
- Otros Impactos
  - salud

Frameworks y Regulaciones en Ciberseguridad

1. NIST Cybersecurity Framework (CSF)

   Descripción: Publicado por el National Institute of Standards and Technology (EE.UU.), establece un marco de referencia para identificar, proteger, detectar, responder y recuperar frente a incidentes de ciberseguridad.

   https://www.nist.gov/cyberframework

2. ISO/IEC 27001:2022

   Descripción: Estándar internacional para la gestión de la seguridad de la información. Define requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

   https://www.iso.org/standard/27001

Funciones NIST Cybersecurity Framework, CSF 2.0

1. Identificar: Comprender los riesgos: activos, datos, sistemas, procesos, proveedores. Incluye Asset Management, Governance, Risk Assessment, etc.
2. Proteger: Implementar salvaguardas: control de acceso, capacitación, seguridad de información, tecnologías protectoras.
3. Detectar: Identificar eventos de seguridad mediante monitoreo continuo, detección de anomalías y procedimientos de detección.
4. Responder: Atender incidentes: planificación, comunicación, análisis, mitigación y mejora tras eventos.
5. Recuperar: Restaurar operaciones: planificación de recuperación, comunicación y aprendizaje para mejorar procesos futuros.
6. Gobernar: Enfocada en la estrategia, la gobernanza de la ciberseguridad y la supervisión organizacional

Familia ISO/IEC 27000

- Objetivo: proporcionar un marco común de referencia, conceptos y vocabulario para todas las normas de la serie.
- Enfoque principal :Definiciones y términos normalizados en seguridad de la información.
- Principios de gestión de la seguridad de la información.Introducción al enfoque de Sistema de Gestión de Seguridad de la Información (SGSI).
- Importancia: facilita la coherencia en la interpretación de las demás normas de la serie, asegurando un lenguaje unificado entre organizaciones, auditores y certificadores.

Familia ISO/IEC 27000, Núcleo SGSI

- **ISO/IEC 27000: conceptos y vocabulario.**
- **ISO/IEC 27001: requisitos para establecer, implementar, mantener y mejorar un SGSI (norma certificable).**
- **ISO/IEC 27002: código de buenas prácticas y controles de seguridad (guía para implementar ISO 27001).**
- **ISO/IEC 27003: guía de implementación del SGSI.**
- **ISO/IEC 27004: monitoreo, medición, análisis y evaluación del SGSI.**
- **ISO/IEC 27005: gestión de riesgos de seguridad de la información.**

Familia ISO/IEC 27000, Núcleo SGSI

Evaluación y Auditoria

- **ISO/IEC 27006: requisitos para organismos de certificación/acreditación de SGSI.**
- **ISO/IEC 27007: directrices para auditoría de SGSI.**
- **ISO/IEC 27008: guía para auditores en controles de seguridad.**

Familia ISO/IEC 27000, controles adicionales

- **ISO/IEC 27017: seguridad en servicios de cloud computing (controles adicionales).**
- **ISO/IEC 27018: protección de datos personales en la nube pública.**
- **ISO/IEC 27019: sector de energía (sistemas de control industrial).**
- **ISO/IEC 27011: telecomunicaciones (alineada con ITU-T X.1051).**
- **ISO/IEC 27014: gobernanza de la seguridad de la información.**
- **ISO/IEC 27031: continuidad del negocio y TIC.**
- **ISO/IEC 27032: ciberseguridad (directrices generales).**

Familia ISO/IEC 27000, controles adicionales…

- **ISO/IEC 27033 (serie): seguridad en redes.**
- **ISO/IEC 27034 (serie): seguridad en aplicaciones.**
- **ISO/IEC 27035 (serie): gestión de incidentes de seguridad.**
- **ISO/IEC 27036 (serie): seguridad en relaciones con proveedores.**
- **ISO/IEC 27037 a 27043: gestión y evidencia digital (forense).**
- **ISO/IEC 27040: seguridad para almacenamiento de datos.**
- **ISO/IEC 27050 (serie): descubrimiento electrónico (e-discovery).**

ISO /IEC 27000:2022

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commision) que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización

Visión general de las normas que componen la seria Principios y vocabulario	ISO 27000: 2016 (Primer versión: 2009)
Norma principal de la serie. Requisitos del SGSI	ISO 27001:2017 Primer versión: 2005
Buenas prácticas que describe los objetivos de control y controles recomendables	ISO 27002:2017 Primer versión: 2005

Frameworks y Regulaciones en Ciberseguridad…

3. CIS Critical Security Controls (CIS Controls)

Descripción: Conjunto de 18 controles de seguridad desarrollados por el *Center for Internet Security*, priorizados para mitigar amenazas más comunes.

