Trabajo Práctico Integrador

introducción a la ciberseguridad

Martínez Osti, María Josefina — Legajo 21583/5

Año 2025

Parte 1 - Hardening utilizando Lynis a nivel de sistema operativo.

En mi equipo:

¿Qué Hardening index obtuvo?

El Hardening index obtenido fue 67

¿Cuántos warnings?

Me indicó un solo warning.

¿Cuántas sugerencias?

33 sugerencias.

En la máquina vulnerable:

¿Qué Hardening index obtuvo?

El Hardening index obtenido fue 51

¿Cuántos warnings?

6 warnings.

¿Cuántas sugerencias?

Me indicó 59 sugerencias

Utilizando las referencias que provee lynis, google, etc, intente solucionar los warnings, y algunas sugerencias. Documente detalladamente los comandos utilizados.
Tenga en cuenta de que no se puede apagar el firewall y que debe existir una regla que bloquee las conexiones entrantes de telnet, compruebe que esto sea así, caso contrario cree la regla y fíjese si lynis la marca como solución. ¿Por qué ocurre eso? ¿A algún otro de los warning le pasa lo mismo? ¿Se pueden arreglar todas las sugerencias?
Nota: NO puede modificar la imagen.
Documente detalladamente los comandos utilizados. Verifique con escaneos que los problemas desaparecen, se espera que no haya warnings (si es que fuera posible) y un hardening index de al menos 65.

1. **Multiple users with UID 0 found in passwd file [AUTH-9204]** https://cisofy.com/lynis/controls/AUTH-9204/

   En Lynis la descripción del warning es la siguiente:

   “While allowed, usually configuration of multiple users with an ID of zero (0) is bad practice. Better is to create separated accounts and use proper group membership.”

El UID 0 es usado por el root y cualquier usuario con ese UID tiene los mismos permisos, lo cual es riesgoso.

Al listar los usuarios con UID 0, vemos que hay

- root
- admin2

Más concretamente, admin2 tiene uid=0(root) gid=0(root) groups=0(root), es decir que tanto el GID como el UID es 0.

Lo que voy a hacer para solucionar el warning es cambiar el UID y el GID de admin2.

Se suele usar ID>1000 para usuarios humanos, y como 1001 ya estaba ocupado, le puse el 1002. Cree un grupo con el mismo ID para también cambiarlo a ese grupo.

Una vez actualizado el UID y GID de admin2 (entrando a /etc/passwd):

uid=1002(admin2) gid=1002(admin2) groups=1002(admin2)

Hice el cambio entrando al archivo ya que usando el comando usermod me daba error porque admin2 era PID 1 en el contenedor y eso no me permitía cambiarle UID y GID.

Lo que hice luego fue actualizar el propietario de los archivos de admin2, porque actualmente no puede acceder a ellos ya que son propiedad de root.

Una vez ejecutado:

sudo chown -R admin2:admin2 /home/admin2

puedo ver que admin2 ahora sí tiene acceso a sus archivos:

drwxr-x--- 2 admin2 admin2 4096 Nov 10 21:29 /home/admin2

Y queda solucionado este primer warning.

2. Multiple accounts found with same UID [AUTH-9208]

https://cisofy.com/lynis/controls/AUTH-9208/

La descripción de este warning es:

“Lynis checks for any duplicates by checking the passwd file and count them. Any ID which shows up more than a single time is reported as a finding. Accounts and user IDs should be unique to enable proper accounting. Using several accounts with the same ID may result in data loss.”

Este warning nos indica que hay UIDs duplicados, es decir, que hay dos o más usuarios que comparten el mismo ID. En este caso, Los usuarios con el mismo UID eran root y admin2, por lo que al solucionar el anterior warning también se solucionó este.

3. iptables module(s) loaded, but no rules active [FIRE-4512]

https://cisofy.com/lynis/controls/FIRE-4512/

Lynis nos dice:

“Lynis checks for the availability of IPtables, but also if the ruleset is not empty. This might indicate bad configuration or a missing ruleset on the system.”

En el cómo resolver, lo que dice es que este warning suele saltar cuando está cargada la tabla de Iptables pero no hay reglas de firewall cargadas. Lo que en otras palabras quiere decir que hay un firewall pero está vacío y por lo tanto no está protegiendo nada.

