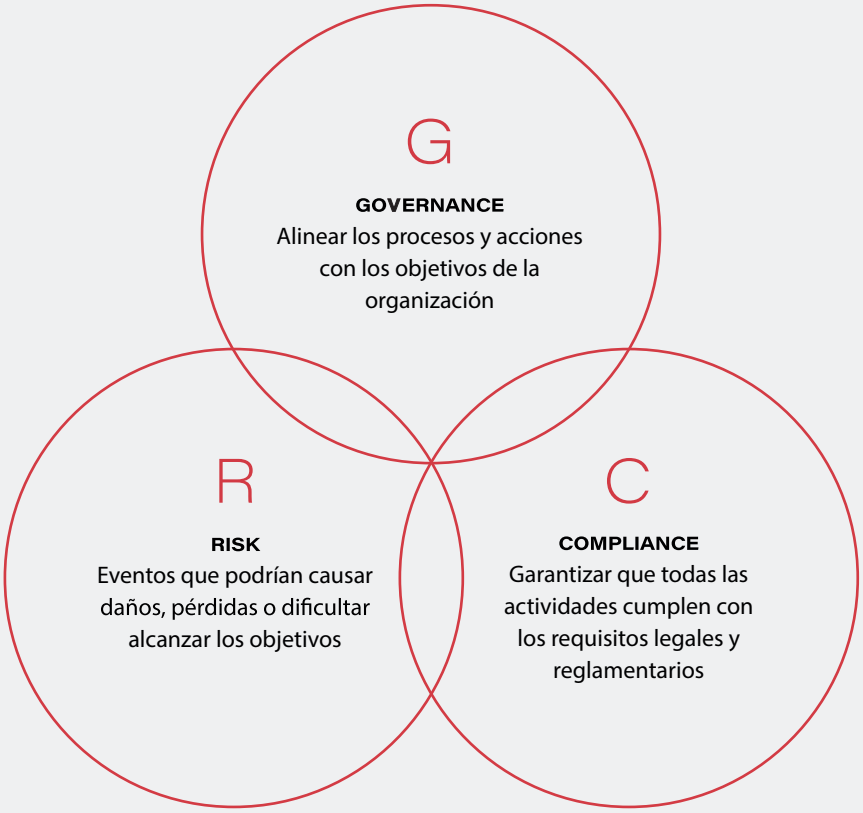

WARRIORS DEFENDER
GRC
Warriors®
"Security that makes difference"

WARRIORS DEFENDER GRC

es una plataforma GRC (Governance Risk Compliance) que puede ser utilizada para cubrir necesidades de Gobierno, Gestión de Riesgos y cumplimientos normativos.

WARRIORS DEFENDER GRC

Ofrece funcionalidades completas al mismo tiempo que mantiene una interfaz sencilla e intuitiva. La plataforma puede implementarse en organizaciones desde pequeñas empresas hasta corporativos con miles de empleados. Así mismo abarcando gran variedad de sectores como gubernamental, financieros, energéticos, educativos, etc.



INFO@WARRIORSLABS.COM
WWW.WARRIORSLABS.COM

¿POR QUÉ UN GRC?

Las organizaciones se enfrentan a un panorama empresarial que cambia rápidamente y es cada vez más complejo.

- **CAMBIOS CONSTANTES EN LAS NORMATIVAS Y SU APLICACIÓN QUE AFECTAN GRAVEMENTE A LAS OPERACIONES EMPRESARIALES.**

- **LA DEMANDA DE LAS PARTES INTERESADAS DE RESULTADOS, CRECIMIENTO CONSTANTE Y PROCESOS TRANSPARENTES.**

- **COSTOS CRECIENTES PARA AFRONTAR LOS REQUISITOS DE CUMPLIMIENTO Y GESTIONAR EL RIESGO.**

- **AUMENTO DE LAS RELACIONES CON TERCEROS Y LOS RETOS DE GOBERNANZA ASOCIADOS.**

- **POSIBLES CONSECUENCIAS LEGALES Y FINANCIERAS DERIVADAS DE LA FALTA DE SUPERVISIÓN EFICAZ Y DE LA OMISIÓN DE AMENAZAS CRÍTICAS.**

¿QUÉ PUEDE HACER POR SU COMPAÑÍA?

GESTIÓN DE CUMPLIMIENTO NORMATIVO

Esto suele ser una forma de demostrar el cumplimiento de normas, regulaciones, etc. Por ejemplo: CSF Cibersecurity Framework NIST, NIST, OWASP Mobile Top 10, OWASP Top 10, ISO27001, ISO27032 y ISO31000., tc. Usted podrá recargar plantillas de cualquier requerimiento que necesite cumplir (o crear el uno propio), vincularlo con sus Controles, Políticas, Etc y a través de estatus, revisiones, auditorías, notificaciones, recolectar la evidencia necesaria demostrar el cumplimiento (o la falta de) de estos requerimientos.