Referencia: Center for Internet Security. (2023). *CIS Critical Security Controls v8*. https://www.cisecurity.org/controls

4. COBIT (Control Objectives for Information and Related Technologies)

Descripción: Framework de ISACA para gobernanza y gestión de TI, con un fuerte componente en la gestión de riesgos y seguridad de la información.

Referencia: ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. https://www.isaca.org/resources/cobit

CIS Controls v8 – Los 18 controles

Inventario y control de activos de empresa: Mantener un listado actualizado de todos los dispositivos autorizados en la red para prevenir usos no autorizados

Inventario y control de activos de software: Identificar y gestionar todas las aplicaciones instaladas, asegurando sólo software autorizado y actualizado

Protección de datos: Clasificar, gestionar y proteger datos sensibles mediante cifrado, controles de acceso y políticas de retención/eliminación seguras.

Configuración segura de activos de empresa y software: Aplicar configuraciones seguras en sistemas, servidores y aplicaciones,.

Gestión de cuentas y accesos: Controlar el ciclo de vida de las cuentas de usuario y privilegios, aplicando el principio de mínimo privilegio.

Gestión de acceso: Restringir y auditar accesos a sistemas y datos críticos, aplicando controles de autenticación robusta y revisiones periódicas.

CIS Controls v8 – Los 18 controles…

Gestión continua de vulnerabilidades: Identificar, priorizar y remediar vulnerabilidades conocidas mediante scans periódicos y parches.

Gestión de auditoría y registro (Logging & Monitoring): Generar, proteger y revisar logs de sistemas y aplicaciones críticos para detectar accesos indebidos o incidentes.

Protección de correo electrónico y navegador web: Aplicar filtros de contenido, listas negras, bloqueo de macros y protección contra phishing en el correo y navegadores.

Defensas contra malware: Uso de antimalware avanzado, listas blancas de aplicaciones y EDR (Endpoint Detection & Response).

Recuperación de datos: Respaldos periódicos (backup), verificados y protegidos contra manipulación, para recuperación después de incidentes.

CIS Controls v8 – Los 18 controles…

Gestión de infraestructura de red: Diseño seguro de redes (segmentación, firewalls, VLANs, VPNs), asegurando que solo el tráfico autorizado fluya.

Monitorización y defensa de red: Monitoreo continuo de tráfico, IDS/IPS, detección de anomalías y respuesta a incidentes en tiempo real.

Concienciación y formación en seguridad: Capacitación periódica, phishing, ingeniería social y buenas prácticas, fortaleciendo la “primera línea de defensa”.

Gestión de proveedores de servicio: Evaluar y supervisar a proveedores externos (cloud, outsourcing, SaaS), asegurando que cumplan con controles de ciberseguridad.

Gestión de seguridad en aplicaciones: Aplicar seguridad durante todo el ciclo de vida del software (DevSecOps), revisiones de código, pruebas de seguridad y control de librerías externas.

CIS Controls v8 – Los 18 controles…

Respuesta a incidentes: Planificar, probar y mejorar un IRP (Incident Response Plan) que permita detectar, responder, mitigar y aprender de incidentes.

Pruebas de penetración y ejercicios Red Team: Realizar pentesting y simulaciones de ataque para identificar debilidades que no se detectan con escaneos automáticos.

- **cada control incluye “Implementation Groups (IGs):**
  - IG1 = esenciales para pymes.
  - IG2 = medianas organizaciones.
  - IG3 = grandes/entornos críticos.

COBIT: Marco de Gobierno y Gestión de TI

Framework desarrollado por ISACA para gobernanza y gestión de la información y las tecnologías asociadas (IT Governance & Management).

- Conecta los objetivos del negocio con la estrategia y las operaciones de TI. Alinea TI con objetivos empresariales.
- Integra estándares como ISO/IEC 27001, ITIL, NIST y COSO.
- Asegura valor, optimiza recursos y mitiga riesgos.

