TABLA DE CONTENIDO

RESUMEN.

El presente proyecto de investigación tiene como finalidad primordial el estudio y análisis de metodologías de sistemas de Ciber-resiliencia, en busca de seleccionar la metodología más adecuada para garantizar el desarrollo de sitios web seguros.

Se realiza una revisión y recopilación de información sobre el tema expuesto en las diferentes bases de datos disponibles que maneja la universidad con el objetivo de crear un marco teórico y elaborar el estado del arte donde se exponga su naturaleza basándose en ideas, conceptos, opiniones etc. Cada ítem fue analizado en relación al tema expuesto de la manera más detallada para que el lector pueda entender las bases fundamentales que sostienen y con que se trabajan en este pilar además de poder alcanzar los objetivos que se establecieron en la propuesta de investigación.

De acuerdo al análisis establecido y los resultados obtenidos, se logrará identificar la metodología de trabajo para implementar un software seguro, donde el mismo permita lograr una seguridad sólida y basada en la resiliencia con el fin de detectar vulnerabilidades y atacar o crear mecanismos de defensa ante cualquier amenaza que se pueda presentar.

Esta investigación y análisis estructurado puede servir como base de estudios e investigaciones en un futuro próximo o lejano para otros estudiantes de la universidad que deseen conocer y aplicar más sobre el tema en relación, queriendo exponer y desarrollar sistemas seguros ante las amenazas que día por día salen e intimida con la confianza y protección de los datos de varios grupos de personas.

Palabras claves: Ciber resiliencia, sistemas, organizaciones, metodologías, técnicas, Ciber seguridad, software seguro.

OBJETIVO GENERAL.

Elaborar el estado del arte de las diferentes metodologías resilientes existentes en el desarrollo de software orientado a la web.

OBJETIVOS ESPECÍFICOS.

- Recopilar información en las diferentes bases de datos académicas sobre las diferentes metodologías resilientes existentes en el desarrollo de software.
- Clasificar y organizar la información obtenida, a través de la herramienta Mendeley.
- Elaborar un artículo de revisión resultado del proceso investigativo.
- Socializar los logros obtenidos en esta fase.

INTRODUCCIÓN

El presente proyecto busca incorporar las investigaciones y metodologías que se han realizado para uno de los temas de mayor avance e impacto de los últimos años. La Ciber resiliencia ha registrado múltiples avances últimamente, permitiendo interceder en los diferentes Ciber ataques y garantizar el desarrollo de entorno web seguros, creando nuevas metodologías y estrategias aplicándolas en un sistema "expuesto".

Para lograr entender y poner en práctica esta útil practica como lo es la Ciber resiliencia, los estudiantes y docentes de la Fundación Universitaria Los Libertadores utilizan el estado del arte donde se reúnen y condensa información relacionada al tema en cuestión, fusionando artículos, informes, extracciones de libros e investigaciones para generar como resultado un escrito con una construcción de un análisis de tipo documental.

1. **SOFTWARE SEGURO.**

La dinámica actual y las actividades cotidianas demandantes de las empresas influenciadas por las nuevas tecnologías han permitido un rápido progreso y exigen que el ser humano esté informado en todo momento de lo que sucede a su alrededor. En un mundo cada vez más cambiante en donde la información está o debe estar disponible en cualquier momento, en cualquier lugar en el mundo y a cualquier hora del año, se requiere tener un mayor acceso, garantizando la usabilidad y accesibilidad como factores primarios de calidad en un desarrollo estimado para software seguro [1].

Calidad en software seguro.

El principal objetivo de la seguridad del software es la construcción del software de más calidad, más robusto y libre de defectos que sigue funcionando correctamente bajo ataque malicioso [1] [2]. Hay una gran cantidad de definiciones en relación al concepto de Calidad, pero una ampliamente aceptada es la establecida por la ISO 9000 [3], la cual define la calidad en un sistema como el "grado en que un conjunto de características inherentes cumple los requisitos".

Estos son establecidos por los usuarios y, por lo tanto, se puede decir que la calidad es un problema subjetivo dependiendo del nivel de satisfacción que el usuario siente con respecto al producto utilizado.

El software también está sujeto a la evaluación de su calidad, de tal manera que los usuarios puedan establecer el grado en que satisfaga sus necesidades. Por otro lado, la calidad se divide en el enfoque tradicional que es responsable de identificar y controlar la calidad, esto se hace a través de una inspección que muestra qué servicio se vería afectado. La responsabilidad se debe a que el inspector tenga el objetivo del departamento y del desarrollo para cumplirlo. Dando al cliente un producto de calidad [1].

En el enfoque utilizado en la actualidad, la persona encargada de la prevención es quien verifica que actividades de la empresa se verán afectadas y es responsable de todos los miembros del grupo de trabajo, preservando la cultura y el compromiso para lograr el pleno cumplimiento del proyecto. Además de la calidad, se debe lograr un buen diseño, accesibilidad confiable y conocimiento de las condiciones de uso de tal manera que la percepción del cliente de un producto permita demostrar que lo que se entregó ha superado las expectativas imaginadas por el cliente [1]

En muchos estudios, se han descritos algunas propiedades que deben cumplir los sistemas para cumplir con las expectativas de los usuarios y evaluar los modelos de calidad [4], entre ellos se pueden resumir tres características, las cuales son:

- **Número de Capas**: Es el nivel de detalle para describir el dominio de software.

- **Tipos de elementos del modelo**: Se distinguen los elementos de alto nivel, para el propósito de clasificación; y los de bajo nivel, para la descripción detallada y evaluación de características observables de los componentes

- **Propósito del modelo**: Al construir un modelo es necesario considerar al menos dos dimensiones: la “específico/general” y la “reutilizable/descartable”.

Así pues, el desarrollo de software seguro es un asunto de alta importancia en las compañías y debería serlo para todas las mismas que tienen procesos que requieren calidad para entregar un producto final, en este caso, se toman las empresas tecnológicas y de consultoría en especial de las aplicaciones web, puesto que la mayoría de ellas dependen altamente de sus aplicaciones para su operación normal [5].

Por consiguiente, es necesario aplicar de forma efectiva las metodologías de desarrollo seguro, determinado en cada fase del ciclo de vida, ciertos aspectos como son:

- Requisitos
- Diseño
- Desarrollo
- Pruebas

A causa de las diferentes metodologías que deben utilizarse para el desarrollo de software seguro, se han podido evidenciar los diferentes estándares que se han generado para su correcta evaluación, entre ellos está por ejemplo el ISO/IEC 9126 [4]. Dicho estándar está muy relacionado con el desarrollo de sitios web de calidad, puesto que es uno de los estándares de evaluación que ha sido reconocido internacionalmente en la evaluación de software desde la perspectiva de la ingeniería de software [6].

Este modelo se considera un estándar válido, confiable y eficiente para evaluar la calidad del software [6]. Cabe resaltar, que dentro del estándar se deben evaluar puntos como la seguridad del software, tanto de escritorio como web.

Por consiguiente, el software seguro que ha sido desarrollado pensando en la seguridad en general, refleja las siguientes propiedades a lo largo de su ciclo de vida de desarrollo, [2]:

- **Ejecución predecible**: Hay confianza justificable que el software cuando se ejecuta funcione Como es debido. La capacidad de entradas maliciosas para alterar la ejecución o resultado de una manera favorable para el atacante se reduce significativamente o se elimina.

- **Confiabilidad**: El número de vulnerabilidades explotables se minimiza intencionadamente en la mayor medida posible. El objetivo es que no haya vulnerabilidades explotables.

- **Conformidad**: Planeadas, las actividades sistemáticas y multidisciplinarias garantizan que los componentes de software, los productos y los sistemas cumplan con los requisitos, las normas y procedimientos aplicables para usos específicos

Las propiedades que se reflejan en un desarrollo de software seguro son importantes, puesto que en la actualidad esta falta de seguridad es la vulnerabilidad que queda en el sistema. Llegando a dudar de la calidad del software presentado [5].

Iniciando con los requisitos, los mismos no deben ser simples listas de chequeos de implementación de controles, como firewalls y antivirus, sino que deben ir más enfocados a la protección de los activos críticos [5].

Por consiguiente, es necesario que las empresas apliquen metodologías y herramientas que permitan desarrollar aplicaciones seguras que cumplan con las exigencias de seguridad en este tiempo [7]. De acuerdo con [5], El Ciclo de Vida de Desarrollo de Software o por sus siglas CDVS (En español), se puede definir como un proceso iterativo, es decir es un proceso que se repite varias veces hasta alcanzar su posible éxito. Estas iteraciones se podrían ver replicadas y aplicadas en alguna metodología a trabajar.

Una vez resumidas y presentado el concepto de calidad en un desarrollo de software seguro, se pasa a revisar la seguridad, la cual debe estar implícita desde la misma concepción del software, porque es un error dejarla para etapas posteriores del desarrollo. Por lo que para el uso de cualquier metodología se recomienda identificar patrones de ataque en todas las fases y almacenarlos en una base de conocimiento que permita prevenir futuros ataques en otras aplicaciones [5] [7].

Un patrón de ataque está basado en vectores de ataque. Este último hace referencia a los tipos de rutas y métodos de ataque de personas con intensiones maliciosas o como se conocen en

algunos sectores “hackers” los cuales buscan aprovecharse de las vulnerabilidades de un sistema con un objetivo específico [8].

Así pues, un patrón de ataque seria las diferentes rutas y métodos que utiliza una persona para la extracción de información de un sistema a partir de una vulnerabilidad encontrada, tomando como punto de partida la experiencia en soluciones que el usuario ha ejecutado pero que no son suficientes para cerrar la brecha [9]

Por consiguiente, es importante saber implementar y manejar los procesos y métodos de “buenas prácticas”, como los que se comentan a continuación por [10].

- Hacer que las prácticas sean ampliamente aplicables, que no específicas de tecnologías, plataformas particulares, lenguajes de programación, modelos SDLC, entornos de desarrollo, funcionamiento ambiente, herramientas, etc.

- Poder ayudar a una organización que actualmente utiliza un modelo clásico de desarrollo de software en transición de sus prácticas de desarrollo de software seguro para usar con un software moderno modelo de desarrollo (p. ej., ágil, DevOps).

Estos son establecidos por los usuarios así pues se puede decir que la calidad es un problema subjetivo dependiendo del nivel de satisfacción que el usuario estos son establecidos por los usuarios y, por lo tanto, se puede decir que la calidad es un problema subjetivo dependiendo del nivel de satisfacción que el usuario [10].

PROPIEDADES DEL SOFTWARE ORIENTADO A LA WEB

Se ha resumido brevemente los parámetros de calidad y seguridad que serán características principales de evaluación en el desarrollo de software seguro, tomando como base la seguridad y las posibles medidas y buenas prácticas que se puedan utilizar para su éxito. No

obstante, a continuación, se describen las propiedades fundamentales del software seguro, para este caso orientado a la web, no sin antes definirlo.