GESTIÓN DE RIESGOS

Warriors Defender GRC puede ayudar a documentar los Riesgos de Activos, de Terceros o de Negocio, hacer un seguimiento de sus revisiones mediante notificaciones e informes, así como describir la forma de resolverlos, Etc. La configuración del módulo de Riesgos le permite definir su propia Clasificación de Riesgos, elegir entre cuatro tipos diferentes de Cálculo de Riesgos, definir su propia Matriz de Riesgos, Etc.

GESTIÓN DE POLÍTICAS

Podrá subir documentación (Políticas, Procedimientos, Normas, Diagramas, Etc) y mostrarlos si lo desea en un Portal de Políticas. A través del uso de filtros, notificaciones y estados, con ello podrá recopilar las pruebas de revisión de las personas en la organización y completar las revisiones a tiempo.

CONTROLES INTERNOS

Podrá documentar sus controles internos, es decir, las actividades que su organización lleva a cabo para mitigar los riesgos y los requisitos de cumplimiento. Describirá cómo y cuándo se deberán llevar a cabo las auditorias.

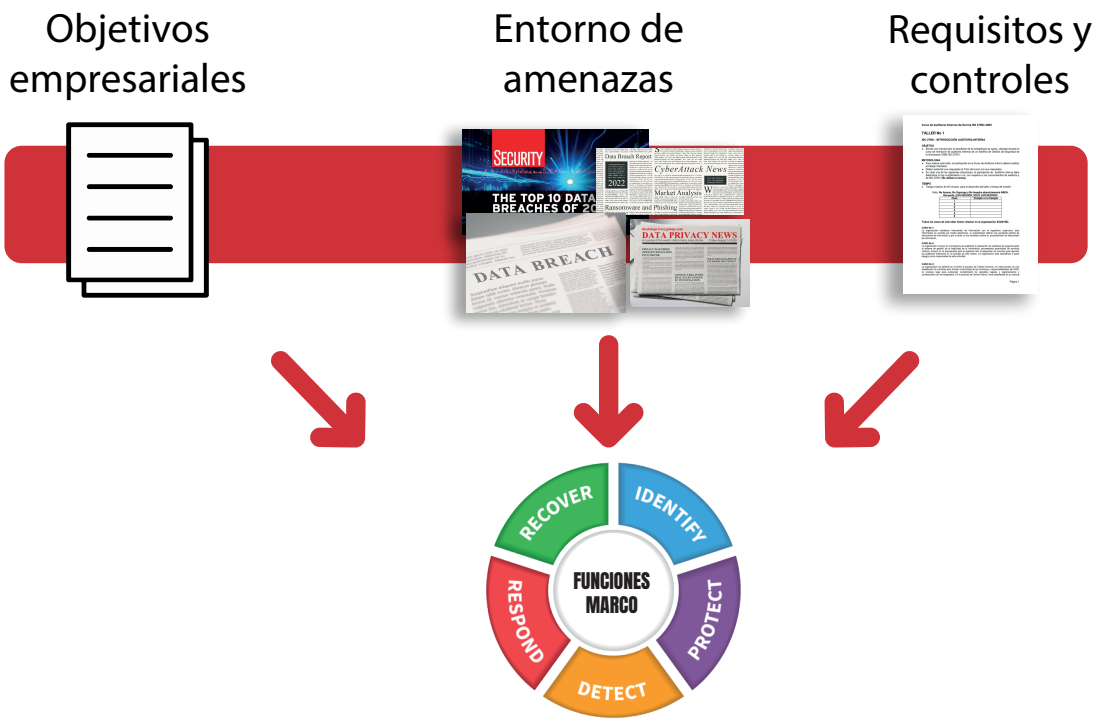
PROTECCIÓN DE DATOS

Este módulo permitirá documentar cómo se mueve la información sensible por la organización (cómo se recopilan, transmiten, modifican, Etc) y para cada uno de ellos describirá qué Controles Internos, Políticas, Riesgos, Proyectos tiene para protegerlos. Una simple matriz hará el trabajo de explicar qué está protegido (¡o no!) y cómo.

- *La solución ofrece un enfoque a la gestión de riesgos acorde a las mejores prácticas internacionales definiendo niveles de riesgo, impacto, frecuencia.*
- *Despliegue fácil y preciso.*
- *Definir la clasificación de información de acuerdo a sus niveles de sensibilidad, así como relacionar con los dueños de la información.*
- *Definir planes de mitigación, acción seguimiento, responsables y vencimientos de controles.*
- *CSF Cibersecurity Framework NIST, NIST, OWASP Mobile Top 10, OWASP Top 10, ISO27001, ISO27032 y ISO31000.*
- *Administrar la evidencia de las acciones realizadas para la aceptación o mitigación de riesgos.*
- *A través de tableros identifique las acciones de implementación y los riesgos gestionados, así como identificar aquellos que tienen o no acciones de mitigación.*
- *Revisar la trazabilidad de los riesgos con sus respectivas soluciones.*

Perfiles del Marco

Los perfiles son la alineación única de una organización de sus requisitos y objetivos organizativos, apetito de riesgo y recursos con los resultados deseados del Marco Básico. Los perfiles se pueden utilizar para identificar oportunidades para mejorar la postura de ciberseguridad mediante la comparación de un perfil "actual" con un perfil "objetivo".



