Las organizaciones utilizan marcos de seguridad como punto de partida para crear sus propias políticas y procesos de seguridad. Los frameworks de seguridad son directrices utilizadas para construir planes que ayudan a mitigar los riesgos y amenazas a los datos y la privacidad, es mas que solo el espacio virtual, también incluye el físico, como lo es el acceso restringido. Entre todos los planes, se pueden crear algunos que aumenten la concienciación de los empleados y educarlos sobre como proteger tanto la aplicación, como a ellos mismos. Existen diversos marcos, los que vamos a destacar son:

* **Marco de la amenaza cibernética:** fue desarrollado por el gobierno de EE.UU para proporcionar “un lenguaje común para describir y comunicar información sobre la actividad de las ciberamenazas”. Al proporcionar un lenguaje común, el CTF ayuda a los profesionales a analizar y compartir información de forma mas eficaz
* **Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC) 27001:** permite a las organizaciones de todos los sectores y tamaños a gestionar la seguridad de los recursos, como la información financiera, la Propiedad Intelectual, los datos de los empleados y la información confiada a terceros

**Controles:** a diferencia de los frameworks, estos son usados para reducir riesgos específicos. Si no son aplicados adecuadamente, una organización podría enfrentarse a importantes impactos financieros y daños a su reputación. Existen 3 tipos comunes de controles:

1. *Encriptación:* proceso de convertir datos de un formato legible a uno codificado. Típicamente implica convertir datos de texto plano a cifrado, el cual es el mensaje en bruto que es ilegible para humanos y ordenadores, la única forma de leerse es que se desencripten a su forma original
2. *Autenticación:* proceso de verificar quien es alguien o algo, como registrarse en un sitio web con su nombre y usuario. Existen métodos mas avanzados como la autenticación multifactor, o MFA, desafían al usuario a demostrar que es quien dice ser exigiendo tanto una contraseña como una forma adicional de autenticación, como datos biométricos. Los datos biométricos hay que manejarlos con cuidado ya que el **vishing** podría explotarlos para generar un ataque de ingeniería social, el mismo consiste en la explotación de comunicaciones electrónicas de voz para obtener información sensible o suplantar la identidad de una fuente conocida
3. *Autorización:* se refiere al concepto de otorgar acceso a recursos específicos dentro de un sistema, se utiliza para verificar que una persona tiene permiso para acceder a un recurso

**Triada CID:** es un modelo que ayuda a informar como las organizaciones consideran el riesgo al establecer sistemas y políticas de seguridad, CID significa confidencialidad, integridad y disponibilidad, pilares fundamentales de la ciberseguridad

* **Integridad:** los datos son correctos, auténticos y confiables
* **Disponibilidad:** los datos son accesibles para quienes están autorizados
* **Confidencialidad:** solo los usuarios autorizados pueden tener acceso a datos o activos específicos

**Instituto Nacional de Estándares y Tecnología (NIST):** una organización con sede en EE.UU. Proporciona una orientación que puede ayudar a los analistas de todo el mundo a entender como implementar practicas esenciales de ciberseguridad. Ofrece distintos marcos tales como:

* *Marco de ciberseguridad del NIST, o CSF:* marco voluntario que consiste en estándares directrices y mejores prácticas para gestionar el riesgo de ciberseguridad. Es ampliamente respetado y esencial para mantener la seguridad independientemente de la organización para la que trabaje. Consta de 6 funciones principales importantes:  
  1- **Identificar:** se relaciona con la gestión del riesgo de ciberseguridad y su efecto en las personas y los activos de una organización

2- **Proteger:** estrategia utilizada para proteger una organización mediante la implementación de políticas, procedimientos, capacitación y herramientas que ayudan a mitigar las amenazas de ciberseguridad  
3- **Detectar**  
4- **Responder:** asegurarse que se utilizan los procedimientos adecuados para contener, neutralizar y analizar los incidentes de seguridad e implementar mejoras en el proceso de seguridad  
5- **Recuperar:** proceso de devolver a los sistemas afectados su funcionamiento normal  
6- **Gobernar:** hace hincapié en la importancia de una sólida gobernanza de la ciberseguridad en todos los niveles de la organización. Se trata de establecer y mantener las estructuras y procesos necesarios para gestionar eficazmente los riesgos de ciberseguridad.