Las propiedades de software se podrían bautizar como un conjunto de atributos fundamentales cuya presencia (o ausencia) son la realidad del terreno que hace el software seguro (o no) y un conjunto de propiedades influyentes que no hacen directamente el software seguro, pero hacen que sea posible caracterizar el grado de seguridad del software [2].

Por consiguiente, se presenta a continuación, una breve descripción de las propiedades fundamentales del software seguro, conforme a lo que habla [11]:

- **Integridad**: capacidad que garantiza que el código del software, activos manejados, configuraciones y comportamientos no puedan ser o no hayan sido modificados o alterados

- **Disponibilidad**: capacidad que garantiza que el software es operativo y accesible por usuarios.

- **Confidencialidad**: capacidad de preservar que cualquiera de sus características, activos manejados, están ocultos a usuarios no autorizados.

Las tres propiedades descritas anteriormente hacen parte de un conjunto de características que componen la seguridad del software y según [11] se estructura de la siguiente forma;

Ilustración 1 - Propiedades del software seguro. Fuente: [11]

Aunque hay conjuntos con más o menos atributos, se sobre entiende la importancia de algunos y los pares que se requieren para su cumplimiento, donde por ejemplo en el apartedo [2] hablan de solo 5 aspectos, entre los cuales agrega dos más a los tres presentados, siendo rendición de cuentas y no repudio.

Estas propiedades básicas son los más utilizados normalmente para describir la seguridad de un software seguro, sirviendo al proyecto puesto que al ser orientado a la web muchas de sus propiedades básicas se pueden asimilar y aplicar al proyecto sin sufrir grandes cambios.

CICLO DE VIDA DEL SOFTWARE.

Es un marco de referencia que contiene los procesos, las actividades y las tareas involucradas en el desarrollo, la explotación y el mantenimiento de un producto de software, abarcando la vida del sistema desde la definición de los requisitos hasta la finalización de su uso [5].

El ciclo de Vida de Desarrollo de Software Seguro describe las fases del ciclo del software y el orden en que esas fases se ejecutan de acuerdo a los requerimientos del negocio, con el fin de implementar los métodos y clases disponibles que se requieren para un procesamiento seguro en por ejemplo diferentes navegadores [12].

Esta herramienta permite a los desarrolladores identificar y mitigar fallas en la seguridad. En la siguiente imagen se describe el ciclo de vida de esta herramienta de acuerdo a [7].

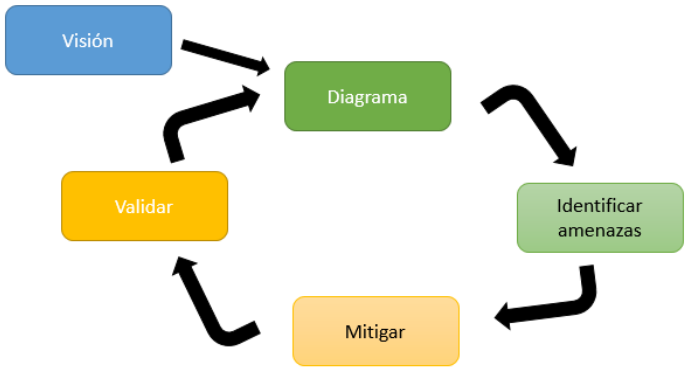

Ilustración 2 - Proceso de modelado de amenazas SDL, Fuente [7]

A continuación, se muestra el ciclo de Vida de un software de acuerdo a los comentarios y análisis de importantes ilustres en sistemas en “pasos”, los cuales serían, [5]:

Security risks:

- Requerimientos
- Análisis / Diseño
- Construcción
- Pruebas
- Producción / Mantenimiento

Llorens, Fábregas, Roger, Pressman:

- Análisis
- Diseño
- Codificación
- Prueba
- Mantenimiento

James A. Senn:

- Investigación Preliminar
- Determinación de los requerimientos
- Desarrollo de software
- Prueba del Sistema
- Implantación y evaluación.

Como se pudo identificar en los comentarios anteriores, existen varias formas de trabajar y desarrollar un SDLC (ciclo de vida del desarrollo de software), muchos de estos SDLC, están creados para enfocarse en proyectos web, donde uno de ellos, siendo el más conocido es el de Microsoft. El cual se muestra a continuación [12];

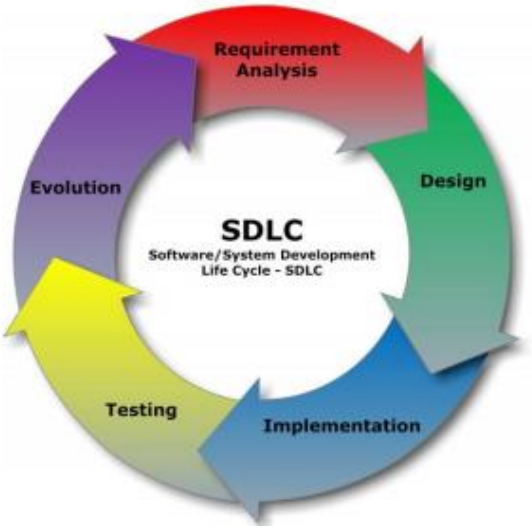

Ilustración 3 - Ciclo de Vida de Desarrollo de Software/Sistemas, Fuente [12]

Como se muestra en la imagen anterior, Microsoft establece cinco (5) parámetros o ítems en los que se debe enfocar un grupo en el desarrollo de un software seguro, por lo que a continuación se describirá brevemente cada ítem del ciclo de Microsoft.

1. **Análisis de requerimientos.**

En esta fase se deben añadir a todos los requerimientos del proyecto, los requisitos de seguridad que surjan como gestión de password y autenticación, la gestión de roles, los requisitos de conocimientos del equipo, el sistema de logs, entre otros [12].

Se debe realizar una evaluación de riesgos que permita identificar los posibles riesgos tales como:

- La cesión de datos a terceros
- La política de confidencialidad
- Los planes de recuperación ante desastres

- La seguridad de los datos de los usuarios.

Los requerimientos en esta fase serían:

- Control de autenticación
- Control de roles y privilegios
- Requerimientos orientados al riesgo
- Aprobación de Privilegios

2. **Proceso de diseño.**

Una vez identificados los requerimientos, durante esta fase, se deberán diseñar las medidas de actuación para los requisitos de seguridad detectados anteriormente [12]. Por ejemplo, se deberá resolver casos como el de la política de contraseñas: se tendrá que determinar si se prefieren contraseñas largas y con pocos cambios o si por el contrario se prefieren cortas y de una menor duración.

Antes de implementar el diseño, se deben tener en cuenta los posibles riesgos de seguridad que puedan existir en la arquitectura o en el propio diseño, ya que, si se detectan en una fase posterior, el coste de solucionar estos problemas será mucho más elevado. En esta fase, el diseño debe tener una segunda revisión vista desde el prisma de la seguridad en el que se traten temas como el cifrado de las comunicaciones, el cifrado de los datos o el uso del cloud en caso de ser contemplado.

3. **Modelado de Amenazas.**

Se representa de manera estructurada, toda la información que afecta a la seguridad del software, buscando capturar, organizar y analizar esta información para tomar decisiones informadas sobre los riesgos de seguridad en las aplicaciones. Permite a las organizaciones

determinar el control correcto y producir contramedidas efectivas dentro del presupuesto [12].

Pasos para llevar a cabo un análisis de modelo de amenazas:

- Recopilar información básica.
- Crear y analizar el modelo de amenazas.
- Analizar las amenazas.
- Identificar las técnicas y tecnologías de mitigación
- Documentar el modelo de seguridad y las
- consideraciones de implementación.
- Implementar y probar las mitigaciones.
- Mantener el modelo de amenazas sincronizado con el
- diseño.

Requerimientos de seguridad en esta fase:

- Acceso a componentes y administración del sistema
- Pistas de auditoria
- Gestión de Sesiones
- Datos Históricos
- Manejo Apropiado de Errores
- Separación de Funciones (Segregación)

4. Proceso de Codificación

Requerimientos de Seguridad en el Proceso de Codificación, [12]:

- Aseguramiento del ambiente de desarrollo.
- Elaboración de Documentación Técnica
- Codificación Segura

- Seguridad en las Comunicaciones
- Seguridad en promoción a ambientes de Producción

Los programadores, suelen seguir algunos patrones propios al realizar código. Lo que se busca en este punto es que el equipo de desarrolladores siga una serie de medidas comunes, Como pueden ser el manual de código de buenas prácticas del CERT o de OWASP o las guías de safecode.

5. **Proceso de Pruebas**

- Requerimientos de Seguridad en la Fase de Pruebas:
- Control de Calidad en Controles de Seguridad
- Inspección de Código por Fases
- Comprobación de Gestión de Configuraciones
- Caja Negra (Top Ten de OWASP, Guía de Pruebas)

Proceso de Despliegue y Mantenimiento

- Requisitos de Seguridad en Fase de Mantenimiento:

Aseguramiento basado en riesgos.
Pruebas de Seguridad (Caja Blanca y Caja Negra) después de los cambios.

Antes de subir la aplicación a producción, se debe revisar que la configuración sea correcta a nivel de seguridad, evitando errores comunes como devolver más información de la debida en caso de error, pues un atacante puede conseguir información adicional que le ayude a preparar su ataque contra nuestra aplicación [12].

Una vez, se ha revisado diferentes características propias del SDCL, es prudente traer a colocación los diferentes estándares que existen de acuerdo a los entes organizacionales internacional de normalización que existe, entre ellos se encuentra precisamente ISO, Cuya

principal actividad es la elaboración de normas y técnicas internacionales [13], entre ellas están las anteriormente descritas ISO 9000 e ISO 9126. A continuación, se describo la ISO 27034, la cual hace referencia a la norma para el ciclo de vida de desarrollo de aplicación, sitios web, seguridad, metodologías, Microsoft SDL [14] .

Es decir. El ciclo de vida de un desarrollo de software es un enfoque por fases del análisis y el diseño que sostiene que los sistemas son desarrollados de una mejor forma mediante el uso de un ciclo especifico de actividades del analista y del usuario [14]. Una aplicación o software basado en el ciclo de vida en su desarrollo permitirá que la misma aplicación se ajuste de acuerdo a las necesidades del negocio.

Por lo que se podría decir que el ISO/IEC 27034 proporciona una orientación para ayudar a las distintas organizaciones a integrar la seguridad en procesos de la aplicación [15].
Algunas soluciones de desarrollo de software orientado a web.

Los objetivos como la velocidad, la agilidad, la flexibilidad y la portabilidad a menudo no se alinean bien con los patrones de arquitectura tradicionales, las estructuras organizativas y las cadencias de entrega. Para satisfacer la velocidad de las demandas del mercado contemporáneo y, por lo tanto, seguir siendo competitivas, las empresas están adoptando filosofías culturales y de entrega, como Agile Development y DevOps [16].