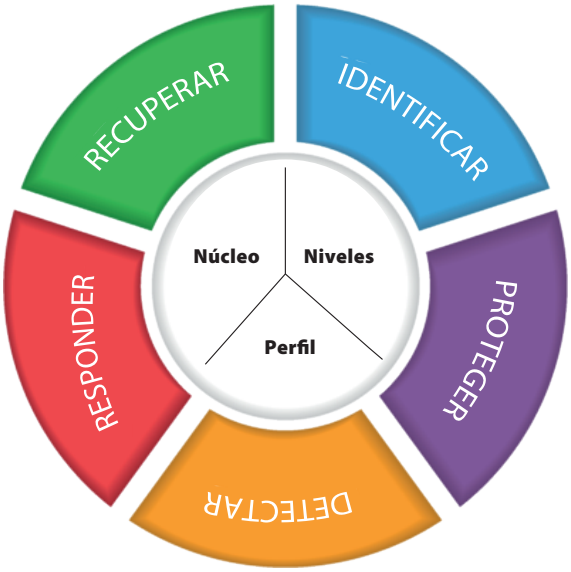
Componentes del Marco

El Marco de Ciberseguridad consta de tres componentes principales:

Núcleo del Marco

Niveles de implementación

Perfiles



Niveles de aplicación del marco

Los niveles describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización presentan las características definidas en el Marco. Los niveles van de Parcial (Nivel 1) a Adaptativo (Nivel 4) y describen un grado creciente de rigor, el grado de integración de las decisiones sobre riesgos de ciberseguridad en las decisiones sobre riesgos más generales y el grado en que la organización comparte y recibe información sobre ciberseguridad de partes externas.

Núcleo del Marco

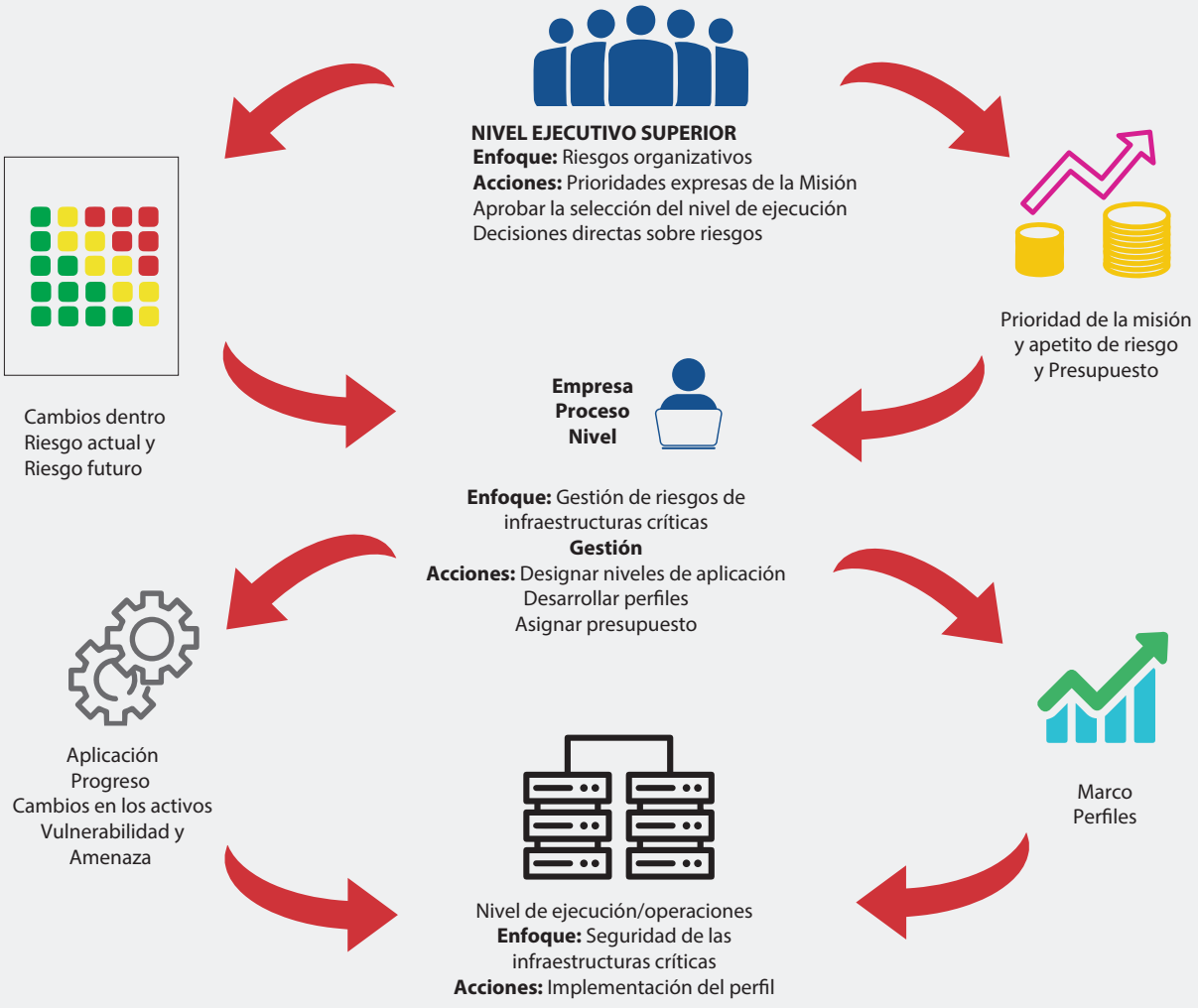
El núcleo es un conjunto de actividades y resultados de ciberseguridad deseados organizados en categorías y alineados con referencias informativas. El Marco Básico está diseñado para ser intuitivo y actuar como una capa de traducción que permita la comunicación entre equipos multidisciplinares utilizando un lenguaje simplista y no técnico. El núcleo consta de tres partes: Funciones, Categorías y Subcategorías. El núcleo incluye cinco funciones de alto nivel: Identificar, Proteger, Detectar, Responder y Recuperar. Estas 5 funciones no sólo son aplicables a la gestión de riesgos de ciberseguridad, sino también a la gestión de riesgos en general. El siguiente nivel son las 23 Categorías que se reparten entre las cinco Funciones. La siguiente imagen muestra las Funciones y Categorías del Marco Básico.