Componentes del Modelo COBIT 2019

Principios de Gobernanza y Gestión:

- 1. Satisfacer necesidades de stakeholders.
- 2. Cobertura integral de la empresa.
- 3. Integración con marcos existentes.
- 4. Enfoque holístico.
- 5. Diferenciación entre gobernanza y gestión.

Componentes del Modelo COBIT 2019

Dominios principales:

- Governance (EDM): Evaluar, Dirigir y Monitorear.

- Management (APO, BAI, DSS, MEA): Planificar, Construir, Ejecutar y Monitorear.

Componentes: objetivos, procesos, políticas, cultura, información, personas, habilidades e infraestructura.

COBIT y la Ciberseguridad

- Define objetivos de control y gestión de riesgos que fortalecen la seguridad en todos los niveles organizacionales.
- Promueve la responsabilidad compartida entre dirección, TI y auditores.
- Alinea la estrategia de ciberseguridad con los objetivos de negocio y cumplimiento normativo.
- Favorece la madurez organizacional al identificar brechas en políticas, controles y gobernanza.
- • Se complementa con marcos técnicos como NIST CSF o ISO 27001.

Frameworks y Regulaciones en Ciberseguridad…

5. GDPR (General Data Protection Regulation – UE)

Descripción: Reglamento europeo sobre protección de datos personales y privacidad, aplicable a todas las organizaciones que procesen datos de residentes en la UE.
Referencia: Regulation (EU) 2016/679 of the European Parliament and of the Council.
https://gdpr-info.eu/

6. ISO/IEC 27032 (Cybersecurity Guidelines)

Descripción: Norma internacional que proporciona directrices específicas en ciberseguridad (distinguida de la seguridad de la información de ISO/IEC 27001).
Referencia: ISO/IEC 27032:2012. Guidelines for Cybersecurity.
https://www.iso.org/standard/76070.html

GDPR: Protección de Datos y Privacidad en la Era Digital

- Aplica a todas las organizaciones que procesen datos de residentes en la UE.
- Principios:
  - licitud,
  - transparencia,
  - finalidad,
  - minimización,
  - exactitud,
  - limitación del almacenamiento,
  - integridad
  - responsabilidad.

La Seguridad de la Información como Pilar del GDPR

- Exige medidas técnicas y organizativas para proteger los datos
- Vincula directamente la ciberseguridad con la protección legal de datos.
- Ejemplos de medidas:
  - Cifrado y seudonimización.
  - Control de acceso y autenticación.
  - Gestión de vulnerabilidades y resiliencia.
  - Protocolos de notificación de incidentes (72 h).
- • Se complementa con ISO 27001, NIST CSF y COBIT 2019.

Derechos y Responsabilidades en el GDPR

- El responsable del tratamiento debe demostrar cumplimiento (accountability).
- Derechos del usuario:
  - Acceso, rectificación y supresión (derecho al olvido).
  - Portabilidad, limitación y oposición.
- Requiere 'Privacy by Design' y 'Privacy by Default'.
- Sanciones: hasta el 4 % del volumen global de negocios anual.

Privacy by Design

Protección de datos desde el diseño y por defecto” (Privacy by Design & by Default).

- Los principios son:
  - Proactivo, no reactivo; preventivo, no correctivo.
  - Privacidad como configuración por defecto.
  - Privacidad incrustada en el diseño.
  - Funcionalidad total — ganar/ganar, no suma cero.
  - Seguridad de extremo a extremo — protección completa del ciclo de vida.
  - Visibilidad y transparencia.
  - Respeto por la privacidad del usuario — centrado en el individuo.

Tipos de Datos Personales en el GDPR

- Datos identificativos directos: nombre, DNI, email, imagen, voz.
- Datos indirectos: IP, geolocalización, ID de dispositivo, hábitos de uso.
- Datos sensibles (Art. 9): salud, biometría, ideología, religión, orientación sexual, origen étnico.
- Datos financieros y de menores: sujetos a consentimientos y controles específicos.

Implicancias técnicas:

- Requieren medidas de ciberseguridad proporcionales al riesgo.
- Los datos sensibles exigen cifrado fuerte, segmentación de acceso y monitoreo activo.

Ciberseguridad y Técnicas de Cifrado en el GDPR

- Cifrado de datos:
  - En tránsito: TLS 1.3, HTTPS, VPN, SSH.
  - En reposo: AES-256, ChaCha20, BitLocker, LUKS.
  - Cifrado homomórfico o seudonimización para análisis.
- Control de acceso y autenticación multifactor (MFA).
- Políticas de mínimo privilegio (Least Privilege) y registros de acceso.
- Resiliencia: backups cifrados, redundancia y planes de continuidad.
- Gestión de incidentes y comunicación a autoridades en 72 h.