Cuando se cumplen, estos principios abordan simultáneamente la tecnología, la cultura, el proceso y la organización, y su valor proviene de usarlos en combinación. Estos principios ayudan a enmarcar las diversas decisiones que deben tomarse al construir sistemas. El diseño informado por estos principios es crucial, porque, aunque los micros servicios pueden ser pequeños, la amplitud y el impacto de sus arquitecturas no lo son. La arquitectura distribuida también plantea nuevos desafíos y preocupaciones de seguridad, como la autorización y la comunicación de servicio a servicio [16].

Independientemente de la arquitectura, la estructura y cultura de una organización es clave para su resiliencia y éxito. De hecho, la Ley de Conway establece que "Cualquier organización que diseñe un sistema (definido más ampliamente aquí que solo los sistemas de información) inevitablemente producirá un diseño cuya estructura es una copia de la estructura de comunicación de la organización" [16].

La velocidad y la agilidad apuntalan el éxito en la era digital. Desde una perspectiva de desarrollo de software, una pregunta fundamental es cómo lograr innovaciones seguras a velocidad y escala, en lugar de simplemente introducir más vulnerabilidades en los sistemas aún más rápido. Para comprender mejor el papel de los desarrolladores de aplicaciones en el nuevo ecosistema de seguridad, este documento exploró la evolución de las arquitecturas de desarrollo de software y las consecuentes implicaciones en la seguridad que han resultado e impulsado la innovación del marco SDLC.

Después de rescatar los conceptos y aplicaciones de los estándares ISO que se han realizado en el desarrollo al tipo de software seguro que se desea recrear, es imperativo revisar las metodologías que existen para u complete desarrollo e implementación.

Los métodos agiles que permiten tener un desarrollo iterativo, con continuos ciclos de entrega, un permanente contacto con el cliente, accediendo a que los diferentes gestores de riesgo, certificadores, auditores y personal responsable por las políticas de seguridad sean incluidos como parte de los Stakeholders [7].

Así pues, existen metodologías de trabajo en el desarrollo de tecnología de software, como Espiral, cascada, 101 ágil y DevOps (Desarrollo y operaciones) [10], donde a continuación se expone las más conocidas y tenidas en cuenta de acuerdo a [17].

- **MODELO CONSTRUIR Y MEJORAR:** Utilizado por la Volkswagen en la producción y venta de sus vehículos cuyo esquema promueve que el artefacto

terminado se use, y se recopilen las fallas detectadas por los usuarios para mejorarlo. Hoy en día, a pesar de su popularidad, recibe justificadas críticas.

- **MÉTODO EN CASCADA:** Esta fue la época en que Edsger Dijkstra creó la programación estructurada y funciona si cada fase está perfectamente desarrollada, lo cual casi nunca se cumple Propone un desarrollo secuencial.

- **MODELO ITERATIVO RUP:** Se considera uno de los más realistas, pues hace seguimiento entre cada estado y el anterior. El modelo tradicional, que envuelve a la gran mayoría de las metodologías, contempla los siguientes ciclos: especificaciones o modelo funcional, diseño o arquitectura, programación, pruebas, documentación, entrenamiento y mantenimiento. Se acostumbra a expresar la Complejidad del software como una función del tipo de programa (N), el número de entradas (I), el número de salidas (O), y una potencia p de tal manera que:

  Complejidad = N*I*(O elevado a la potencia p).

- **SCRUM**, debido a que está enfocado a la gestión de los procesos de desarrollo y hacer variadas actividades de análisis, diseño, desarrollo, implementación. Se realizan ciclos (o iteraciones) de duración fija llamadas Sprints. Se recomienda que la duración de un Sprint sea de 2, 3 o 4 semanas, Durante el Sprint el objetivo del equipo es generar un incremento visible, utilizable, entregable [5].

No obstante, es imperativo describir y enfocarse más que todo, en las metodologías orientadas al desarrollo web, puesto que algunas de las metodologías descritas anteriormente hacen parte para el desarrollo de proyectos más pequeños o grandes enfocados a aplicaciones de escritorio, store apps etc.

Así pues, se describe a continuación algunas metodologías enfocadas en el desarrollo de software seguro orientado a la web.

Una vez se ha revisado los ítems de calidad y seguridad en las metodologías de desarrollo para determinado software seguro, se describe a continuación algunas metodologías enfocadas en el desarrollo de software seguro orientado a la web.

Dentro de las mismas, se encuentra proyectos de metodologías para el desarrollo de software seguro orientado a la web, como OWASP (Open Web Application Security Project) cuya definición puede tratarse como un espacio abierto de la comunidad dedicada a la búsqueda y lucha contra las causas del software no seguro [18].

Ahora bien, para entender la función de OWASP y otras metodologías, es necesario hablar de temas tan frecuente para todos los estudiantes, profesores y trabajadores enfocados en estos temas, como seria los conceptos de amenazas, riesgos y vulnerabilidades, por lo que a continuación se brinda una breve definición del concepto de cada tema, no obstante, los mismos se buscan ampliar en el capítulo de ciber ataques. Se define qué;

- **Amenaza**, desde sistemas e informática.

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información [19] [20]. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas.

Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

Nota: Los tipos de amenazas se podrán revisar a más detalle, en la sección de ciber ataques.

La presencia de una amenaza es una advertencia de que puede ser inminente el daño a algún activo de la información, o bien es un indicador de que el daño se está produciendo o ya se ha producido [20].

- **Riesgo**, desde sistemas e informática.

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo [21] [22].

Es requerido cuando se revisa la definición de riesgos, analizar la evaluación de riesgos en seguridad de la información, puesto que se utilizan metodologías como matriz de riesgo para su misma evaluación [21].

Esta hace parte de una buena práctica al realizar la gestión de riesgos a los activos de información que se consideren con nivel de clasificación X dependiente de los criterios de clasificación, los cuales seria confidencialidad, integridad y disponibilidad de acuerdo a la siguiente manera, al cuadro que se presenta, [21].

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 4 - Criterios de Clasificación, fuente [21]

Al evaluar los ítems mediante A, B y M. A continuación, se presenta a que hace relación cada evaluador y porque se mide de esta forma, de acuerdo a [21].

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Ilustración 5 - Niveles de Clasificación, fuente [21]

Y en su forma general contiene cuatro fases, [22].

- **Análisis**: Determina los componentes de un sistema que requiere protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo.

- **Clasificación**: Determina si los riesgos encontrados y los riesgos restantes son aceptables.

- **Reducción**: Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas.

- **Control**: Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

La metodología de OWASP por sus siglas en inglés trabaja se basa en los conceptos anteriormente descriptos [7] [23]. Esta metodología y entidad propone un modelo de análisis de amenazas que debe aplicarse a lo largo de vida del desarrollo de aplicaciones, ya que en la medida en que este ciclo se está ejecutando es examinado, identificado y mitigado.

Todas las herramientas, documentos, foros, y los capítulos de OWASP son gratuitos y abiertos a cualquier persona interesada en mejorar la seguridad de aplicaciones [18].

El software es un elemento que es intangible, de acuerdo a las reglas del mercado. En su medida se ha podido corroborar la evolución del mismo debido al creciente desarrollo de aplicaciones que brinda profesiones como ingeniería de sistemas, de software y demás [7].

Como también las múltiples empresas de desarrollo y consultoría que han involucrado diferentes áreas para la gestión de soluciones para la comunidad en cuestiones tecnologías. Estas áreas y demás han colaborado con las múltiples técnicas, métodos y herramientas que hay en el mercado para la construcción de sistemas seguros, utilizando entidades del mercado de seguridad como OWASP [18]. El mismo, no está afiliado con ninguna compañía de tecnología, sin embargo, apoya la utilización de tecnología de seguridad.

Durante el modelado para OWASP existen tres pasos de alto nivel que debe llevar a cabo para la implementación de esta implementación, los cuales de acuerdo a [7] son;

Descomponer la aplicación: Esto significa que se debe hacer un barrido en la aplicación, para conocer e identificar las relaciones o interacciones que tiene esta aplicación con el exterior y el medio ambiente en el que se encuentra. La información es de entrada y salida, además de revisar que tipos de data se pueden manejar y Como es manejada esta información y el almacenamiento, además de identificar las amenazad severas y luego categorizarlas y darles una jerarquía.

Dar jerarquía a las amenazas: Una vez identificada las diferentes amenazas es importante asignarles una jerarquía, que puede ser usada en diferentes modelos Como STRIPE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) o español como Suplantación de identidad, manipulación indebida, repudio, divulgación de información, denegación de Servicio, elevación de privilegios. Que ayuda a identificar las amenazas en los componentes del sistema a un nivel de ataque dependiendo de las categorías, permitiendo la creación de árboles de ataque.

Estos árboles ayudan a identificar tanto las amenazas como las causas del mismo. Se pueden utilizar modelos como DREAD (Damage, Reproducibility, Exploitability, Affected users, Discoverability) en inglés o español como Daños, reproducibilidad, explotabilidad, usuarios afectados, defectibilidad, que ayuda a sopesar las amenazas identificadas en función de su riesgo.

Mitigar las amenazas: Después de asignar la jerarquía a las amenazas. Un mapa de mitigación se requiere hacer, donde la amenaza puede ser asignada y la acción tomada para mitigarla. Es importante destacar que cada uno de estos pasos debe documentarse y comunicarse con las partes interesadas. Es importante realzar cada uno de los pasos que se documentan y comunican con las partes interesadas, indicando como se puede mitigar y dar el seguimiento para identificar el estatus que se encuentra cada una. OWASP ha aplicado esta misma técnica para identificar las vulnerabilidades en los dispositivos móviles que se muestran a continuación.

En la siguiente tabla se muestra 10 vulnerabilidades encontradas que han podido identificar con dicha metodología, a partir de eso se puede determinar las vulnerabilidades que en común afectan en su gran medida para software seguros orientados a la web, de acuerdo a [7].

Vulnerabilidades	Descripción
Uso inapropiado de la plataforma	Uso indebido de los controles de seguridad del sitio web
Almacenamiento de datos inseguros	Es una combinación junto con la vulnerabilidad 4, La cual abarca el almacenamiento inseguro y fugas de información no deseada
Comunicación insegura	Cubre protocolos, versiones SSL incorrectas, negociación débil, comunicación sin cifrar de datos sensibles.
Criptografía insuficiente	El código aplica la criptografía a un activo de información sensible.
Autorización insegura	Sirve para capturar cualquier falla de autenticación
Calidad del código del cliente	Desbordamiento de búfer, vulnerabilidades de cadena de formato y varios otros errores de nivel de código donde la solución es reescribir un código
Código de alteración	Cubre parches binarios, modificación de recursos locales, métodos ganchos, método swizzling y modificación de memoria dinámica. Un atacante puede modificar directamente el código, cambiar dinámicamente el contenido de la memoria, cambiar o reemplazar las API del sistema utilizado por la ampliación o modificar los datos y recursos de la aplicación
Ingeniería inversa	Esta categoría incluye análisis de kernel binario final para determinar su código fuente, bibliotecas, algoritmos y otros activos.
Funcionalidad extraña	Los desarrolladores incluyen una funcionalidad de puerta trasera oculta u otros controles de seguridad internos que no se deben colocar en un entorno de producción.