Listando las reglas, me da la siguiente respuesta:

```
Chain INPUT (policy ACCEPT 14941 packets, 24M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 6677 packets, 394K bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Lo que podemos ver es que todas las conexiones entrantes, salientes y reenviadas son aceptadas sin revisión.

Para cumplir con lo que pide la consigna (no apagar el firewall y bloquear las conexiones de telnet entrantes) puedo ejecutar:

sudo iptables -A INPUT -p tcp --dport 23 -j DROP

que agrega una regla que bloquea cualquier conexión entrante TCP al puerto 23 (telnet).

No obstante, Lynis todavía marca el warning ya que INPUT, FORWARD y OUTPUT siguen con la política ACCEPT y eso no es lo suficientemente restrictivo para Lynis.

Una forma de resolverlo es establecer DROP como política por defecto para INPUT y FORWARD (no para OUTPUT porque estas son nuestras conexiones salientes y no querríamos bloquearlas). Una vez configurado drop como política por defecto, habría que permitir manualmente aquello que nos interese.

Sin embargo, incluso después de cambiar esa configuración, el informe sigue devolviendo el mismo warning.

El problema está en que como estamos ejecutando Lynis dentro de un contenedor, no existe una pila de red propia, sino la del host, por lo que Lynis interpreta siempre reglas vacías.

4. **Redis configuration file /etc/redis/redis.conf is world readable and might leak sensitive details [DBS-1882]**
   - Details : /etc/redis/redis.conf
   - Solution : Use chmod 640 to change file permissions
     https://cisofy.com/lynis/controls/DBS-1882/

   Lo que nos está indicando este error es que el archivo redis.conf (que es un archivo con información sensible) es wird-readable, lo que significa que cualquier usuario del sistema lo puede leer.
   Actualmente los permisos del archivo son:
   -rw-r--r-- 1 redis redis 85926 Nov 12 17:12 /etc/redis/redis.conf
   Como en “others” hay permiso de lectura, cualquier usuario puede ver el archivo.
   Para solucionarlo, podemos ejecutar lo que nos dice el warning mismo:
   sudo chmod 640 /etc/redis/redis.conf
   que hace que el dueño pueda leer, escribir y ejecutar(6), el grupo pueda solo leer(4) y el resto de usuarios del sistema no pueda hacer nada(0).
   Con esto, el warning queda solucionado.

5. **klogd is not running, which could lead to missing kernel messages in log files [LOGG-2138]**
   https://cisofy.com/lynis/controls/LOGG-2138/
   La información sobre este warning es:
   “For most Linux systems the kernel log daemon is used. Newer Linux versions may not include this kernel logger, but have an alternative to capture kernel related events. In that case, this control can be ignored. For all other systems it is advised to check why the kernel log daemon is not running.”
   En este caso Lynis detectó que no está corriendo klogd, que es un demonio del kernel para logs. No obstante, en sistemas más nuevos este servicio puede no existir, porque el registro del kernel se maneja mediante otros mecanismos.
   El detalle importante es que en este caso estamos corriendo el análisis dentro de un contenedor, no en un sistema completo. Esto hace que no sea necesario usar demonios de logging del kernel, ya que el kernel registra mensajes únicamente en el buffer accesible mediante dmesg, sin escribirlos en /var/log.
   No obstante, si ejecutamos manualmente un demonio de logging, como rsyslogd, Lynis deja de mostrar el warning ya que detecta que un demonio de logging está activo, incluso aunque este demonio no va a funcionar realmente dentro del contenedor porque no tiene acceso al kernel ni al subsistema completo de logging.

6. **Found one or more cronjob files with incorrect file permissions (see log for details) [SCHD-7704]**

   https://cisofy.com/lynis/controls/SCHD-7704/

   La descripción de este warning es:

   “Lynis triggers this control when files have their file permissions set to a dangerous value. For example when everyone can write to them.”

   Nos está indicando que los permisos a los cronjob files están incorrectamente configurados. Los cronjobs son archivos donde se definen tareas programadas para ejecutarse automáticamente, por lo que es peligroso que usuarios no autorizados puedan modificarlos.

   Con el comando:

   sudo find /etc/cron* -type f -perm /022 -ls

   obtuve la respuesta:

   56689 4 -rwxrwxrwx 1 root root 1469 Nov 13 00:14 /etc/crontab