Frameworks y Regulaciones en Ciberseguridad…

7. **CMMC (Cybersecurity Maturity Model Certification – EE.UU.)**

   Descripción: Modelo de madurez de ciberseguridad para contratistas del Departamento de Defensa de EE.UU.

   Referencia: U.S. Department of Defense. *CMMC Model v2.0*.
   https://www.cisa.gov/resources-tools/resources/cybersecurity-maturity-model-certification-20-program

8. HIPAA (Health Insurance Portability and Accountability Act – EE.UU.)

   Descripción: Norma que regula la seguridad y privacidad de la información médica y sanitaria.

   Referencia: U.S. Department of Health & Human Services. HIPAA Security Rule
   https://www.hhs.gov/hipaa/index.html

Frameworks y Regulaciones en Ciberseguridad…

9. PCI DSS (Payment Card Industry Data Security Standard)

Descripción: Estándar de seguridad de la industria de tarjetas de pago, obligatorio para entidades que procesan, almacenan o transmiten datos de titulares de tarjetas.
Referencia: PCI Security Standards Council. (2022). PCI DSS v4.0.
https://www.pcisecuritystandards.org/resources-overview/

10. Reglamento Europeo de Ciberseguridad.

Establece requisitos para la ciberseguridad de productos con componentes digitales, y la enmienda al Reglamento de Ciberseguridad de 2019 (Reglamento (UE) 2019/881), que amplía los esquemas de certificación a servicios de seguridad gestionados.

Referencia: Decreto EU 2024/2847

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202402847

Política Seguridad de la Información

- Modelo de Política de Seguridad de la Información para Organismos Públicos.

https://www.argentina.gob.ar/noticias/elaboran-modelo-de-politica-de-seguridad-de-la-informacion-para-organismos-publicos

- Requisitos mínimos de Seguridad de la Información para Organismos. Decisión Administrativa 641/2021 Jefatura de Gabinete de Ministros.
- Política de seguridad de la información de las Instituciones Universitarias Públicas.
    - Resolución C.E. CIN: 1669/22

Aspectos a incluir en Politica de Ciberseguridad

Protección de datos: El RGPD establece los requisitos específicos para empresas y organizaciones sobre recogida, almacenamiento y gestión de los datos personales. Se aplican tanto a las organizaciones europeas como a las organizaciones que tienen su sede fuera de la UE.

Responsable de Privacidad de la Información de la Organización, CPO

Datos personales

Privacidad

Derecho al olvido

Https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Privacidad: ejemplo de cookies

- Almacenar o acceder a información en un dispositivo
- Desarrollar y mejorar productos
- Utilizar estudios de mercado a fin de generar información sobre el público
- Medir el rendimiento de los anuncios
- Seleccionar contenido personalizado
- Crear un perfil para la personalización de contenidos
- Seleccionar anuncios básicos
- Seleccionar anuncios personalizados
- Crear un perfil publicitario personalizado
- Utilizar datos de localización geográfica precisa
- Medir el rendimiento del contenido
- Analizar activamente las características del dispositivo para su identificación

Estructura en Seguridad de la Informacion

- Organización: Política Seguridad de la Información
  - Comité de Ciberseguridad
  - CISO (Chief Information Security Officer) Reporta a la alta gerencia.
  - Definir la estrategia de ciberseguridad.
  - Gestionar políticas y cumplimiento normativo.
  - Evaluar y mitigar riesgos organizacionales.
  - Coordinar equipos (SOC, CSIRT, IT, Legal).
  - Comité de Ciberseguridad
- Director en Privacidad (CPO)
  - RGPD es el Reglamento General de Protección de Datos de la Unión Europea
  - CCPA (Ley de Privacidad del Consumidor de California)

Estructuras Ciberseguridad

- **SOC (Security Operations Center)**
  - **Monitorear** en tiempo real la infraestructura.
  - Uso de **SIEM, IDS/IPS, EDR**.
  - Detección y respuesta inicial a incidentes.
  - Generación de alertas y reportes.
- **CSIRT (Computer Security Incident Response Team)**
  - **Gestión completa de incidentes** (detección, contención, erradicación, recuperación).
  - Coordinación con organismos externos y reguladores.
  - **Análisis forense** y lecciones aprendidas.
  - Elaborar planes de **respuesta y continuidad**.