Ilustración 6 - Vulnerabilidades identificadas por OWASP, Fuente: [7]

Dentro de las vulnerabilidades de seguridad que se muestran en la Ilustración 6, se tomaron las vulnerabilidades más relevantes, donde la aplicación de las pautas de OWASP para con los siguientes elementos, de acuerdo a [7]

- Manejo de contraseñas y autenticación
- La ofuscación del código
- Seguridad de la comunicación
- Almacenamiento y protección de datos.
- Control de pagos
- Gestión de la sesión

De acuerdo con las tendencias descritas, se considera que ocurre antes de la aparición de lo que algunos investigadores llaman ingeniería de seguridad, como complemento de la Ingeniería de Software Seguro, cuyo alcance incluye de acuerdo a [7], algunos de los siguientes:

- La ingeniería de requisitos de seguridad,
- El modelo de seguridad y
- El desarrollo de software seguro

Su principal objetivo como campo de investigación es la producción de:

- Técnicas
- Métodos
- Procesos
- Herramientas

Que integren los principios de ingeniería de seguridad y calidad, y que permitan a los desarrolladores de software analizar, diseñar, implementar, probar e implementar sistemas de software seguro [7].

Esta nueva área de ingeniería ofrece varias ventajas, entre las que se encuentran:
Permitir el desarrollo de mejores técnicas relacionadas con la seguridad y mejores definiciones de esquemas metodológicos de trabajo.

Ofrecer la base para una ontología de seguridad completa y reconocida, que permita a los desarrolladores considerar no solo los desafíos tecnológicos relacionados con la seguridad, sino también las implicaciones sociales derivadas de ellos.

Es importante entender que, al igual que la tecnología está en constante evolución, también están evolucionando las técnicas de Ciber crimen [7]. También debe tenerse en cuenta que la revisión de vulnerabilidades no es una tarea estática con el tiempo, sino una tarea dinámica y en evolución, porque con cada el grado de seguridad avanzado debe compararse con las características existentes y nuevas que formarán parte de la aplicación.

Otras metodologías y estándares de control, diferentes a OWASP que integran y desarrollan software seguro, están [24];

- **LOS SIETE PUNTOS DE CONTACTO DE GARY MCGRAW.**

De acuerdo a Gary McGraw [11], Se tocan siete puntos de vital importancia, dichos puntos conforman un conjunto de buenas prácticas de seguridad que pueden ser aplicadas sobre los artefactos de software durante la fase de Desarrollo.

A continuación, se explican brevemente los siete puntos, según [25];

- **Revisión del código Paso más efectivo**: El primer paso se sugiere aplicar durante la codificación, eliminando y sustrayendo problemas en la fuente que pueden ocasionar dolores de cabeza más adelante en SDLC.
- **Análisis de riesgo arquitectónico**: Los defectos de diseño no son obvios al mirar el código; necesitan ser identificados en la fase de diseño. El análisis de riesgos arquitectónicos considera la seguridad durante el diseño, entre ellos, se considera las siguientes acciones:
  - ✓ Amenazas de seguridad
  - ✓ Vulnerabilidades
  - ✓ Impacto y probabilidad
  - ✓ Riesgo

- **Pruebas de penetración:** Es una de las partes de la metodología predominante en la actualidad, llegando a ser tan efectivo porque considera un programa en el entorno final. Encontrados problemas reales, como por ejemplo las vulnerabilidades demostrables que facilitan los costos de reparación.

  Incluye como plus para aplicar el famoso comentario de Beware Dijkstra: "Las pruebas muestran la presencia, no la ausencia de errores. Simplemente ejecutar algunas herramientas estándar de prueba de lápiz es una prueba muy mínima"

- **Pruebas de seguridad**: Las pruebas de seguridad complementan los procesos de control de calidad que aseguran que los requisitos funcionales principales estén libres de errores. Dentro de las pruebas se sugiere revisar;

  - ✓ Prueba de la funcionalidad de seguridad: Disposiciones de seguridad y métodos estándar.

  - ✓ Pruebas basadas en patrones de ataque usar casos: aplicar análisis de riesgos para priorizar y considerar patrones de ataque

    Enfocándose en
  - ✓ Requisitos funcionales explícitos: verifique los casos de uso, opere como se espera y el cliente puede agregar / eliminar artículos del carrito
  - ✓ A veces requisitos explícitos no funcionales: comprobar usabilidad, rendimiento la experiencia del usuario es agradable

- **Idea**: Describe el comportamiento deseado del sistema de diferentes tipos de abuso/mal uso.

- ✓ Trabaje a través de patrones de ataque, por ejemplo... entrada ilegal / de gran tamaño.
- ✓ Examine los supuestos hechos, por ejemplo. la interfaz protege el acceso a los datos de texto sin formato.
- ✓ Considere eventos inesperados, por ejemplo. error de memoria, desconexión del servidor

Se deben completar detalles específicos como para un caso de uso. Idea relacionada: anti requisitos

- **Requisitos de seguridad:** Las necesidades de seguridad deben considerarse explícitamente en la etapa de requisitos.

✓ Los requisitos de seguridad funcional, por ejemplo: utilizan una criptografía sólida para proteger los datos confidenciales almacenados.

✓ Requisitos de seguridad emergentes, por ejemplo: Que no revele la configuración del servidor web en solicitudes erróneas.

- **Operaciones de seguridad**: La seguridad durante las operaciones significa administrar la seguridad del software implementado.

Tradicionalmente, este ha sido el dominio de los profesionales de seguridad de la información.

La idea de este punto de contacto es combinar la experiencia de las diferentes áreas involucradas.

- **CORRECTNESS BY CONSTRUCTION (CbyC)**

Enfoque de corrección por construcción para el desarrollo de software está relacionado en el enfoque de varias configuraciones algorítmicas de pequeña a gran escala [26].

Mediante CbyC, se entiende como un enfoque para la construcción de software que comienza con una especificación abstracta del problema en cuestión y que progresa de manera ordenada y gradual hacia especificaciones cada vez más concretas. En cada paso, se siguen las reglas que garantizan y por lo tanto prueban la corrección.

Si se aplica estrictamente, entonces el paso final entrega un algoritmo que se garantiza que es correcto en el mismo sentido que la prueba de un teorema matemático es correcta. Esto requiere que la semántica de la notación en la que se articula el algoritmo esté bien definida. Como el lenguaje de comando protegido (GCL) de Dijkstra cumple con este requisito y también es conciso, se usa comúnmente como una notación [26].

- **COMPREHENSIVE, LIGHTWEIGHT APPLICATION SECURITY PROCESS (CLASP)**

El proceso de integral y ligero de seguridad de aplicaciones (CLASP) introduce un proceso ligero para SSD. CLASP proporciona prácticas estructuradas para derivar los requisitos de seguridad de los sistemas de software [27].

CLASP es el resultado de años de trabajo de campo extenso en el que los recursos del sistema de muchos ciclos de vida de desarrollo se descompusieron metódicamente para crear un conjunto integral de requisitos de seguridad. Estos requisitos resultantes forman la base de las mejores prácticas de CLASP que permiten a las organizaciones abordar sistemáticamente las vulnerabilidades que, si se explotan, pueden provocar la falla de los servicios de seguridad básicos, por ejemplo, confidencialidad, autenticación y control de acceso [27].

CLASP describe siete mejores prácticas clave, como, por ejemplo;

- Conciencia de seguridad
- Evaluaciones de aplicaciones
- Derivación de requisitos de seguridad
- Implementación de prácticas de desarrollo seguras
- Desarrollo de medidas de corrección de vulnerabilidades
- Definición y monitoreo de métricas
- Publicación de pautas operativas.

CLASP también especifica un conjunto de actividades que deben incorporarse en él SDLC. CLASP proporciona roles y seguridad para estructurar y respaldar las actividades en la metodología de recursos [28].

Dado que el modelo CLASP permite la adaptación de sus prácticas, este modelo puede usarse para seleccionar las prácticas más aplicables por la organización, por lo tanto, produce un software seguro aceptable. Además, la organización también podrá mejorar sus debilidades al tomar medidas para lograr todos los factores necesarios para implementar prácticas seguras de desarrollo de software [28].

Es un proceso ligero, consta de 24 actividades relacionadas con la seguridad de alto nivel que pueden incorporarse total o parcialmente en el software que se está construyendo durante el ciclo de vida del desarrollo de software. Cada actividad CLASP se divide en componentes de proceso discretos y está vinculada a uno o más roles específicos del proyecto, esto proporciona una guía para el participante del proyecto y da como resultado mejoras incrementales para la seguridad en el ciclo de vida del software [29].

- **APPROPRIATE AND EFFECTIVE GUIDANCE IN INFORMATION SECURITY (AEGIS)**

Investigadores del University College London han desarrollado un modelo para la Orientación apropiada y efectiva en seguridad de la información (AEGIS), dicho modelo de investigación que ha integrado la seguridad y la usabilidad utilizando un modelo en espiral, basado en UML [28].

AEGIS es una guía para los desarrolladores en el proceso de tratar con los requisitos de seguridad y usabilidad en el diseño del sistema. El metamodelo UML definido por los autores identifica;

- Los activos
- El contexto de operación
- Respaldo el modelado de los requisitos de seguridad

Todas las decisiones de seguridad en AEGIS se derivan del conocimiento de los activos del sistema.

Las actividades básicas de seguridad para las sesiones de diseño del sistema en AEGIS son, [28]:

- Identificación de activos
- Requisitos de seguridad
- Análisis de riesgos
- Diseño seguro
- Identificación de riesgos
- Vulnerabilidades y amenazas para el sistema.

El resultado de estas actividades se documenta en un documento de diseño que consiste en la arquitectura del sistema con todas las contramedidas especificadas [28].

En AEGIS, la experiencia en seguridad está ausente en el proceso de desarrollo. Además, la toma de decisiones en la selección de contramedidas de seguridad es realizada por las partes interesadas. La lógica del autor detrás de esto es que los tomadores de decisiones están "mejor preparados para hacer frente a la aplicación de los requisitos sociales de seguridad", mientras que los desarrolladores son "necesarios para la implementación técnica de la seguridad" [28].

Este proceso, basado en el modelo espiral, se integra en los ciclos de vida normales de ingeniería de software, como se puede ver en su aplicación al modelo Spiral de desarrollo de software como se muestra en la siguiente figura [29].