FUNCIÓN	CATEGORÍA	ID
IDENTIFICAR	GESTIÓN DE ACTIVOS	ID.AM
	ENTORNO EMPRESARIAL	ID.BE
	GOBERNANZA	ID.GV
	EVALUACIÓN DE RIESGOS	ID.RA
	ESTRATEGIA DE GESTIÓN DE RIESGOS	ID.RM
	GESTIÓN DE RIESGOS EN LA CADENA DE SUMINISTRO	ID.SC
PROTEGER	GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESOS	PR.AC
	SENSIBILIZACIÓN Y FORMACIÓN	PR.AT
	SEGURIDAD DE LOS DATOS	PR.DS
	PROCESOS Y PROCEDIMIENTOS DE PROTECCIÓN DE LA INFORMACIÓN	PR.IP
	MANTENIMIENTO	PR.MA
	TECNOLOGÍA DE PROTECCIÓN	PR.PT
DETECTAR	ANOMALÍAS Y SUCESOS	DE.AE
	SUPERVISIÓN CONTINUA DE LA SEGURIDAD	DE.CM
	PROCESOS DE DETECCIÓN	DE.DP
RESPONDA	PLANIFICACIÓN DE LA RESPUESTA	RS.RP
	COMUNICACIONES	RS.CO
	ANÁLISIS	RS.AN
	MITIGACIÓN	RS.MI
	MEJORAS	RS.IM
RECUPERAR	PLANIFICACIÓN DE LA RECUPERACIÓN	RC.RP
	MEJORAS	RC.IM
	COMUNICACIONES	RC.CO

ENFOQUE DE APLICACIÓN DEL MARCO DE CIBERSEGURIDAD DE LA BSD

ESTADO ACTUAL	EVALUACIÓN	ESTADO OBJETIVO	HOJA DE RUTA
• Identificar prioridades • Determinar los requisitos de conformidad • Revisar la política y las prácticas existentes • Identificar vulnerabilidades y eventos de riesgo	• Identificar las amenazas • Examinar las vulnerabilidades • Definir la probabilidad • Clasificar los riesgos identificados • Crear un mapa de riesgos	• Identificar enfoques de mitigación • Traducir la mitigación en resultados deseados • Definir objetivos para los resultados deseados • Revisar y definir las prioridades de seguridad	• Cuantificar y puntuar el estado actual • Establecer el presupuesto e identificar los recursos • Definir objetivos dentro del presupuesto • Compartir los resultados con las partes interesadas

MEJORA CONTINUA



Intel utilizó el Marco de Ciberseguridad en un proyecto piloto para comunicar el riesgo de ciberseguridad a la alta dirección, mejorar los procesos de gestión de riesgos y mejorar sus procesos para establecer prioridades de seguridad y los presupuestos asociados a esas actividades de mejora.

Dado que el Marco es voluntario y flexible, Intel optó por adaptarlo ligeramente para ajustarlo mejor a sus necesidades empresariales. Intel modificó los niveles del Marco para establecer criterios más específicos para la medición de su programa piloto de seguridad añadiendo Personas, Procesos, Tecnología y Entorno a la estructura de niveles.

El gráfico que aparece a continuación representa el área de enfoque de Personas de los niveles actualizados de Intel. En el estudio de caso completo se incluyen otras tres áreas de interés.