   Lo que nos muestra que el dueño del archivo pero además todo su grupo y cualquier otro usuario puede leer, escribir y ejecutar el archivo.

   Con los siguientes comandos:

   chmod 600 /etc/crontab

   chown root:root /etc/crontab

   Consigo que solo el root pueda leer y modificar el archivo. Así, se elimina el riesgo de que usuarios externos puedan modificar el archivo y se soluciona el warning de Lynis.

Solucionando todos los warnings posible (el único que me quedó fue el de las iptables), el hardening index que obtuve fue 53.

Para seguir subiéndolo, intenté resolver algunas suggestions

- Consider hardening SSH configuration [SSH-7408]

Hay varias suggestions relacionadas a este archivo:

- X11Forwarding (set YES to NO)
- TCPKeepAlive (set YES to NO)
- AllowAgentForwarding (set YES to NO)
- StrictModes (set NO to YES)
- PermitTunnel (set YES to NO)
- PermitUserEnvironment (set YES to NO)
- PermitRootLogin (set YES to (FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWORD|WITHOUT-PASSWORD))
- MaxSessions (set 10 to 2)

- MaxAuthTries (set 6 to 3)
- LogLevel (set INFO to VERBOSE)
- GatewayPorts (set YES to NO)
- ClientAliveCountMax (set 3 to 2)
- AllowTcpForwarding (set YES to NO)
- Para solucionarlo, entre con vi al archivo con
- vi /etc/ssh/sshd_config

y cambié todo lo que me recomendó Lynis. Con estos cambios, el hardening index obtenido fue de 66.

Resultados finales:

Parte 2 - Analizadores de código estático.

Secrets en el código

Trivy vs. Trufflehog

Instale trivy y trufflehog. Se recomienda docker.

Baje el siguiente .zip.

Nota: NO es necesario hacer un build del docker-compose.yml, ambas herramientas trabajan analizando el código fuente. Busque solo secretos utilizando trivy y trufflehog

¿Cuál encontró más secretos? ¿Cuál le parece que es mejor? Justifique.

Trivy:

Lo ejecuté con el comando:

docker run --rm -v "${pwd}:/src" aquasec/trivy fs --scanners secret /src

Encontró en total 16 secretos:

- 5 en el .env
- 3 en .env.production
- 6 esn config.json
- 2 en secrets/api_key.txt

TruffleHog:

ejecutado con:

docker run --rm -v "${pwd}:/src" trufflesecurity/trufflehog filesystem /src

Encontró un total de 24 secretos.

Aunque TruffleHog identificó más coincidencias, muchos de los “secretos” que reportó son mucho menos relevantes que los de Trivy. Esto se debe a que TruffleHog es una herramienta más agresiva.

La mayoría de los hallazgos extra de TruffleHog son del cosas Git dentro del directorio .git/objects/. Allí encontró cadenas largas que coinciden con patrones de credenciales, pero que no son secretos reales del proyecto.

Por ejemplo:

Found unverified result 🐷🔑❓

Detector Type: Stripe

Decoder Type: PLAIN

Raw result: sk_live_51H1vSlLkdIwHu0bS9876543210zyxwvutsrqponmlkjihgf

Rotation_guide: https://howtorotate.com/docs/tutorials/stripe/

File: /src/.git/objects/1d/6cdd4bcf9bea2d47c452e171eed8316ed80afd

Line: 14

Ahí nos está detectando como secret algo que está dentro de un objeto de git, no en el código fuente del proyecto.

A su vez, los logs de Trivy son mucho más simples de leer, ya que da un resumen estructurado de los secretos encontrados y los clasifica por tipo, gravedad y archivo, lo que facilita su interpretación. Además, todos los secretos detectados por Trivy son de credenciales críticas, como tokens de GitHub, GitLab, Stripe Keys o claves privadas.

Sin embargo, si la idea es hacer una auditoría más profunda del repositorio y revisar el historial de commits, entonces la herramienta indicada es TruffleHog, porque puede detectar secretos antiguos o eliminados que hayan quedado en el repositorio.

Vulnerabilidades en las dependencias

Investigue cómo utilizar trivy, para analizar vulnerabilidades en el archivo requeriments.txt que está en el repositorio. Luego trate de solucionarlas y vuelva a realizar un escaneo, ¿se soluciono todo?

Desarrolle los conceptos de major, minor y bug fix y explique por qué no siempre es posible actualizar a la última versión.

Comando utilizado:
docker run --rm -v "${pwd}:/src" aquasec/trivy fs --scanners vuln /src

Resultado:

requirements.txt (pip)

==========

Total: 29 (UNKNOWN: 0, LOW: 1, MEDIUM: 17, HIGH: 10, CRITICAL: 1)

Hay muchas vulnerabilidades que se relacionan con librerías típicas de proyectos Python, tales como Flask, Jinja2, etc.

Lo que se puede apreciar en el reporte es que muchos de los errores ya fueron arreglados en versiones más nuevas de las librerías. Por ejemplo, uno de las vulnerabilidades de alto riesgo es:

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
Flask	CVE-2023-30861	HIGH	fixed	1.0.2	2.3.2, 2.2.5	flask: Possible disclosure of permanent session cookie due to missing Vary: Cookie… https://avd.aquasec.com/nvd/cve-2023-30861

Aquí Trivy nos indica que esta vulnerabilidad de Flask fue arreglada en la versión 2.3.2 y la que está instalada es la 1.0.2.

Simplemente reemplazando las versiones obsoletas del requirements.txt por versiones estables más modernas, el escaneo de Trivy me devolvió 0 vulnerabilidades.

No obstante cabe aclarar que en un proyecto real, actualizar tantas versiones es probable que rompa algo, ya que no siempre va a haber compatibilidad hacia atrás cuando son versiones de hace tantos años.

El versionado semántico utiliza el formato major.minor.patch.

- MAJOR se usa para representar cambios importantes que rompen la compatibilidad hacia atrás
- MINOR se utiliza para nuevas funcionalidades compatibles con versiones
- PATCH se usa para corregir errores o vulnerabilidades sin cambiar funcionalidades.

Hardening

Investigue cómo utilizar trivy para analizar un Dockerfile, utilícelo en el Dockerfile

que hay en el repositorio, si encuentra cosas que no estén bien configuradas, modifiquelo hasta que no encuentre nada.

Comando utilizado:

docker run --rm -v "${pwd}:/src" aquasec/trivy config /src/Dockerfile

Resultado:

11 errores de configuración (UNKNOWN: 0, LOW: 1, MEDIUM: 1, HIGH: 2, CRITICAL: 7)

1. AVD-DS-0002 (HIGH): Last USER command in Dockerfile should not be 'root'
   El dockerfile tiene USER root. Esto hace que toda la aplicación corra como root.
   Corregirlo es tan simple como crear un usuario seguro y sacar la línea mencionada.
   RUN adduser --disabled-password --gecos "" appuser
   USER appuser
2. AVD-DS-0004 (MEDIUM): Port 22 should not be exposed in Dockerfile
   El archivo tiene EXPOSE 22 3306 5432 6379. Esto implcia que se puede acceder con SSH desde fuera del contenedor, lo cual es inseguro. Solo hay que exponer el puerto que use la app.
3. AVD-DS-0026 (LOW): Add HEALTHCHECK instruction in your Dockerfile
   El contenedor no define un HEALTHCHECK, entonces Docker no pueden saber si la aplicación está funcionando correctamente.
   Se debe agregar
   HEALTHCHECK --interval=30s --timeout=10s \
     CMD curl -f http://localhost:5000/health || exit 1
4. AVD-DS-0029 (HIGH): '--no-install-recommends' flag is missed: 'apt-get update && apt-get install -y curl wget openssl sqlite3 sudo && rm -rf /var/lib/apt/lists/*'
   Al no tener la flag mencionada, la imagen instala paquetes adicionales innecesarios.
   Esto se soluciona simplemente agregando la flag mencionada.
5. AVD-DS-0031 (CRITICAL): Possible exposure of secret env "ADMIN_PASSWORD" in ENV
   Los últimos 7 errores son muy graves. se exponen 7 secretos críticos:SECRET_KEY, DATABASE_PASSWORD, API_TOKEN, ADMIN_PASSWORD, JWT_SECRET, ENCRYPTION_KEY, AWS_SECRET_KEY.
   Esto es muy grave porque los secretos quedan almacenados en al imagen, incluso si después se borran.

No es seguro usar ENV en el Dockerfile. Hay que mover los secretos a variables de entorno en tiempo de ejecución.

NOTA: dejo en la carpeta de la entrega el dockerfile entero corregido.
Con esto, Trivy no indica más problemas.

Parte 3 - “Pentesting” de un ejecutable

Descargue el archivo: Sap.zip
Dentro del cual hay un ejecutable de windows y el código fuente correspondiente en python. No es malware, pero puede instalar una máquina virtual de windows, para ejecutarlo.
Tareas:
Describir qué hace el programa, ya sea vía la ejecución del archivo o analizando el código fuente. Ignore los mensajes sobre la VPN y la autenticación, tampoco es muy relevante saber qué es y que hace SAP.
Encontrar vulnerabilidades en el ejecutable, que afecten a la máquina donde se está ejecutando y aunque no lo podamos demostrar al servidor.
Utilizando el documento: Informe pentest realizar un informe que documente los hallazgos encontrados.

El programa es un ejecutable escrito en Python que intenta automatizar tareas dentro del sistema SAP mediante librerías como pyautogui y win32com. No obstante, al ejecutar el programa, como no tengo SAP, ejecutó sobre la ventana que tenía activa (que en mi caso fue el navegador), escribiendo los códigos de transacción en la barra de búsquedas y posteriormente buscando.

El objetivo original del programa, leyendo el código, es leer la lista de transacciones desde transacciones.csv, abrir ventanas del SAP usando combinaciones de teclas simuladas y escribir el código de cada transacción en SAP y ejecutarla.