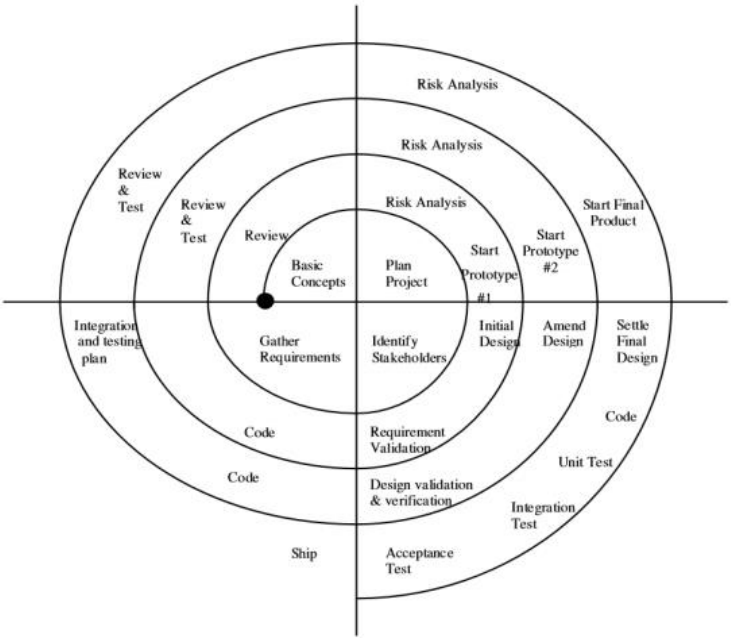

Ilustración 7 – Modelo en espiral para el desarrollo de software AEGIS, Fuente [29]

El proceso identifica los requisitos de seguridad primero determinando los activos del sistema y sus relaciones, luego el análisis de riesgos en el que se identifican vulnerabilidades, amenazas y riesgos [29].

- **SECURE SOFTWARE DEVELOPMENT MODEL (SSDM).**

El modelo de desarrollo de software seguro (SSDM) desarrollado en la Universidad de Agricultura de Nigeria integra actividades de seguridad en el proceso de ingeniería, que son: capacitación en seguridad, modelado de amenazas, especificación de seguridad, revisión de la especificación de seguridad y pruebas de penetración. Además, SSDM ha separado la especificación de seguridad de la especificación funcional [28].

La capacitación en seguridad proporciona educación de seguridad adecuada a las partes interesadas en el desarrollo de software. El modelo de amenaza identifica a los atacantes y sus capacidades y se realiza durante la fase de requisitos. Después de eso, la especificación de seguridad debe definirse estableciendo las pautas sobre cómo se logrará la seguridad.

Este modelo incorpora diversas actividades de seguridad en un modelo de ciclo de vida de desarrollo de software en cascada, como se muestra a continuación;

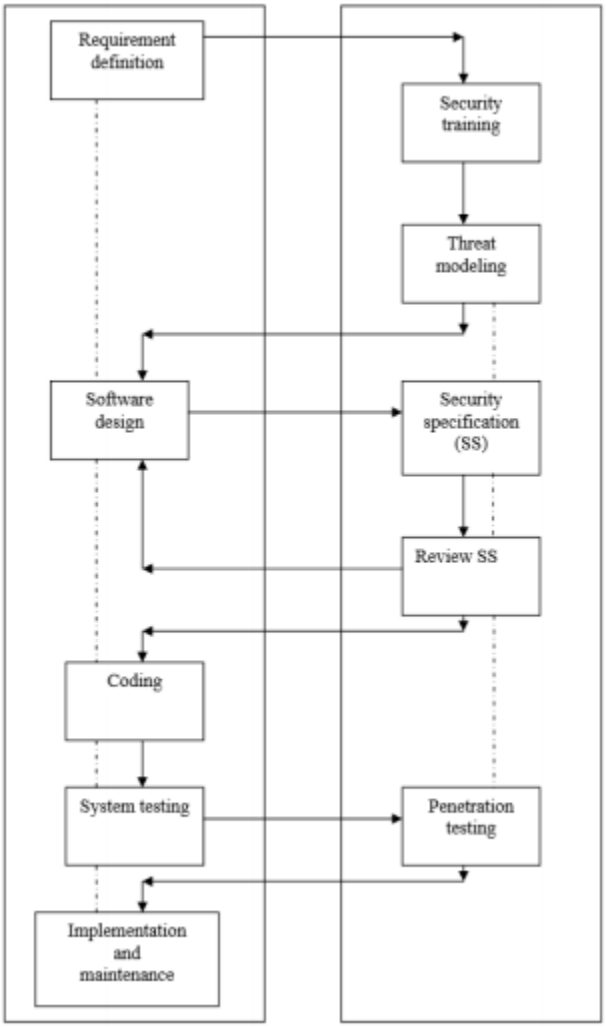

Ilustración 8 - Flujo de Secure Software Development Model, fuente *[30]*

Este modelo inicialmente se enfoca en construir conceptos de seguridad en las primeras etapas de SDLC. Proporcionando un medio para obtener, clasificar y priorizar los requisitos de seguridad para los sistemas y aplicaciones de tecnología de la información.

- **SOFTWARE ASSURANCE MATURITY MODEL (SAMM)**

El Modelo de Madurez de Software Assurance (SAMM) es un marco abierto para ayudar a las organizaciones a formular e implementar una estrategia de seguridad de software que se adapte a los riesgos específicos que enfrenta la organización [31] .

Los recursos proporcionados por SAMM ayudarán a:

- Evaluar las prácticas de seguridad de software existentes de una organización.
- Construir un programa de garantía de seguridad de software equilibrado en iteraciones bien definidas.
- Demostrar mejoras concretas a un programa de garantía de seguridad.
- Definir y medir actividades relacionadas con la seguridad en una organización

SAMM se definió teniendo en cuenta la flexibilidad de modo que pueda ser utilizado por organizaciones pequeñas, medianas y grandes utilizando cualquier estilo de desarrollo. Además, este modelo se puede aplicar en toda la organización, para una sola línea de negocio o incluso para un proyecto individual. Dentro de la metodología, se encuentras los puntos que trata, de tal forma de acuerdo a [31]

- El comportamiento de una organización cambia lentamente con el tiempo: un programa de seguridad de software exitoso debe especificarse en pequeñas iteraciones que brinden ganancias de seguridad tangibles mientras se trabaja progresivamente hacia objetivos a largo plazo.

- No existe una receta única que funcione para todas las organizaciones: un marco de seguridad de software debe ser flexible y permitir a las organizaciones adaptar sus elecciones en función de su tolerancia al riesgo y la forma en que construyen y usan el software.

- La orientación relacionada con las actividades de seguridad debe ser prescriptiva: todos los pasos para construir y evaluar un programa de aseguramiento deben ser simples, bien definidos y medibles. Este modelo también proporciona plantillas de hoja de ruta para tipos comunes de organizaciones

- **TEAM SOFTWARE PROCESS (TSP)**

El Team Software Process conocido también como TSP, es de gran ayuda para los ingenieros informáticos, ya que provee métodos para el fácil desarrollo de software por medio de miembros que llegan a formarse en equipos, en el cual se desenvuelven de una manera organizada [32].

Estos miembros tienen su función propia y los coordina un líder de proyecto el cual recopila información y los mantiene ordenados, para conseguir los objetivos planteados. En lo general, un desarrollo de proyectos de software, viene a ser realizado por equipos de ingenieros, este desarrollo es, un esfuerzo colectivo que necesita conocimientos y orientación de las actividades planeadas. Si se desea desarrollar un software, siempre es imprescindible utilizar un método como lo es el TSP, para lograr un producto confiable, organizado y de buena calidad.

Esta herramienta es considerada como una metodología para administrar el trabajo de mejora desarrollo de los procesos de software, además de garantizar un entorno de trabajo agradable y natural para los equipos [32]. El TSP brinda un conjunto de pasos bien estructurados que indican qué hacer en cada fase del desarrollo del proyecto y muestra cómo conectar cada fase para construir un producto completo, además brinda una ayuda acerca de cómo conformar equipos para el desarrollo de software de calidad.

Los objetivos de TSP son:

- Tener equipos rápidos y confiables.
- Maximizar calidad del software, minimizar costos.
- Integrar equipos independientes de alto rendimiento que planeen y registren su trabajo, establezcan metas, y sean dueños de sus procesos y planes.
- Mostrar a los gerentes como monitorear y motivar a sus equipos de trabajo y como ayudarlos a alcanzar su máxima productividad.
- Acelerar la mejora continua de procesos.
- Proveer de una guía para el mejoramiento en organizaciones maduras.

- **ORACLE SOFTWARE SECURITY ASSURANCE (OSSA)**

Para poder abarcar cada fase del SDLC, Oracle Software Security Assurance (OSSA) es la metodología de Oracle para crear seguridad en el diseño, el desarrollo, la prueba y el mantenimiento de los productos ya sea que los clientes los usen en las instalaciones o se entreguen a través de Oracle Cloud [33]. El objetivo de Oracle es garantizar que sus productos ayuden a los clientes a cumplir con sus requisitos de seguridad y proporcionen la experiencia de propiedad de costo más efectivo.

OSSA es un conjunto de normas, tecnologías y prácticas líderes en el sector que cuenta con los siguientes objetivos, conforme a [33];

- **Promover innovaciones de seguridad.** Oracle tiene una larga tradición en innovaciones de seguridad. En la actualidad, este legado continúa con soluciones que ayudan a las organizaciones a implementar y administrar políticas de seguridad coherentes en todo el centro de datos de la nube híbrida: seguridad de base de datos y administración de identidades, y monitoreo de seguridad y análisis.

- **Reducir la incidencia de las deficiencias de seguridad en todos los productos de Oracle.** Los principales programas de OSSA incluyen los Estándares de codificación segura, el entrenamiento obligatorio en seguridad para el desarrollo, la formación de líderes en seguridad dentro de los grupos de desarrollo y el uso de herramientas automatizadas de análisis y prueba de Oracle.

- **Reducir el impacto que tienen sobre los clientes las deficiencias de seguridad de los productos lanzados.** Oracle ha adoptado políticas transparentes sobre corrección y divulgación de vulnerabilidades de seguridad. La empresa se compromete a tratar a todos los clientes por igual y a brindar la mejor experiencia posible en actualización de la seguridad a través de los programas de Actualización de versión crítica y alertas de seguridad.

- **RATIONAL UNIFIED PROCESS-SECURE (RUPSec)**

El Ratonar Unified Process (RUP) es la metodología de desarrollo de sistemas más apropiada que puede guiar a los investigadores en la generación de artefactos seguros [34] [35]

RUP podría considerarse como una de las mejores y más completas metodologías para el desarrollo de sistemas que se puede utilizar como investigación de un dominio determinado en la ingeniería de software [35].

RUP es uno de esos enfoques de SDLC que permite producir software de calidad. RUP consta de las siguientes cuatro fases [36]:

- Inicio
- Elaboración
- Construcción
- Transición

RUP proporciona un enfoque disciplinado sobre cómo asignar tareas y responsabilidades dentro del proceso de desarrollo de software [36].

Se compone de nueve flujos de trabajo de proceso entre ellos: modelado empresarial, requisitos, análisis y diseño, implementación, prueba, implementación, gestión de configuración, gestión de proyectos y entorno. En cada flujo de trabajo de proceso se correlaciona un conjunto de artefactos y actividades, por ejemplo, modelo de negocio, modelo de caso de uso, etc. RUP proporciona un marco de proceso genérico, que se puede personalizar para adaptarse muchos proyectos diferentes, diferentes tipos de organizaciones, diferentes niveles de competencia y diferentes tamaños de proyectos [36].