FOCUS ÁREA	Nivel 1 Parcial	Nivel 2 Riesgo informado	Nivel 3 Repetible	Nivel 4 Adaptable
Personas	Los profesionales de la ciberseguridad (personal) y la población general de empleados han recibido poca o ninguna formación relacionada con la ciberseguridad. El personal tiene una formación limitada o inexistente. La concienciación en materia de seguridad es limitada. Los empleados tienen poca o conocimiento de los recursos recursos de seguridad y seguridad de la empresa.	El personal y los empleados han recibido formación relacionada con la ciberseguridad. El personal dispone de un plan de formación. Existe una concienciación del riesgo de ciberseguridad a nivel organizativo. Los empleados tienen un conocimiento general de la seguridad y de los recursos de seguridad de la empresa y de las vías de escalado.	El personal posee los conocimientos y habilidades para desempeñar sus funciones y responsabilidades designadas. Los empleados deben recibir capacitación y sesiones informativas periódicas relacionadas con la ciberseguridad. El personal de ciberseguridad tiene una capacitación robusta y continua incluyendo conferencias de seguridad o entrenamiento en seguridad interna y externa. La organización y las unidades de negocio tienen un líder en ciberseguridad o personal dedicado.	Los conocimientos y competencias del personal se revisan periódicamente para comprobar su vigencia y aplicabilidad, y se identifican y abordan nuevas competencias y necesidades de conocimientos. Los empleados reciben regularmente formación relacionada con la ciberseguridad y sesiones informativas sobre temas de seguridad relevantes y emergentes. El personal dispone y asiste regularmente a cursos de seguridad interna y externa.

INFO@WARRIORSLABS.COM
WWW.WARRIORSLABS.COM

Frameworks

1.- Marco de ciberseguridad de NIST

El Marco de Ciberseguridad de NIST se organiza en cinco funciones clave: Identificar, Proteger, Detectar, Responder y Recuperar. Cada una de estas funciones tiene una serie de actividades asociadas que, consideradas conjuntamente, proporcionan una visión integral del ciclo de vida de la gestión del riesgo de ciberseguridad en el tiempo.

IDENTIFICAR

Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de: sistemas, activos, datos capacidades.

PROTEGER

Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios.

DETECTAR

Desarrollar e implementar las actividades para identificar cuando ocurra un evento de ciberseguridad.

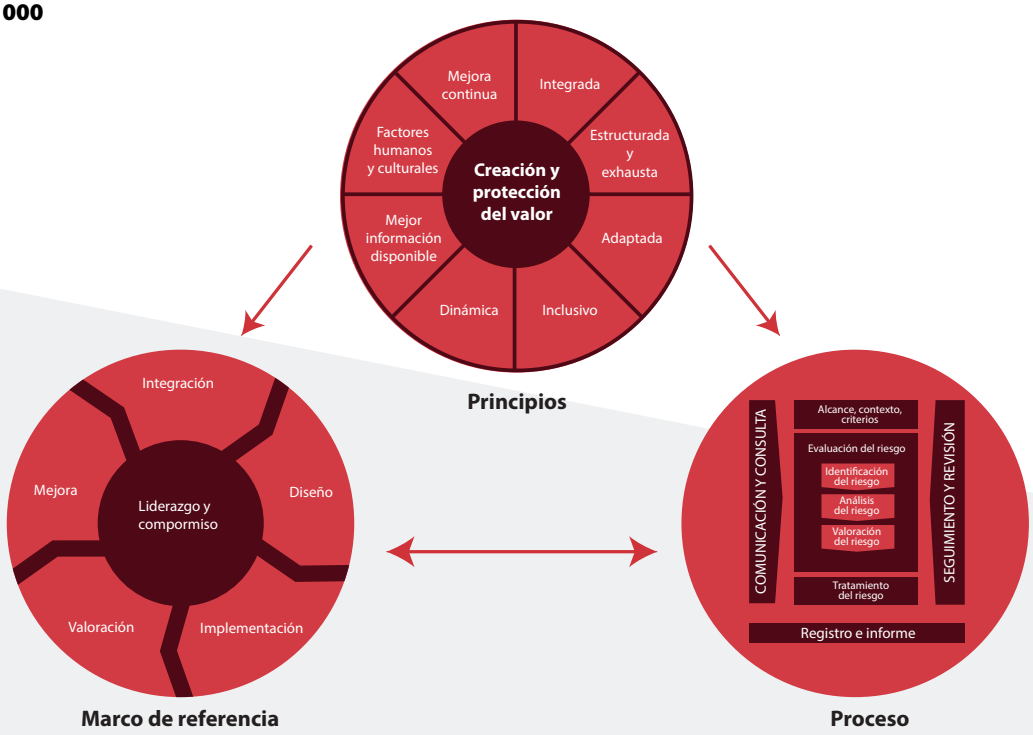
RESPONDER

Desarrollar e implementar las actividades apropiadas para tomar acción en relación con un con un evento de ciberseguridad detectado.