Hallazgo 1: Ejecución de acciones en el sistema mediante pyautogui

Severidad	Alta	**CVSS**	7.0 - CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
Descripción	El programa usa la librería pyautogui para mover el mouse, escribir texto y ejecutar combinaciones de teclas basadas en datos del archivo transacciones.csv sin ninguna validación ni		

	límites. Esto permite que un atacante modifique el archivo mencionado para inyectar secuencias de teclas o comandos que el script ejecutará automáticamente pudiendo realizar acciones maliciosas.		
CWE	CWE-927	**Stride**	Elevation of privilege (obtener permisos que el atacante no debería tener) o en su defecto Tampering (modificación del sistema mediante entradas maliciosa)
Impacto	El impacto directo es que el atacante podría ejecutar las acciones que quiera dentro del sistema operativo, tales como la modificación, creación o eliminación de archivos del sistema accesibles al usuario. En palabras simples, el impacto es equivalente a darle al atacante control al teclado y mouse de la víctima.		
Referencias	https://cwe.mitre.org/data/definitions/927.html https://pyautogui.readthedocs.io/en/latest/		
Prueba de concepto			
1. Editar el archivo *transacciones.csv* y reemplazar la transacción por un valor malicioso, por ejemplo: https://catedras.linti.unlp.edu.ar/ 2. Ejecutar el script. 3. El programa escribirá el contenido directamente en la ventana activa (que puede no ser el SAP). 4. En caso de que el foco esté en un navegador web, se accederá a cátedras linti. 5. Esto confirma que el programa usa la entrada del CSV sin validación ni restricciones. No existe ningún mecanismo que limite, valide o controle qué puede ser ejecutado, lo que permite al atacante inyectar comandos arbitrarios.			
Recomendaciones			
1. **Validación estricta de entrada:** Permitir únicamente códigos de transacción válidos. Esto podría hacerse, por ejemplo, teniendo una whitelist con entradas que se permita y bloquear todo el resto de operaciones. 2. **Verificación de ventana activa:** Confirmar que la ventana de SAP esté en foco antes de enviar cualquier acción.			

Hallazgo 2: Escritura de Archivos en Rutas Arbitrarias

Severidad	Alta	**CVSS**	7.0 -

			CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
Descripción	El ejecutable permite que el usuario controle la ruta relativa donde se guardan capturas de pantalla, logs y archivos generados por el script ya que construye la ruta de escritura concatenando el valor leído en el archivo transacciones.csv con un valor preestablecido. de esta forma, es posible generar rutas no deseadas usando secuencias como ..\.., afectando la estructura de archivos por encima del directorio esperado.		
CWE	CWE-22	**Stride**	Tampering
Impacto	El impacto directo es que, como no se validan los valores leídos en el archivo csv, es posible incluir cosas tales como ..\..\..\Windows\System32 y así crear directorios y archivos en cualquier ruta accesible del sistema, sobreescribiendo y modificando archivos del usuario o del sistema operativo. Esto puede permitir, por ejemplo, que el atacante pueda preparar un escenario para ejecutar malware o scripts maliciosos sin restricciones del programa mediante la modificación de archivos sensibles como scripts, configuraciones o ejecutables.		
Referencias	https://cwe.mitre.org/data/definitions/22.html https://owasp.org/www-community/attacks/Path_Traversal		
Prueba de concepto			
1. Editar el archivo *transacciones.csv* y colocar como transacción:..\..\..\Users\Public\Desktop 2. Ejecutar el script. 3. El programa creará esa carpeta (si no existe) y escribirá dentro de ella capturas y archivos de log. 4. Modificando esta ruta por una ubicación sensible (por ej. C:\Windows\System32), el programa intentará guardar archivos allí, demostrando que no existe ninguna restricción.		
Recomendaciones			
3. **Validación de rutas de salida:** Rechazar cualquier entrada que contenga . ., barras invertidas, rutas absolutas o caracteres especiales. 4. **Limitación de rutas:** Permitir únicamente directorios dentro de un directorio específico permitido.			

Hallazgo 3: Filtración de información mediante capturas de pantalla automáticas

Severidad	Media	**CVSS**	6.9 - CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L

			/SI:N/SA:N