SOC (Security Operations Center)

- **Monitoreo en tiempo real de la infraestructura**
  - **Zabbix** / **Nagios** → monitoreo de infraestructura y servicios.
  - **Prometheus + Grafana** → métricas y dashboards en tiempo real.
  - **Elastalert** (con Elastic Stack) → alertas basadas en logs.

- **SIEM, IDS/IPS, EDR**
  - **Wazuh** → SIEM open source con correlación de eventos, integración con Elastic, capacidades de EDR.
  - **TheHive** → gestión de incidentes, integrable con Cortex y MISP.
  - **Suricata** → IDS/IPS de red con soporte para detección avanzada.
  - **Snort** → IDS/IPS muy usado en entornos SOC.
  - **Osquery** → para monitoreo y análisis de endpoints (similar a EDR).

SOC (Security Operations Center)…

- **Detección y respuesta inicial a incidentes**
  - **Cortex (integrado con TheHive) → automatiza respuestas y análisis de IOCs.**
  - **MISP (Malware Information Sharing Platform) → intercambio de indicadores de compromiso.**
  - **Velociraptor → recolección y análisis forense en endpoints.**

- **Generación de alertas y reportes**
  - **Elastic Stack (ELK: Elasticsearch, Logstash, Kibana) → procesamiento y visualización de logs.**
  - **Graylog → alternativa ligera para centralización de logs y dashboards.**
  - **Grafana Loki → recolección de logs con visualización en Grafana.**

CSIRT (Computer Security Incident Response Team)

- **Gestión completa de incidentes**
  - TheHive Project → plataforma de gestión de casos de incidentes.
  - RTIR (Request Tracker for Incident Response) → herramienta de tickets especializada en IR.
- **Coordinación con organismos externos y reguladores**
  - MISP → permite compartir indicadores de compromiso (IOCs) con comunidades y organismos.
  - OpenDXL (McAfee, open source) → para orquestar y compartir información de amenazas.

CSIRT…

- **Análisis forense y lecciones aprendidas**
  - **Autopsy / Sleuth Kit → análisis forense de discos e imágenes.**
  - **Volatility / Rekall → análisis forense de memoria.**
  - **Plaso (log2timeline) → análisis forense de líneas de tiempo de logs.**
- **Planes de respuesta y continuidad**
  - **DRLM (Disaster Recovery Linux Manager) → para gestión de recuperación ante desastres.**
  - **Odoo Community (con módulos IR/BCP) → ERP adaptable para documentar planes de continuidad.**
  - **LibreNMS + Ansible → automatización de restauración y continuidad en infraestructura.**

Combinación típica SOC/CSIRT open source:

Wazuh + ELK Stack + Suricata + TheHive + Cortex + MISP + Velociraptor

- **Recopilación de datos y monitorización de seguridad**
  - Wazuh: Host-based Intrusion Detection System (HIDS),
    - Log analysis: Análiza logs de diversas fuentes para detectar actividad sospechosa..
    - File integrity monitoring (FIM): Alerta modificación de archivos críticos del sistema.
    - Vulnerability detection: Identificación de software obsoleto y vulnerabilidades.
    - Configuration assessment: Comprobación de configuraciones incorrectas riesgosas .
  - Suricata: Network Intrusion Detection/Prevention System (NIDS/NIPS). Monitorea el tráfico de red en tiempo real para detectar amenazas basándose en reglas predefinidas (firmas) y análisis de comportamiento.

Combinación típica SOC/CSIRT open source…

- **Procesamiento y análisis de datos (SIEM): ELK Stack (Elasticsearch, Logstash, Kibana):**
  - **Logstash:** Ingiere y procesa datos de diversas fuentes (como Wazuh y Suricata), normalizándolos y enriqueciéndolos antes de almacenarlos**.**
  - **Elasticsearch:** motor de búsqueda y análisis. Es una base de datos altamente escalable que almacena todos los eventos de seguridad, lo que permite realizar búsquedas y correlaciones complejas rápidamente**.**
  - **Kibana:** La capa de visualización. Proporciona paneles y gráficos que permiten a los analistas de seguridad visualizar datos de seguridad, analizar alertas y realizar búsquedas de amenazas