Por lo tanto, se puede decir que RUP tiene la fuerza y la capacidad de ayudar a los investigadores a generar artefactos de manera sistemática y producir los documentos necesarios en la fase inicial y de elaboración. Esto se debe a las características de RUP en sí que pueden guiar a los investigadores en la creación de una arquitectura centralizada, un proceso iterativo y adicional [36].

- **WATERFALL-BASED SOFTWARE SECURITY ENGINEERING PROCESS MODEL**

Hace parte del modelo clásico y conocido también como lineal o “cascada” [37]. *El* modelo de *cascada* es el primer enfoque SDLC (ciclo de vida de desarrollo de software) que se utilizó para el desarrollo de software [38].

Características del modelo, de acuerdo a [37] ;

- Está compuesto por una serie de fases que se ejecutan secuencialmente
- Paso de fase al conseguir los objetivos
- Obtención de documentos como criterio de finalización de fase

- El final de una fase puede suponer un punto de revisión

En su enfoque, el proceso se divide en cuatro fases separadas. El resultado de una fase actúa como entrada para la siguiente fase, continuando este proceso hasta el final [38]. Esto significa que cualquier fase del proceso de desarrollo comienza solo si se completa la fase anterior.

El modelo de cascada es un proceso de diseño secuencial en el que se ve que el progreso fluye constantemente hacia abajo (como una cascada) a través de las fases de ***Concepción, Iniciación, Análisis, Diseño, Construcción, Pruebas, Producción / Implementación y Mantenimiento*** [38].

CIBER ATAQUES

Un ciberataque puede definirse como un delito cibernético, el cual puede tener múltiples consecuencias cuya gravedad dependerá de cada caso y de la intención del delincuente [39]. En consecuencia, es importante tomar medidas de seguridad para proteger la información que reside en los dispositivos tecnológicos, reduciendo el robo de identidad y prevenir ataques de entes maliciosos [40]

Con los continuos Ciberataques que se han presentado en los últimos meses y años [41], es fundamental que las personas entiendan y aprendan las formas de prevenir estos ataques. Conociendo como opera un Ciberataque se pueden generan los pasos para proteger la información, tomándose también como medidas para reducir la posibilidad de que se vuelva a producir otro ataque.

Es una clave para aumentar la seguridad en un sistema también [40] [41].

Un Ciberataque puede iniciar desde un computador a otro a un sitio web, comprometiendo a su paso la integridad, confidencialidad y disponibilidad de la información que allí reside. Un Ciber ataque puede considerarse como un Ciber crimen [40]

Un Ciber ataque tiene tres factores diferentes, los cuales según. [40] Son;

- Ataque o realizar un evento ilegal
- Ganar algo
- Curiosidad

De igual forma es necesario, conocer los tipos de un Ciberataque o Cibercrimen, con suficiente altruismo para lograr identificar a un Ciberdelincuente [41].

A continuación se relaciona las causas de un Ciberataque y su porcentaje de ocurrencia de acuerdo a [42] , los cuales son:

- Phishing e ingeniería social, esta causa ocupa el 61%.
- Malware 45%
- Spear-phishing attack 37%
- Negociación del servicio 24%
- Software desactualizado. 21%

En la siguiente gráfica, se puede observar las causas comentadas anteriormente, centralizadas en un estudio y marco referencial del 100%, donde cada causa se ordenó de manera que su total del marco referencial propuesto, y de esta manera determinar por lo menos de cada 100 ciberataques el porcentaje total de cada causa.

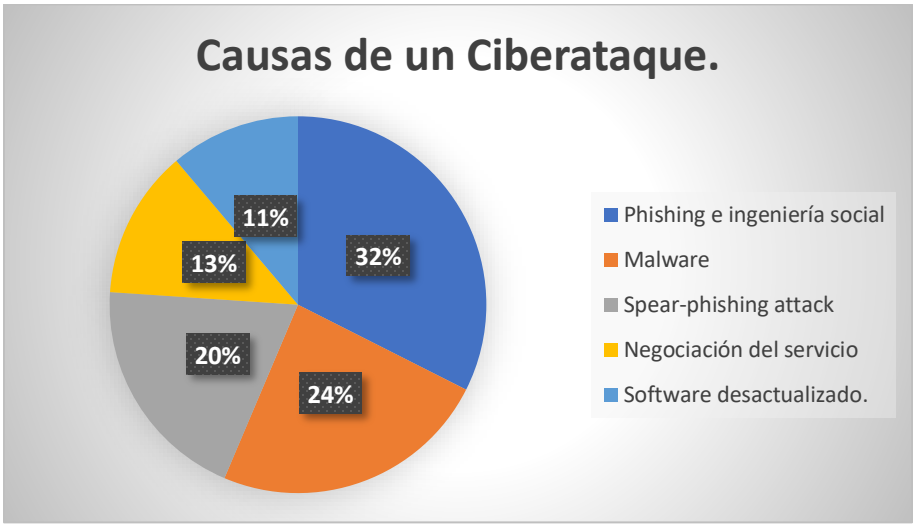

Ilustración 9 - Causas de Ciberataques, Fuente [42]

En la imagen anterior, se destaca, por ejemplo, que de un 100%, el ciberataque que más se presenta es Phishing e ingeniería social con un total de 32%, seguido de malware o mejor conocido como "virus" con el 24%. Estos estudios y resultados son fundamentales a la hora de determinar estrategias de Ciber seguridad para su prevención y corrección.

Dada la rápida evolución de las amenazas a los sistemas cibernéticos, se necesitan nuevos enfoques de gestión que aborden el riesgo en todos los dominios interdependientes (es decir, físicos, de información, cognitivos y sociales) de los sistemas cibernéticos [43].

Adicional, la incertidumbre extrema y la rápida evolución de las amenazas cibernéticas dejan los esfuerzos de evaluación de riesgos incapaz de abordar adecuadamente los argumentos y preocupaciones de Ciber seguridad para los sistemas cibernéticos críticos [43]. Por esta razón, el enfoque tradicional del endurecimiento de los sistemas cibernéticos contra amenazas identificadas ha demostrado ser imposible.

La única verdadera defensa que los profesionales de la Ciber seguridad podrían tomar para endurecer los sistemas de la multitud de amenazas cibernéticas potenciales incluiría la desautorización de los sistemas cibernéticos de acceder a Internet [43].

Definiendo un sistema, como una colección de unidades que trabajan colectivamente hacia un objetivo común [44]

Es por ese motivo que, de la misma manera que los sistemas biológicos desarrollan inmunidad como una forma de responder a las infecciones y otros ataques, también los sistemas cibernéticos deben adaptarse a las amenazas siempre cambiantes que siguen atacando las funciones vitales del sistema, y para recuperarse de los efectos de los ataques.
Una vez, revisado los factores por los cuales se puede ocasionar un Ciber ataque, se debe indagar sobre los tipos de personas que existen, como Ciber delincuentes. Conforme indica [41], existen dos tipos, los cuales se describen de la siguiente forma:

Los primeros son expertos en cometer crímenes, incluyendo Ciber crímenes [41]

Los segundos conocen las vulnerabilidades en un sistema determinado, ya puede ser como una organización o empresa y lo hacen para tener ventajas o beneficios. Este grupo puede conformarse por empleado o ex empleados de la misma compañía.

De acuerdo a [37], el Ciber crimen está compuesto en su gran medida por desarrolladores e investigadores. Los mismos suelen ser responsables por crear o innovar en nuevos métodos para entrar sin el permiso necesario a en dominios de sistemas de datos o explotar vulnerabilidades de seguridad, de igual forma consiguen tomar ventaja mediante métodos como ingeniería social para infectar sistemas a través de trucos, Ocultar información y resistir.

De la misma manera, se puede encontrar a estudiantes con conocimientos básicos para comenzar a probar y con una mejor actitud en dirección a la noción específica que quieren explotar, probando en la generación de malware en relación a compañía.

Se puede observar que hay páginas web dedicadas a explicar cómo crear y desarrollar un virus, o como hacker un sistema de acuerdo a ciertos parámetros que ellos mismos explican y si contenido es en su mayoría gratis y accesible para todo el mundo.

En muchos casos las investigaciones exageran con la amenaza del impacto del daño que causa y en otros casos no determinan de forma acertada el riesgo real que implica el uso de las tecnologías de la información. Siendo que el Ciber crimen representa el 15% de actos ilegales cometidos en empresas solo en Colombia [37].

De acuerdo con [37], existen una serie de Ciber crímenes en los cuales se debe tener especial cuidado para no llegar hacer una víctima del mismo, a continuación, se describen algunos:

- ✓ Delitos contra la confidencialidad, integridad y Disponibilidad de datos y sistemas informáticos.
  - Acceso ilícito a los sistemas informáticos
  - Interceptación ilegal de datos informáticos
  - Interferencia en el funcionamiento de un sistema
  - Abuso de dispositivos que faciliten la comisión de delitos

- ✓ Crímenes informáticos
  - Falsificación informática a través de introducción, alteración o eliminación de datos informáticos o interferencia en los sistemas informáticos
  - Fraude informático a través de la introducción, alteración o eliminación de datos informáticos o interferencia en los sistemas informáticos.
  - Borrado de datos fraudulentos o corrupción de archivos.

- ✓ Delitos relacionados con el contenido.

  - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

- ✓ Delitos relacionados con infracciones de propiedad intelectual y derechos afines:

  - En este grupo de delitos está la copia y distribución de programas informáticos, o hacking.

TIPOS DE DELITOS INFORMATICOS

Los delitos informáticos son aquellas actividades en las cuales un sujeto activo lesiona física y psicológicamente a otro sujeto por medio de la utilización indebida de medio informáticos [45], dicha lesión, está relacionada con el daño o intromisión no autorizada en equipos electrónicos ajenos, violando la intimidad de sus propietarios.

A continuación, se describe, algunos de los más utilizados delitos informáticos, tanto en Colombia como en el resto del mundo.

- ➢ *PHISHING*

Este es un método en donde los Ciber delincuente usan para engañar a las personas y que revelen información personas como cuentas bancarias, contraseñas etc. [41]

Esto lo puede ejecutar mediante mensajes de texto en el celular, páginas web que simulan ser un banco, publicidad que aparece en la ventana, correos etc. La persona que diligencia todo el formulario sin darse cuenta de que pueden estar cometiendo cayendo en una trampa al brindar toda su información.

Esta modalidad no podría llegar a ser eliminada del todo, es muy extensa sin embargo lo que se puede ayudar en previniendo, como por ejemplo no respondiendo los mensajes de texto o links que llegan por correo o por el celular, tampoco brindando ningún tipo de información. Como protección se recomienda cambiar periódicamente las claves además de validar de forma correcta las URL's del sitio donde van a ingresar [41].

- *SKIMMING*

Esta modalidad permite clonar las tarjetas de crédito o débito. Consiste en duplicar una carta en otro con la misma información obtenida de la tarjeta que están clonando.