Descripción	El ejecutable realiza capturas de toda la pantalla cada pocos segundos, lo que podría capturar credenciales, ventanas de correo, carpetas del sistema, entre otros datos sensibles del usuario. No hay control, anonimización ni borrado seguro de dichas imágenes.		
CWE	CWE-200	**Stride**	Information disclosure
Impacto	El impacto principal es que se expone información confidencial del usuario y su sistema. Podría, por ejemplo, sincronizarse el directorio donde se almacenan las capturas con la nube y generar así una fuga de datos hacia terceros.		
Referencias	https://cwe.mitre.org/data/definitions/200.html		
Prueba de concepto			
5. Entrar a algún programa con información sensible (como por ejemplo, gmail) y dejar la pestaña abierta 6. Ejecutar el script. 7. El programa sacará capturas de pantalla a toda la vista, incluyendo cualquier ventana que el usuario tiene abierta.			
Recomendaciones			
5. **Limitación de capturas:** Permitir al programa que capture únicamente el SAP, nunca la pantalla completa u otras ventanas. 6. **Protección de capturas:** Borrar automáticamente capturas antiguas. 7. **Informar al usuario:** Agregar un aviso explícito y solicitar consentimiento sobre la toma de capturas de pantalla.			

4. Análisis y reflexión sobre normativas

En este punto deberán recuperar el código GDPR (General Data Protection Regulation – UE) y realizar un análisis crítico, teniendo en cuenta las siguientes condiciones:

- Identificar y seleccionar diez artículos del GDPR que consideren directamente relevantes para el abordaje y la gestión de la ciberseguridad en una organización.
- Deberán argumentar detalladamente la elección de cada artículo, explicando cómo su cumplimiento impacta o moldea las políticas y prácticas de seguridad de la información (ej., en relación con el cifrado, el manejo de incidentes o el diseño de sistemas).

- Elaborar una crítica fundamentada sobre los puntos débiles o las limitaciones, que consideren del GDPR en relación con los desafíos actuales de la ciberseguridad (ej., tecnologías emergentes, big data, o la aplicación en contextos de ataque avanzado).

El GDPR es una normativa europea del 2016 cuyo objetivo es proteger los datos personales y la privacidad de las personas dentro de la Unión Europea, brindando derechos a los ciudadanos y responsabilidades y obligaciones a las organizaciones que recopilan, almacenan o procesan dichos datos.
10 artículos que me parecieron relevantes para las organizaciones son:

- **Artículo 5: "Principles relating to processing of personal data"**
  Este artículo es altamente relevante ya que establece las responsabilidades que debe tener una organización con los datos de las personas.
  En particular, establece que:
  - Deben ser procesados de manera lícita y transparente en relación con el interesado.
  - Tienen que obtenerse y utilizarse con fines determinados y explícitos.
  - No deben guardarse durante más tiempo del necesario para los fines expresados.
  - Tienen que ser tratados asegurando seguridad adecuada.

  Este artículo impacta en las organizaciones y su gestión de la ciberseguridad ya que obliga a adoptar prácticas que garanticen la integridad, la confidencialidad y la disponibilidad de los datos personales a lo largo de todo su ciclo de vida.

  Además, el artículo exige que solo se recolecten los datos estrictamente necesarios para la finalidad declarada, prohibiendo la acumulación de información irrelevante o excesiva y definiendo políticas de retención, borrado seguro y anonimización. Esto tiene repercusión en la ciberseguridad de las organizaciones porque, al tener menos datos almacenados y reducir su tiempo de exposición, se reduce la superficie vulnerable facilitando así la seguridad de la información.

- **Artículo 6: "Lawfulness of processing"**
  En esta sección se plantean las bases legales para procesar datos personales: consentimiento, contrato, obligación legal, interés vital, interés público o interés legítimo. Es relevante para las organizaciones ya que obliga a que toda actividad relacionada al tratamiento de datos esté bien justificada y documentada, registrando quién accede a los datos, para qué y bajo qué base legal, influyendo en la trazabilidad y controles de acceso.

Artículo 12: “Transparent information, communication and modalities for the exercise of the rights of the data subject”

Este artículo establece la necesidad de que las organizaciones proporcionen a los usuarios información clara y fácilmente accesible sobre cómo procesan sus datos personales y sobre sus derechos y las formas de ejercerlos. Además, exige que las comunicaciones relacionadas con la protección de datos se realicen de manera transparente.