Combinación típica SOC/CSIRT open source…

- **Respuesta a Incidentes y Automatización (SOAR)**
  - **TheHive: Security Orchestration, Automation, and Response (SOAR).** Una vez que el SIEM genera una alerta, los analistas de TheHive la utilizan para:
    - **o Crear y gestionar incidentes y casos.**
    - **o Colaborar en las investigaciones.**
    - **o Seguimiento del estado y el progreso de un incidente.**
  - **Cortex:** motor de análisis, funciona con TheHive. Cuando un analista identifica un posible indicador de compromiso (IOC), como una dirección IP, un hash de archivo o un nombre de dominio, Cortex puede enriquecer automáticamente los datos procesándolos a través de varios analizadores. Po.ej. puede comparar el hash de un archivo con VirusTotal o una dirección IP con fuentes de inteligencia de amenazas.

Combinación típica SOC/CSIRT open source…

- **Inteligencia de Amenazas y Respuesta en Endpoints**
    - **MISP (Malware Information Sharing Platform): Plataforma de Inteligencia de Amenazas (TIP). Recopila, comparte y correlaciona inteligencia de amenazas, mediante**
    - **o La ingesta de datos de amenazas de diversas fuentes.**
    - **o indicators of compromise (IOCs) compartirlos con la comunidad.**
    - **o Enriquecimiento de alertas en TheHive/Cortex con indicadores maliciosos conocidos, ayuda a los analistas a identificar actividad maliciosa.**
    - **Velociraptor:** : Herramienta de Visibilidad y Respuesta en Endpoints.
        - **o Digital y Respuesta a Incidentes (DFIR):** para realizar análisis forense en vivo en el endpoint afectado.
        - **o Threat Hunting:** Permite a los analistas escribir consultas personalizadas para buscar artefactos específicos en miles de endpoints simultáneamente, p.ej. un archivo malicioso, una clave de registro específica o un proceso en ejecución. Búsqueda proactiva de amenazas

Flujo de trabajo de seguridad integral:

- **Detección: Wazuh y Suricata** recopilan datos de endpoints y de red.
- **Análisis: ELK Stack** ingiere, almacena y analiza estos datos, generando alertas.
- **Respuesta: TheHive y Cortex** gestionan el proceso de respuesta a incidentes, automatizando el enriquecimiento de datos y proporcionando un entorno colaborativo.
- **Inteligencia: MISP** proporciona contexto al compartir y correlacionar la inteligencia de amenazas.
- **Remediación/Búsqueda: Velociraptor** permite un análisis forense exhaustivo y la búsqueda de endpoints.

Equipos operativos en Ciberseguridad

- **Red Team *(ataque controlado)***
- Simula ataques reales para probar defensas.
- Pentesting, explotación de vulnerabilidades.
- Genera insumos para fortalecer al Blue Team.

- **Blue Team *(defensa activa)***
- Refuerza defensas y responde a incidentes.
- Correlación de eventos, hardening, respuesta inmediata.
- Trabaja de la mano con SOC y CSIRT.

Herramientas open source SOC

Monitoreo en tiempo real de la infraestructura

- **Zabbix / Nagios → monitoreo de infraestructura y servicios.**
  - Zabbix y Nagios soluciones reconocidas para monitoreo de infraestructura de TI y disponibilidad de servicios. Permiten supervisar servidores, redes, aplicaciones y dispositivos mediante la recopilación de métricas, verificación de estados y detección de fallos.
  - Nagios, se destaca por su enfoque basado en plugins y su capacidad para notificar interrupciones en tiempo real.
  - Zabbix, ofrece una arquitectura más moderna, con soporte nativo para la recolección de métricas, visualización gráfica, descubrimiento automático de dispositivos y escalabilidad en entornos grandes.