Los delincuentes pueden adaptar partes donde ellos configuran los sensores para capturar la información de las tiras magnéticas en un cajero además de poner cámaras donde toman la cuenta de los titulares de la cuenta y horas más tarde eliminan estos objetos y extraen la información para hacer la clonación respectiva [41].

- *RANSOMWARE*

De acuerdo con [41] es un software con el que los Ciber delincuentes infectan computadoras. Tiene la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar los archivos mediante la eliminación del control de toda la información, y luego solicitar el pago de un rescate, dicho pago se realiza a través de una moneda virtual.

- *LA INGENIERÍA SOCIAL*

La ingeniería social es el fragmento central del componente humano de la Ciber Seguridad, definiéndose en cómo obtener un acceso no autorizado a redes informáticas mediante el uso de trucos psicológicos, engaños o manipulación [46].

El verdadero secreto de un ataque exitoso mediante las técnicas de la ingeniería social es que logran recopilar información sin levantar ninguna sospecha de lo que en realidad se está haciendo, [47].
Los empleados de las organizaciones son los objetivos de las tácticas de ingeniería social porque son la parte más vulnerable del entorno de Ciber Seguridad y son mucho más fáciles y requieren menos tiempo para los piratas informáticos que intentar la intrusión a través de un plan de prevención de infracciones que tiene una organización [46].

Se logra especificar y describir 4 ataques en relación de la ingeniería social [46], los cuales son:
Físicos: Los atacantes pudieran tener un acceso “físico" a la información de una organización, como por ejemplos, notas post-it con información escrita, como contraseñas o papel en la basura.

- **Sociales**: Podría ser un evento donde un individuo llama a un empleado dentro de la organización con fines inescrupulosos, como que ha pasado algo dentro de la organización y él puede ayudar, solicitando data como usuarios y password.

- **Técnicos**: En este ítem podría utilizarse la información que hay contenida en una red social, y ya sea perfil o imágenes etc. y utilice esto para pedir información y manipular a un empleado con el fin de que le proporciones data para el acceso a dicha red.

- **Socio-técnicos**: Precisa de una combinación entre el enfoque social y técnico. Incluyendo el phishing. Un ejemplo podría ser el cebo. El hostigamiento ocurre cuando un atacante deja un medio que contiene malware, como una unidad flash USB, cerca o en un edificio de oficinas con la intención de que la persona que encuentre el medio lo coloque en una computadora de la oficina.

Se ha realizado una investigación mínima que examina la relación entre los factores de personalidad y los comportamientos de Ciber Seguridad.

No obstante, algunas investigaciones realizadas hasta ahora, como [46] [47]. Los cuales han logrado entre otras cosas, determinar ciertos puntos en el comportamiento de seguridad de la información.

De igual forma, se ha podido conocer y establecer que cada ataque ocasionado en relación a un Ciber ataque e ingeniería social son diferentes, sin embargo, como menciona [47], existe un patrón común para cualquier ataque de ingeniería social, que genera como un ciclo que incluye por lo menos 4 fases, las cuales se describe a continuación;

Ilustración 10 - Ciclo de vida de un ataque de ingeniería social. Fuente: [47]

- La primera fase consiste en que el atacante reúne la información acerca del objetivo y el entorno.

- Luego de reunir suficiente información del objetivo, se mueve a la segunda fase donde el atacante intentara desarrollar la confianza del individuo. Maneja la manipulación.
- Una vez obtenida la confianza, ingresa a la tercera fase, donde el atacante manipula esa confianza del individuo y comienza con la extracción de información.
- Para la última fase, el atacante crea una salida limpia de tal manera que no queden pruebas y que nada pueda llevar un rastro a su identidad real, completando así el ciclo.

2. CIBER SEGURIDAD.

Temas expuestos en relación a la calidad, seguridad y metodologías que anteriormente se exponen, requieren de generar nuevas tecnologías y efectuar tendencias de gran impacto en los últimos años para su correcta implementación.

Dentro de las mismas tendencias, una muy nombrada en Colombia es la tecnología de la información (IT por sus siglas en ingles), la cual ha tenido una gran marca en la última década y se ha podido visualizar en como las organizaciones realizan sus negocios en pro de su aplicación e inclusive como los analistas y colaboradores pueden realizar de manera más eficiente y eficaz su trabajo [46].

Por otra parte, es de común panorama, ver la interconexión que se ha reflejado durante también los últimos años, entre humanos y dispositivos informáticos. Por ejemplo, en 2011, por primera vez, la cantidad de dispositivos conectados a Internet superó a la población de la Tierra, y se espera que esa cantidad (7 mil millones) se triplique para el año 2020, con analistas que proyectan que 24 mil millones de dispositivos conectados a Internet serán en uso [46].

La variedad de dispositivos que se han conectado entre sí, varia en la cantidad de tamaños, precios y aún más importante la tecnología principal, es decir, computadores, smartphones, impresoras, la nube, redes privadas virtuales, iPod etc. Tanta variedad ha llevado a facilitar la comunicación y productividad de la civilización actual, brindando a su vez, grandes facilidades en el estudio y trabajo, llegando a dejar actividades laboral remotas, puesto tienen el acceso como si trabajan desde la oficina.

Esta facilidad de conexión laboral y tecnologías de información, ha dado paso a una necesidad de las organizaciones en proteger y conservar la información que manejan desde cualquier punto cardinal de la ciudad, país y el resto del mundo, generando demanda y aumentando el costo del mismo, pues dicha necesidad se basa en la información personal de miles de personas, inversiones, capital e interés de propiedad intelectual etc. que ha dado paso a la Ciber resiliencia.

Esta última se basa en el análisis que la persona identifique en determinado momento y las formas para poder atacar esta amenaza, de acuerdo a las vulnerabilidades que halle y su conocimiento [48].

El riesgo en sí y el análisis de riesgo son uno de los temas populares en comunidades de científicos, ingenieros y políticos, entre otros. Debido a los múltiples significados que Riesgo puede representar en las diferentes áreas de por ejemplo economía, política, negocios e informática. De igual forma la evaluación de riesgos ha estado madurante a través de los últimos años con el objetivo de analizar la probabilidad de daño del sistema después de perturbaciones [49].

No obstante, para el proyecto en cuestión, se basará en Riesgo en relación a sistemas informáticos y desarrollo de software seguro orientado a la web, pudiendo identificar los diferentes riesgos y su procedente evaluación que se puedan presentar durante el desarrollo

de la misma. Basándose en este caso, en la seguridad informática que se puede brindar y generar para evitar precisamente los riesgos y amenazas que se presenten.

La ciber seguridad efectiva reduce el riesgo de un ciberataque y protege a las organizaciones de la explotación deliberada de sus activos [42].

La evaluación de riesgos está basada en el peligro y la vulnerabilidad que exista sobre el sistema u objeto, Este riesgo puede presentarse a nivel de software y hardware [49]. A continuación, se presenta un marco conceptual acerca del riesgo, dicho marco está construido desde lo general, de tal manera;

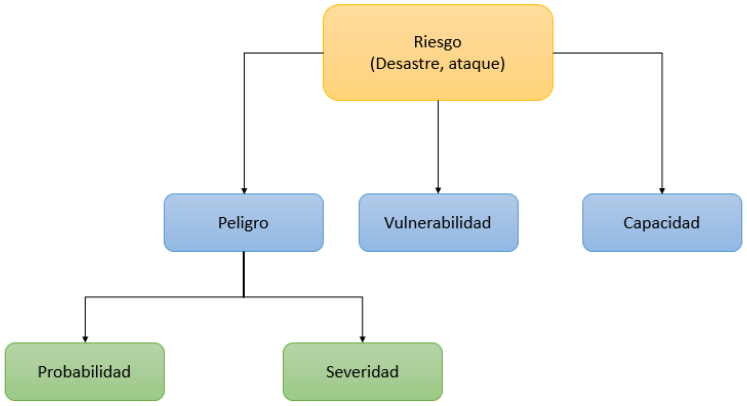

Ilustración 11 - Marco conceptual del riesgo. Fuente: [49]

Como se muestra en la ilustración anterior, el daño de un sistema tiene como consecuencia 4 diferentes parámetros, [49] entre ellos esta:

- Probabilidad del evento
- Severidad del evento
- Vulnerabilidad del sistema
- Capacidad del sistema al absorber del evento

Entender la naturaleza de un riesgo y sus consecuencias en un punto que es parte del todo en el procedimiento de evaluación de riesgos, es tan importante, que se debe tomar como el primer paso para la misma. La última meta es construir un sistema poderoso que pueda resistente y ágil ante los riesgos. Modernos sistemas necesitan adoptar mecanismos para hacer frente a los riesgos y recuperarse rápidamente [49].

El éxito de un Ciber ataque se fundamenta en la capacidad de explorar y explotar los hallazgos encontrados en un sistema cibernético, donde la complejidad puede ir aumentando, y a la velocidad con la que se ha trabajado este campo en los últimos años se podría indicar que la complejidad de realizar un ataque aumenta anualmente, e inclusive mensualmente [48].

Dicho crecimiento ha llevado a un cuantioso grupo a expandir y estudiar las vulnerabilidades cibernéticas incluyendo la piratería. Donde, gran parte de este estudio y en el área de ingeniería, describen que los humanos que analizan o estudian cada sistema para un ataque, se clasifican como un componente importante del sistema cibernético de acuerdo a su función de encontrar y mitigar cada riesgo vulnerabilidad encontrada en cada momento. Mediante las tareas de hallazgo y escalamiento entre humanos y tecnología acceden a una complejidad nueva, debido a la data que se maneja y el tráfico en la red.

ESTRATEGIAS DE CIBER SEGURIDAD.

La Estrategia de Ciber Seguridad Nacional en España, tiene como una de sus líneas de acción, la seguridad y resiliencia de las TIC en el sector privado, y entre sus medidas impulsar el desarrollo de estándares de Ciber Seguridad a través de los organismos y entidades de normalización y certificación nacionales e internacionales, y promover su adopción [50].

En el ámbito internacional la Agencia Europea de Seguridad de las Redes y de la Información, dispone de un inventario de metodologías, métodos y herramientas para la gestión de la Ciber Seguridad y gestión de riesgos.

El inventario de la ENISA contempla diecisiete metodologías, con información detallada de manera homogénea, sobre cada uno de los métodos contemplados. Esta información detalla, entre otras cuestiones el alcance, los niveles de madurez disponibles, el mapeo contra otros estándares, las herramientas disponibles de la metodología, etc.

A continuación, se hace un breve resumen de cada metodología, de acuerdo a [50] [51];

- **ENISA** – SME. Guía de evaluación y gestión del riesgo para Pymes [51].

- **MAGERIT**. "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información". Si se habla Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico [52].

- **OCTAVE**. "Operationally Critical Threat, Asset, and Vulnerability Evaluation" Metodología de Análisis y Gestión de Riesgos desarrollada por el CERT. Está compuesto por una serie de talleres y/o programas que son llevados a cabo por la propia organización, aprovechando de esta manera los conocimientos propios de los niveles de la misma. Este grupo se centra únicamente en establecer los puntos críticos y las posibles amenazas, asimismo las vulnerabilidades tantos físicos como lógicas que atente a la organización y plantear la estrategia a utilizar [53].