Es importante porque a diferencia de otros artículos que plantean proteger la información de manera técnica, en este se establece la importancia de que las personas sepan cómo se manejan sus datos y qué riesgos puede haber. La transparencia ayuda, por ejemplo, a reducir la probabilidad de fraudes y mejora la confianza del usuario en la organización.

- **Artículo 25: “Data protection by design and by default”**

Aquí se plantea que las medidas técnicas y organizativas para proteger los datos tienen que incorporarse desde el diseño inicial del sistema, antes de empezar a procesar datos. Además, establece que, por defecto, la configuración de seguridad sea la más segura y restrictiva posible haciendo que:

- Solo se recolecten los datos estrictamente necesarios
- Se limiten los plazos de almacenamiento
- Se restrinja el acceso únicamente a quienes lo necesitan
- Los datos no sean accesibles a terceros de forma automática.

Este artículo es relevante para las organizaciones porque obliga a que desde el momento en que se diseñan los sistemas se tenga en cuenta medidas de seguridad informática.

Además, la obligación de que por defecto solo se recolecten los datos estrictamente necesarios impacta directamente en el funcionamiento de aplicaciones y servicios: por ejemplo, una organización no puede activar automáticamente la geolocalización de un usuario sin solicitar el permiso correspondiente. Esto garantiza un mayor control del usuario sobre su información y reduce la superficie de ataque ante posibles incidentes de seguridad.

- **Artículo 28: ”Processor”**

En este artículo se regula la relación entre una organización y un tercero que procesa datos personales en su nombre. Establece que el responsable solo puede contratar procesadores que ofrecen garantías suficientes de que aplican medidas

técnicas y organizativas adecuadas para proteger los derechos de los interesados. Además, el procesador no puede recurrir a otros subprocesadores sin una autorización previa y explícita del responsable.

Esta relación entre la organización y el procesador se regula por un contrato que describe la finalidad del procesamiento, la duración, el tipo de datos a tratar, las obligaciones de confidencialidad y las medidas de seguridad a aplicar.

Es un artículo fundamental porque hace que las organizaciones no deban solo controlar sus propios sistemas sino también la seguridad de todos los proveedores externos que procesan datos, tales como plataformas de cloud, empresas de soporte técnico, hosting, almacenamiento externo, call centers, etc.

- **Artículo 30: "Records of processing activities"**

Este artículo obliga a las organizaciones a mantener un registro actualizado de todas las actividades de procesamiento de datos bajo su responsabilidad que contenga:

- Los datos de contacto del responsable, corresponsable y del delegado de protección de datos
- Las finalidades del procesamiento
- Las categorías de datos personales y de interesados involucrados
- Los destinatarios a los que se comunican los datos, incluyendo transferencias internacionales
- Los plazos previstos para la eliminación de cada categoría de datos

Este artículo es relevante para las organizaciones porque obliga a mantener un inventario detallado de datos y sistemas con el fin de saber qué datos se procesan, dónde se almacenan y quién tiene acceso y cómo son los flujos de información, lo que permite detectar posibles puntos críticos de seguridad y definir medidas de protección adecuadas.

- **Artículo 32: "Security of processing"**

Este artículo exige que al tratar datos, tanto el controlador como el 'procesador apliquen técnicas apropiadas para garantizar un nivel de seguridad adecuado al riesgo teniendo en cuenta, entre otras cosas:

- La seudonimización y el cifrado de los datos personales
- La capacidad de garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia continuas de los sistemas y servicios de tratamiento
- La capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico.