Herramientas open source SOC…

Monitoreo en tiempo real de la infraestructura

- **Prometheus + Grafana → métricas y dashboards en tiempo real.**
  - **Prometheus y Grafana conforman un stack ampliamente adoptado para el monitoreo basado en métricas y la visualización en tiempo real.**
  - **Prometheus sistema de recolección y almacenamiento de series temporales, diseñado para entornos dinámicos como los basados en contenedores o microservicios. Recoge métricas mediante un modelo de pull y permite consultas avanzadas con su lenguaje PromQL.**
  - **Grafana, se integra perfectamente con Prometheus (y otras fuentes de datos) para ofrecer dashboards interactivos, altamente personalizables y en tiempo real, facilitando la observabilidad del rendimiento del sistema, la capacidad de respuesta ante incidentes y la toma de decisiones basada en datos.**

Herramientas open source SOC…

Monitoreo en tiempo real de la infraestructura

- **Elastalert (con Elastic Stack) → alertas basadas en logs.**
  - **ElastAlert, (Yelp) herramienta de alertas diseñada para trabajar en conjunto con el Elastic Stack (Elasticsearch, Logstash y Kibana).**
  - **Permite definir reglas que analizan flujos de logs almacenados en Elasticsearch y generan notificaciones cuando se cumplen ciertas condiciones, como picos de errores, patrones sospechosos o umbrales superados.**
  - **Para observabilidad basada en el análisis de logs, transforma datos crudos en alertas accionables mediante canales como correo electrónico, Slack, PagerDuty, entre otros.**
  - **con Kibana, también facilita la visualización y el ajuste de las reglas de alerta, mejorando la capacidad de respuesta ante incidentes de seguridad o fallos operativos.**

Herramientas open source SOC…

- **Wazuh → SIEM open source con correlación de eventos, integración con Elastic, capacidades de EDR.**

  Wazuh plataforma de seguridad de código abierto, combina funcionalidades de un SIEM (Security Information and Event Management) con capacidades de EDR (Endpoint Detection and Response).

  Permite la centralización, análisis y correlación en tiempo real de eventos de seguridad provenientes de múltiples fuentes, incluyendo sistemas operativos, aplicaciones y dispositivos de red.

  Se integra nativamente con el Elastic Stack (Elasticsearch, Logstash y Kibana), lo que facilita la indexación, visualización y búsqueda eficiente de alertas y logs. Además, ofrece detección de intrusiones, monitoreo de integridad de archivos, cumplimiento normativo (como PCI DSS o GDPR) y respuesta activa en endpoints.

Herramientas open source SOC…

- **TheHive → gestión de incidentes, integrable con Cortex y MISP.**
  - **TheHive una plataforma para la gestión colaborativa de incidentes de ciberseguridad.**
  - **Permite a los equipos de respuesta (CSIRT/SOC) crear, asignar, priorizar y rastrear casos de seguridad de forma eficiente, manteniendo un registro detallado de todas las acciones realizadas.**
  - **Arquitectura modular facilita la integración con herramientas complementarias: se conecta con**
  - ****Cortex** para la automatización de análisis forense mediante analizadores y respondedores**
  - ****MISP** (Platform for Sharing Threat Intelligence) para enriquecer los casos con inteligencia de amenazas en tiempo real.**

Herramientas open source SOC…

- Suricata → IDS/IPS de red con soporte para detección avanzada.
- Snort → IDS/IPS muy usado en entornos SOC.
- Osquery → para monitoreo y análisis de endpoints (similar a EDR).

Herramientas open source SOC…

- Suricata → IDS/IPS de red con soporte para detección avanzada.
- Snort → IDS/IPS muy usado en entornos SOC.
- Osquery → para monitoreo y análisis de endpoints (similar a EDR).

Herramientas para SOC y CSIRT

SIEM: una herramienta de ciberseguridad que:

- **Centraliza logs:** Recopila información de seguridad (registros) de servidores, aplicaciones, dispositivos de red y endpoints en una única ubicación.
- **Analiza eventos:**
- Procesa y correlaciona los datos para identificar patrones, anomalías y posibles amenazas de seguridad.
- **Alerta y responde:**
- Notifica a los equipos de seguridad sobre incidentes críticos y ayuda en la investigación y respuesta a ataques.

SIEM Open Source

- **Graylog: Una plataforma popular de gestión de logs que ofrece funcionalidades para buscar, visualizar y analizar datos de eventos.**
- **Stack ELK (Elasticsearch, Logstash, Kibana):**
  - **Elasticsearch: Un motor de búsqueda y análisis de datos distribuido.**
  - **Logstash: Un pipeline de procesamiento de datos que ingiere datos de múltiples fuentes y los envía a un "stash" como Elasticsearch.**
  - **Kibana: Una interfaz de visualización que permite explorar los datos y crear cuadros de mando (dashboards).**
- **OSSIM (Open Source Security Information Management) y Security Onion:** Soluciones completas que integran otras herramientas de código abierto para ofrecer una plataforma SIEM más integrada.