RECUPERAR

Desarrollar e implementar las actividades apropiadas para mantener planes para la resiliencia y para reestablecer cualesquier capacidad o servicio que haya sido afectado durante un evento de ciberseguridad.

2.- ISO 31000

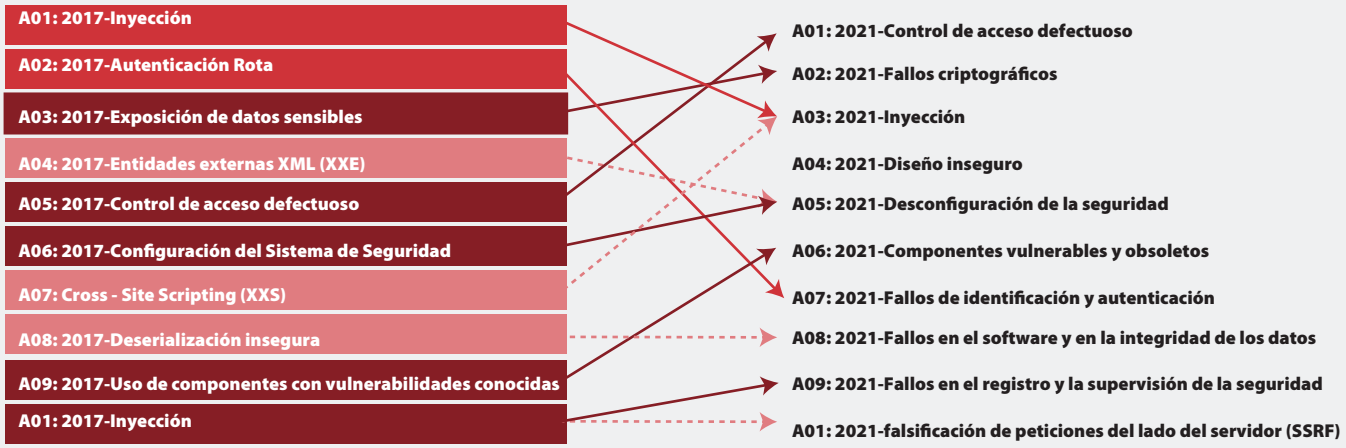


Proceso de gestión de riesgos

La norma ISO 31000 tiene un enfoque de procesos. La implementación de un Sistema de Gestión de Riesgos, portanto, debe seguir una serie de pasos para que sea eficaz y cumpla con los objetivos trazados al inicio. Los pasos básicos son:

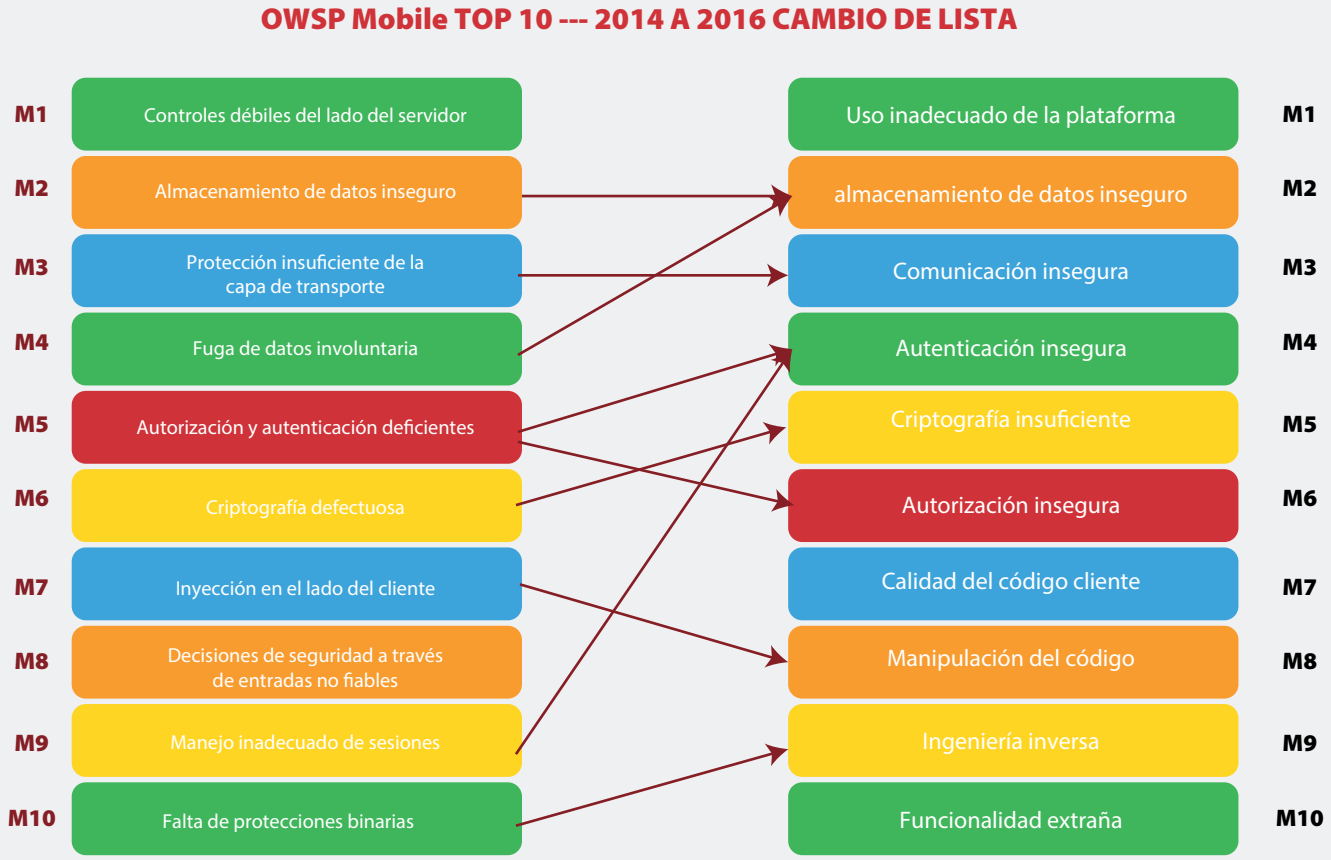
3 .- Owasp Top 10

OWASP Top 10 es una lista de las diez vulnerabilidades de seguridad web más críticas y comunes en las aplicaciones web.



Referencias:
https://owasp.org/Top10/

3 .- Owasp Mobile Top 10



Top 10 Mobile Risks - Final List 2016

- M1: Uso inadecuado de la plataforma
- M2: almacenamiento de datos inseguro
- M3: Comunicación insegura
- M4: Autenticación insegura
- M5: Criptografía insuficiente
- M6: Autorización insegura
- M7: Calidad del código cliente
- M8: Manipulación del código
- M9: Ingeniería inversa
- M10: Funcionalidad extraña

Top 10 Mobile Risks - Final List 2014

- M1: Controles débiles del lado del servidor
- M2: Almacenamiento de datos inseguro
- M3: Protección insuficiente de la capa de transporte
- M4: Fuga de datos involuntaria
- M5: Autorización y autenticación deficientes
- M6: Criptografía defectuosa
- M7: Inyección en el lado del cliente
- M8: Decisiones de seguridad a través de entradas no fiables
- M9: Manejo inadecuado de sesiones
- M10: Falta de protecciones binarias

Referencias

https://owasp.org/www-project-mobile-top-10/

4.- Las 25 debilidades de software más peligrosas del CWE 2022

A continuación se muestra una lista de las debilidades del Top 25 del CWE 2022, incluyendo la puntuación global de cada una. El recuento de KEV (CVE) muestra el número de registros CVE-2020/CVE-2021 de la lista KEV de CISA a los que se ha asignado un número de CVE-2020/CVE-2021.
CISA KEV que fueron asignados a la debilidad dada.

Rango 1D Nombre Puntuación Recuento KEV (CVEs) Rango Cambio frente a 2021

1. CWE-787 Escritura fuera de límites 64,20 62 o)

2. CWE-79 Neutralización inadecuada de entradas durante la generación de páginas web ('Cross-site Scripting')45,97 2 [o]

3. CWE-89 Neutralización incorrecta de elementos especiales utilizados en un comando SQL ('SQL Injection' SQL ('SQL Injection') 22.14 7 +3 tendencia al alza

4. CWE-20 Validación de entrada inadecuada 20,63 20 [o]

5. CWE-125 Lectura fuera de límites 17,67 1 -2 tendencia a la baja

6. CWE-78 Neutralización incorrecta de elementos especiales utilizados en un comando OS ('OS Command Injection') 17.53 32 -1 tendencia a la baja

7. CWE-416 Uso después de libre 15,50 28 o)

8. CWE-22 Limitación indebida de un nombre de ruta a un directorio restringido ('Path Traversal' 14.08 19 [o]

9. CWE-352 Falsificación de petición en sitios cruzados (CSRF) 11.53 1 [o]

10. CWE-434 Carga no restringida de un archivo de tipo peligroso 9.56 6 [o)
11. CWE-476 Desviación de puntero nulo 7.45 O +4 tendencia al alza

12. CWE-502 Deserialización de datos no fiables 46,68 7 +1 tendencia al alza
13. CWE-190 Desbordamiento o envoltura de enteros 653 2 -1 tendencia a la baja
14. CWwE-287 Autenticación incorrecta 6,35 4 [o]

15. CWE-798 Uso de credenciales codificadas 5,66 0 +1 tendencia al alza
16. CWE-862 Falta de autorización 5,53 1 +2 tendencia al alza

17. CWE-77 Neutralización inadecuada de elementos especiales utilizados en un comando ("Command Injection')5.42 5 +8 tendencia al alza