Las funciones principales del CSF del NIST proporcionan orientación y dirección específicas para los profesionales de la seguridad. Este marco se utiliza para desarrollar planes para gestionar un incidente de forma adecuada y rápida a fin de reducir el riesgo, proteger a la organización contra una amenaza y mitigar cualquier posible vulnerabilidad. El CSF del NIST también amplía la protección del gobierno federal de los Estados Unidos con la publicación especial del NIST, o SP 800-53. Proporciona un marco unificado para proteger la seguridad de los sistemas de información dentro del gobierno federal, incluidos los sistemas proporcionados por empresas privadas para uso del gobierno federal. Los controles de seguridad proporcionados por este marco se utilizan para mantener la tríada CID de los sistemas utilizados por el gobierno.

**Proyecto abierto de seguridad de las aplicaciones web (Open Web Application Security Proyect, u OWASP)**

El primer principio del que consta es *minimizar la superficie del ataque*, la cual se refiere a todas las vulnerabilidades potenciales que un agente de amenaza podría explotar, como los vectores de ataque, que son vías que los atacantes utilizan para penetrar en las defensas de seguridad, algunos ejemplos comunes, son los correos electrónicos del phishing y las contraseñas débiles

El principio de *privilegio mínimo* significa asegurarse de que los usuarios tienen la menor cantidad de acceso necesario para realizar sus tareas cotidianas, para reducir los daños que podría causar una brecha de seguridad

Principio de *defensa en profundidad*: significa que una organización debe tener múltiples controles de seguridad que aborden los riesgos y amenazas de diferentes maneras

Principio de *solucionar los problemas de seguridad correctamente:* este principio se basa en que en el momento que se produzca un incidente de seguridad, los profesionales identifiquen la causa raíz rápidamente y corregir cualquier vulnerabilidad para luego realizar pruebas para garantizar que se reparo con éxito

Principio de *separación de funciones:* las acciones críticas deben depender de varias personas, cada una de las cuales debe seguir el principio de privilegio mínimo.

Principio de *seguridad sencilla:* evite las soluciones innecesariamente complicadas. La complejidad dificulta la seguridad.

También existen otros 4 principios adicionales:

1. **Establecer valores predeterminados seguros:** el estado de seguridad optimo de una aplicación es también su estado por defecto para los usuarios, por lo tanto, hacer que la aplicación sea insegura, debería costar un trabajo extra
2. **Falla con seguridad:** fallar de forma segura significa que cuando un control falla o se detiene, debe hacerlo pasando por defecto a su opción mas segura, ´por ejemplo, cuando un cortafuegos falla, debería simplemente cerrar todas las conexiones y bloquear todas las nuevas, en lugar de empezar a aceptarlo todo.
3. **No confíes en los servicios:** la organización no debe confiar explícitamente en que los sistemas de sus socios sean seguros. Por ejemplo, si un proveedor externo realiza el seguimiento de los puntos de recompensa de los clientes de una aerolínea, ésta debería asegurarse de que el saldo es exacto antes de compartir esa información con sus clientes.
4. **Evitar la seguridad por oscuridad:** la seguridad de los sistemas clave no debe basarse en mantener ocultos los detalles, sino en otros factores como políticas de contraseñas razonables, defensa en profundidad, etc

La forma para que los marcos, controles, principios de seguridad y normas de cumplimiento funcionen todos juntos, es mediante la realización de auditorías de seguridad, la cual consiste en una revisión de los controles, políticas y procedimientos de seguridad de una organización en comparación con conjunto de expectativas, su objetivo es identificar y abordar las áreas de remediación y crecimiento, proporcionan una dirección y claridad al identificar cuales son los fallos actuales y desarrollar un plan para corregirlos. Hay 2 tipos principales de auditorias de seguridad

1. Externas
2. Internas (en esta nos centraremos ya que somos principiantes): por lo general la lleva a cabo un equipo de personas que puede incluir al oficial de cumplimiento, al gerente de seguridad y a otros miembros del equipo de seguridad de organización, se utilizan para ayudar a mejorar la postura de seguridad de una organización y ayudar a las organizaciones a evitar multas de las agencias gubernamentales debido a la falta de cumplimiento y ayudan a los equipos de seguridad a identificar el riesgo organizacional, evaluar los controles y corregir los problemas de cumplimiento.