- Un proceso para probar, evaluar y valorar periódicamente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Esto es relevante para las organizaciones porque introduce un enfoque basado en el riesgo, lo que motiva a las organizaciones a realizar periódicamente análisis y evaluaciones constantes de amenazas, vulnerabilidades y probabilidad de impacto. Además, las obliga a gestionar cautelosamente el acceso a los datos promoviendo un principio de mínimo privilegio y hace que tengan que tener evidencia documentada y certificaciones que demuestren el cumplimiento de las medidas de seguridad exigidas.

- **Artículo 33: ”Notification of a personal data breach to the supervisory authority”**

Este artículo establece la obligación de que las empresas notifiquen una brecha de datos personales a la autoridad supervisora competente en no más de 72hs desde que se conoce el incidente. Solamente se exceptúan incidentes que no representan un riesgo para los derechos y libertades de las personas afectadas.

Esto es relevante para organizaciones ya que obliga a las organizaciones a tener un proceso formal de gestión de incidentes con capacidad de detectarlos, analizarlos, comunicarlos y mitigarlos.

La obligación de documentar cada violación promueve la transparrencia y mejora continua, lo que ayuda a la identificación de patrones, corrección de vulnerabilidades y fortalecimiiento de la postura de seguridad de la información.

- **Artículo 34: “Communication of a personal data breach to the data subject”**

Este artículo es similar al anterior, pero en cambio de obligar a las organizaciones a comunicar brechas de seguridad a las autoridades, obliga a que se comuniquen directamente a los afectados de forma clara y rápida explicando el incidente, sus posibles consecuencias y las medidas tomadas.

Este artículo es importante para la ciberseguridad de las organizaciones porque obliga a evaluar de manera inmediata la gravedad de una brecha y mantener canales de comunicación seguros con los usuarios. También incentiva el uso de cifrado, ya que si los datos filtrados estaban cifrados, la organización puede quedar exenta de informar a los afectados, reduciendo el impacto que esto podría tener en su reputación.

- **Artículo 35: “Data protection impact assessment”**

Este artículo es interesante ya que plantea que cuando un procesamiento de datos que involucra nuevas tecnologías tiene probabilidades de generar un riesgo alto para los derechos y libertades de las personas, se debe realizar, antes de comenzar el tratamiento, una evaluación del impacto de la protección de datos para analizar los riesgos, describir el procesamiento y establecer las medidas de seguridad necesarias para mitigarlos.

En particular, de este artículo me resultó interesante la parte que dice que es obligatorio realizar la evaluación de impacto cuando:

“a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;”

Ya que es relevante en el contexto actual dado a que, por la naturaleza de la inteligencia artificial, cualquier operación con los datos de usuarios que use decisiones automatizadas, análisis a gran escala, u otras operaciones similares de datos de usuarios mediante modelos de IA queda automáticamente abarcada por este artículo.

Esto obliga a las organizaciones a evaluar los riesgos que podrían surgir con el uso de algoritmos, modelos predictivos y sistemas inteligentes garantizando que se cumplen medidas de seguridad, transparencia y mitigación antes de comenzar a utilizarlos.

Si bien el GDPR es una regulación bastante completa de la regulación de datos,presenta limitaciones en su aplicación práctica cuando se lo analiza desde la perspectiva de la ciberseguridad moderna y las tecnologías emergentes, ya que hay dificultades en su aplicación y vacíos en contextos donde la velocidad de evolución tecnológica supera la normativa.

Una de las debilidades es la falta de especificidad técnica. Da principios y obligaciones generales pero no define, por ejemplo, qué algoritmos criptográficos usar o qué configuraciones mínimas deben aplicarse. Esto puede hacer que las interpretaciones de algunas organizaciones sean insuficientes o desactualizadas frente a amenazas avanzadas.

Por otro lado, recordemos que el GDPR es del 2016. En esa época, cosas como la IA generativa, big data, IoT, etc no eran tan comunes y por tanto no forman parte explícita de la normativa. Algunos artículos (como el 35 analizado más arriba), puede extenderse para abarcar estos tópicos, pero quedan muchos espacios vacíos al respecto.

En resumen, aunque el GDPR constituye una base sólida de regulación, considero que necesita ser actualizado y complementado con estándares técnicos más específicos y marcos regulatorios adaptados al contexto actual.