18. CWE-306 Falta de autenticación para una función crítica 5.15 6-7 tendencia a la baja

19. CWE-119 Restricción indebida de operaciones dentro de los límites de un búfer de memoria 4,85 6 -2 tendencia a la baja

20. CWE-276 Permisos por defecto incorrectos4,84 0 -1 tendencia descendente
21. CWE-918 Falsificación de petición del lado del servidor (SSRF) 427 8 +3 hacia arriba tendencia

22. CWE-362 Ejecución concurrente utilizando recursos compartidos con sincronización inadecuada ("Race Condition") 3,57 6 +11 tendencia al alza

23. CWWE-400 Consumo incontrolado de recursos3,56 2 +4 tendencia al alza

24. CWE-611 Restricción indebida de referencia de entidad externa XML 338 0 -1 tendencia a la baja

25. CWE-94 Control inadecuado de la generación de código ("inyección de código") 3,32 4 +3 tendencia al alza

INFO@WARRIORSLABS.COM
WWW.WARRIORSLABS.COM

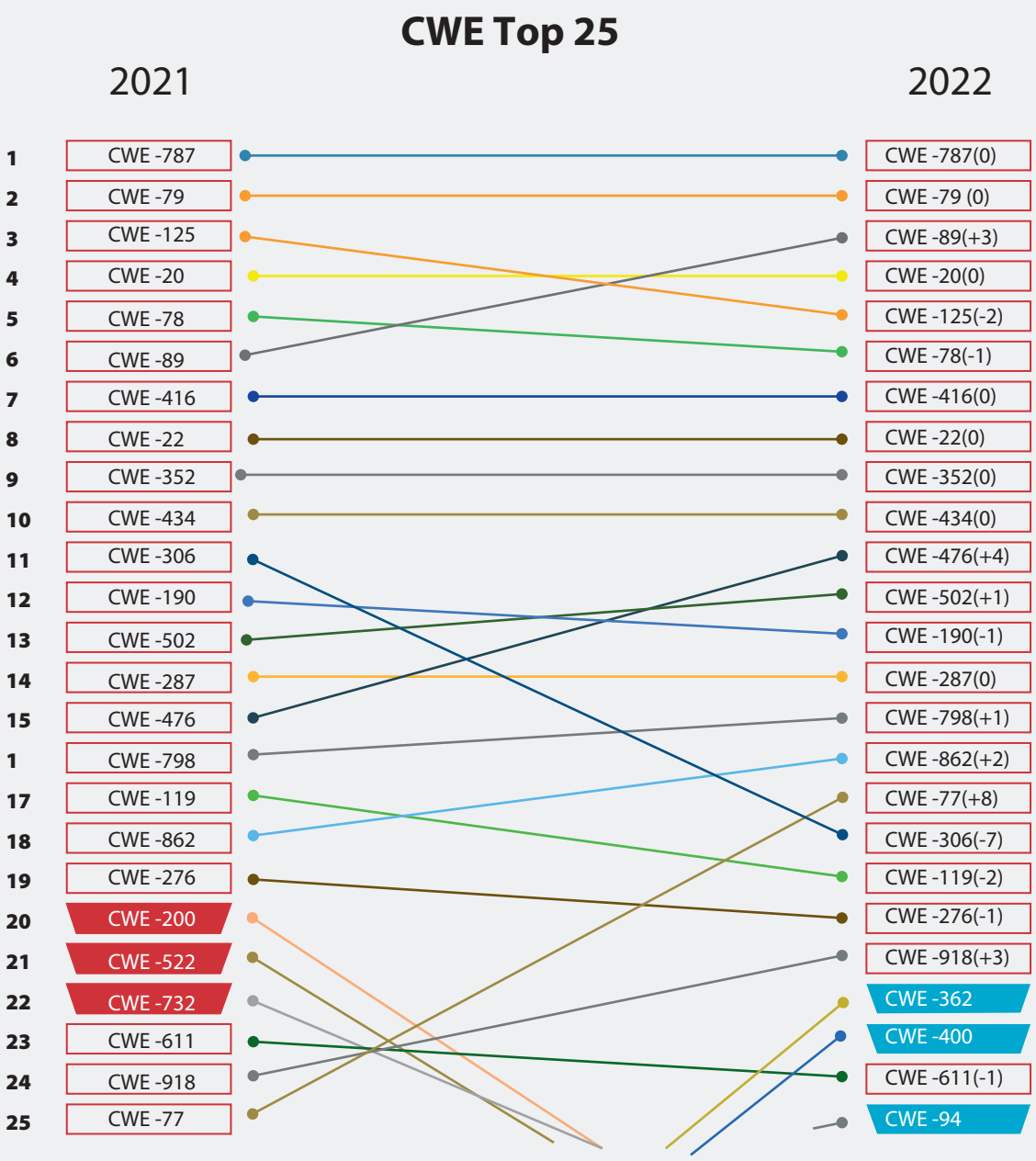


Gráfico Símbolo Clave

Referencias:

https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html


Warriors®
"Security that makes difference"