Las auditorias tienen algunos elementos comunes, los cuales incluyen *establecer el alcance y los objetivos de la auditoria, completar una evaluación de controles, evaluar el cumplimiento y comunicar los resultados a la parte interesada*. Aunque los miembros del equipo de seguridad mas de mas alto nivel y otra parte interesada establecen el alcance y los objetivos de la auditoria, también es posible que un analista principiante revise y comprenda el alcance y los objetivos para completar los otros elementos de la auditoria. Por ejemplo, el alcance de esta auditoria implica la evaluación de los permisos de los usuarios; la identificación de los controles, políticas y procedimientos existentes; y la contabilización de la tecnología que utiliza actualmente la organización. Los objetivos descritos incluyen la implementación de las funciones principales de los marcos, como el CSF del NIST; el establecimiento de políticas y procedimientos para garantizar el cumplimiento; y el fortalecimiento de los controles del sistema. La evaluación de riesgos se centra en identificar posibles amenazas, riesgos y vulnerabilidades, lo que ayuda a considerar que medidas de seguridad deben implementarse y supervisarse para garantizar la seguridad de los activos

**Evaluacion de controles:** implica revisar minuciosamente los activos existentes de una organización y, a continuación, evaluar los riesgos potenciales para esos activos, a fin de garantizar que los controles y procesos internos sean efectivos, por lo cual a los analistas principiantes se les podría encomendar la tarea de clasificar los controles en las categorías de:

1. Controles administrativos: se relacionan con el componente humano de la ciberseguridad. Incluyen políticas y procedimientos que definen la forma en que una organización administra los datos
2. Controles técnicos: son soluciones de hardware y software que se utilizan para proteger los activos, como el uso de sistemas de detección de intrusos y la encriptación
3. Controles físicos: se refieren a las medidas implementadas para impedir el acceso físico a los activos protegidos, como cerraduras o cámaras de vigilancia

**Determinar si la organización cumple o no con las normas necesarias:** este es otro elemento que se refiere a las regulaciones de cumplimiento que son leyes que las organizaciones deben seguir para garantizar que los datos privados permanezcan seguros

**Comunicación:** una vez finalizada la auditoria, los resultados y las recomendaciones deben comunicarse a la parte interesada, por lo general esta comunicación resume el alcance y los objetivos de la auditoria, enumera los riesgos existentes y señala la rapidez con la que deben abordarse esos riesgos. También identifica las normas de cumplimiento que la organización debe cumplir y proporciona recomendaciones para mejorar la postura de seguridad

Hay varios factores que pueden afectar a las auditorias:

* Tipo de industria
* Tamaño de la organización
* Vínculos con las regulaciones gubernamentales aplicables
* La ubicación geográfica de un negocio
* Una decisión empresarial de adherirse a un cumplimiento normativo especifico

**Funcion de los marcos y controles en las auditorias**

Marcos como el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF) y la serie de normas internacionales para la seguridad de la información (ISO 27000) están diseñados para ayudar a las organizaciones a prepararse para las auditorías de seguridad de cumplimiento normativo. Al adherirse a estos y otros marcos relevantes, las organizaciones pueden ahorrar tiempo a la hora de realizar auditorías externas e internas. Además, los marcos, cuando se utilizan junto con los controles, pueden apoyar la capacidad de las organizaciones para alinearse con los Requisitos y Estándares de cumplimiento normativo.

Es necesario crear una *lista de comprobación* de la auditoría antes de llevarla a cabo. Por lo general, una lista de comprobación se compone de las siguientes áreas de atención:

* **Identificar el alcance de la auditoria:** la auditoria debe realizar una lista de los recursos que se evaluaran, indicar como la auditoria ayudara a la organización a alcanzar sus objetivos deseados, indicar con que frecuencia debe realizarse una auditoria, incluir una evaluación de las políticas, protocolos y procedimientos de la organización para asegurarse de que funcionan según lo previsto y de que los empleados los implementan
* **Completar una evaluación de riesgos:** se utiliza para valorar los riesgos organizativos identificados en relación con el presupuesto, los controles, los procesos internos y los estándares externos
* **Realizar una auditoria:** al realizarla, se evaluara la seguridad de los recursos identificados que figuran en la lista del alcance de la auditoria
* **Crear un plan de mitigación:** es una estrategia establecida para reducir el nivel de riesgo y los posibles costes, sanciones u otros problemas que puedan afectar negativamente a la postura de seguridad de la organización
* **Comunicar los resultados a las partes interesadas:** se debe presentar un informe detallado de los resultados, las mejoras sugeridas necesarias para reducir el nivel de riesgo de la organización y las regulaciones y estándares a los que la organización debe adherirse