- **Mehari**. Método de Gestión y Análisis de Riesgos desarrollado por CLUSIF (Club de la Sécurité de Information François. Mehari propone un módulo para analizar los

intereses implicados por la seguridad y un método de análisis de riesgos con herramientas de apoyo [54].

- **EBIOS**. Metodología francesa de análisis y gestión de riesgos de seguridad de sistemas de información. Es una metodología francesa de análisis y gestión de riesgos de seguridad de sistemas de información que comprende un conjunto de guías y herramientas de código libre, enfocada a gestores del riesgo de TI.

- **CRAMM**. Metodología de análisis y gestión de riesgos desarrollada por el CCTA inglés. Puede definirse como una Metodología para el análisis y gestión de riesgos encaminada a brindar confidencialidad, integridad y disponibilidad de los sistemas de información mediante el uso de una evaluación mixta.

- **NIST SP 800-30**. "Guide for conducting risk assessments". Publicada por NIST (National Institute of Standards and Technology) de EEUU. Es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información; sin embargo, esto no es suficiente, pues se necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito.

- **Citicus One**. Software comercial de Citicus, implementa el método FIRM del Foro de Seguridad de la Información. Adicional, brinda un enfoque probado y galardonado para administrar el riesgo de la información, el riesgo del proveedor y otras áreas clave de riesgo operacional en toda una organización [55].

- **ENISA**. Inventario de metodologías y herramientas de análisis y gestión de riesgos de ENISA (European Network and Information Security Agency). Incluye sistema de comparativas. ENISA contribuye a asegurar la sociedad de la información de Europa mediante la sensibilización y el desarrollo y la promoción de una cultura de redes y

seguridad de la información en la sociedad, contribuyendo así al correcto funcionamiento del mercado interior.

- **GxSGSI**. Software de análisis de riesgos, en español, de la empresa SIGEA. Es una solución completa de gestión del análisis de riesgos, que permite la identificación y valoración de las amenazas, vulnerabilidades, e impactos; el cálculo del riesgo intrínseco y residual; la adopción de las contramedidas y los controles, necesarios para la certificación de un Sistema de Gestión de Seguridad de la Información, bajo las normas ISO 27001 e ISO 27002.

- **ISO 27005**. Estándar ISO de la serie 27000 dedicado a la gestión de riesgos de seguridad de la información.

- **UNE-ISO 31000**. Estándar ISO dedicado a la gestión de riesgos, en español. Al proporcionar principios integrales y directivas, esta norma ayuda a las organizaciones con su análisis y evaluación de riesgos. Sea que trabaje en una empresa pública, privada o comunitaria, se puede beneficiar de BS ISO 31000, porque se aplica a la mayoría de las actividades comerciales, incluyendo la planeación, operaciones de gestión y procesos de comunicación [56].

- **BS 7799-3:2006**. Estándar británico de gestión del riesgo de la seguridad de la información de British Standards Institution. Guía para la gestión de riesgos de seguridad de la información. Dicha norma fue definida para soportar la planeación e implementación de Sistemas de Gestión de Seguridad de la Información basados en el estándar ISO/IEC 27001:200551. Consta de los siguientes procesos para el análisis de riesgos: Análisis, evaluación, tratamiento y decisiones de riesgos [57].

- **IRAM**. Information Risk Analysis Methodologies es una metodología de análisis de riesgos del Information Security Forum sólo disponible para sus miembros. IRAM

estudia y publica normas argentinas en todos los campos de actividad, que favorecen y facilitan el desarrollo económico y social, lo cual contribuye a mejorar la calidad de vida y el uso racional de los recursos [58].

- **@RISK**. De Palisade, es un software general de análisis de riesgos basado en la simulación de Monte Carlo. Existe versión en español y tiene coste.
- **COBRA**. Consultative, Objective and Bi-functional Risk Analysis es un software -no gratuito- de evaluación del riesgo de "C&A Systems Security Ltd." Es una metodología que consiste en una serie de análisis de riesgos para consulta y herramientas de revisión de seguridad [59].

- **RiskWatch.** Software no gratuito de realización de análisis de riesgos. Esta herramienta realiza análisis automatizados de riesgos y evaluaciones de vulnerabilidad de los sistemas de información. Las bases de datos de conocimiento que se proporcionan junto con el producto son completamente personalizables por el usuario, incluida la capacidad de crear nuevas categorías de activos, categorías de amenazas, categorías de vulnerabilidad, salvaguardas, categorías de preguntas y conjuntos de preguntas [60]

Tomando como base la definición de continuidad de negocio, el mismo hace referencia al desarrollo de sistemas, combinados con una dependencia estrecha de las organizaciones y su continua utilización, con el objetivo de hacer relevante la gestión de continuidad del negocio, para minimizar la probabilidad y magnitud de las posibles interrupciones del negocio [61], entre ellas riesgos y amenazas, para no improvisar, sino definir las acciones y roles concretos en caso que sucede algún evento [62].

La fase donde se requiere debería desarrollarse un plan de continuidad del negocio, debería ser la de “iniciación y gestión de proyecto”. Con el objetivo de agregar y establecer todas las áreas que estarán involucradas en el plan, su rol en caso de, e información necesaria [61].

Dentro del plan de trabajo para la continuidad del negocio, se deber tener en cuenta aspectos como la contingencia. El último está relacionado como los procesos a ejecutar en caso que sucede algo, para este caso en el negocio. Se podría relacionar la contingencia con un plan también y definiéndolo como una estrategia planificada con una serie de procedimientos que facilitan u orientan a tener una solución alternativa, con el objetivo de restituir rápidamente los servicios en una organización ante la probabilidad de que todo se detenga o cambie, de forma parcial o total.

El plan de contingencia es una herramienta que le ayudará a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando, aunque sea al mínimo [63].

Una vez definida y estructurado el plan de continuidad y negocio, se presenta a continuación algunos estándares y normas que se han contemplado para la continuidad del negocio en caso que suceda algo.

Ilustración 12 - Estándares Revisados, Fuente: [50].

A continuación, se describe y analiza brevemente cada estándar, de la imagen anteriormente presentada y su relación con el plan de continuidad del negocio.

- **SP 800-30 Rev**, de septiembre 2012, desarrollada en Estados Unidos por el NIST; En reemplazo del estándar SP 800-30 de Julio de 2002, su propósito es orientar en la realización de evaluaciones de riesgos de los sistemas y organizaciones de información, ampliando la orientación en la publicación [64].

- **Octave Allegro**, de mayo 2007, desarrollada en Estados Unidos por el SEI (Software Engineering Institute) e implementado en el CERT- Carnegie Mellon University. Su función principal es optimizar y agilizar procesos de evaluación de riesgos de seguridad de la información. Basándose en los activos, que para ellos es la información [65]

- **ISO/IEC 27001:2013**, de octubre de 2013, desarrollada por el organismo internacional ISO IEC. Familia de estándares, con su versión más reciente del 2017,

con el objetivo de ayudar a una organización a administrar la seguridad de sus activos, como información financiera, propiedad intelectual, detalles de empleados o información a terceros [66].

- **CRAMM Versión 5,** de 2003, desarrollada por el gobierno del Reino Unido, comercializada por Insight Consulting y revisada por el SANS Institute. es un método de análisis de riesgos. El método CRAMM es bastante difícil de usar sin la herramienta CRAMM. En la actualidad, CRAMM es el método de análisis de riesgo preferido del gobierno del Reino Unido, pero CRAMM también se utiliza en muchos países fuera del Reino Unido. CRAMM es especialmente apropiado para grandes organizaciones, como organismos gubernamentales e industria [67].

- **Magerit V3**, de octubre de 2012, elaborada en España por el CSAE, y adoptada por el Esquema Nacional de Seguridad (ENS). Metodología de análisis y gestión de riesgos de los sistemas de información, consolidándose desde 1997 hasta la fecha como un paso necesario para la gestión de la seguridad [68].

- **SANS Critical Security Controls Versión 5**, de 2013, coordinados por el SANS Institute. proporciona una serie de recursos y cursos de seguridad de la información [69].

- **ISO 27032 de 2012,** desarrollada por el organismo internacional ISO IEC. Permite enfocarse en la seguridad del Ciberespacio adicionando este factor al sistema de Gestión de Seguridad de la Información. Adicional, aporta un marco metodológico y de buenas prácticas en la implementación de la Ciberseguridad en las empresas, complementando al ISO 27001 en el aporte de nuevos controles relacionados al Ciberespacio [70].

- **UNE/ISO 22301 de diciembre de 2013**, desarrollada por el organismo internacional ISO IEC, y traducida por AENOR. Única referencia global para los sistemas de gestión de la continuidad del negocio, buscar ser reemplazada este año (2019) con una nueva versión. La actualización no incluiría cambios dramáticos, pero si es una mejora que producirá mayor valor. Menos definiciones, más flexibilidad, más pragmatismo; secciones redundantes se han reducido; las definiciones se han vuelto más consistentes y el texto se presenta más lógico [71].

Una vez identificados algunos estándares se logra comprender algo importante, en muchas instancias los estándares y estrategias de la Ciber seguridad están escritas y publicadas en el idioma de inglés. Incluso en países donde el inglés no es su idioma nativo como Republica checa, Holanda, Finlandia, Estonia, Francia, Alemania, Turquía y España etc. [29]

3. CIBER RESILIENCIA.

En los últimos años, se han integrado sensores avanzados, automatizaciones inteligentes, redes de comunicación y tecnologías de la información (TI) entre otros, para mejorar el rendimiento y eficiencia de los diferentes sistemas. La integración de estas nuevas tecnologías ha dado lugar a más interconexiones e interdependencias entre software y hardware [49].

Mientras los progresos en la tecnología de la información y conectividad avanzan y se desarrolla cada día, mejorando tiempos de respuesta y eficiente para contribuir sistemas expertos basados en las diferentes estructuras y algoritmos creados por ingenieros, científicos y personas especializadas en el tema también [49]. A su vez se genera grandes riesgos en relación a los sistemas.

El hecho de poder identificar el impacto y probabilidad que estos sistemas pueden generar al interrumpir su programación o procedimiento y relacionarlo o introducir un Ciber ataque es de gran importancia e interés para el consumidor o en su defecto debería de serlo ya que debido a que gran escala de afectación se deben tomar medidas que aseguren los procedimientos, control y monitoreo de dichos sistemas con el objetivo principal y final de prevenir algún ataque o perdida de información que lo afecte o, a la final que resiste ante dicho Ciber ataque y que de igual forma cree y genere un forma de resistir ante el mismo, guardando en su memoria la forma en que pudo ser atacado, como se defendió y cuales medidas tomo a partir de ese incidente. **Error! Reference source not found.**

El concepto de Ciber resiliencia de un sistema de energía se centra en mantener los estados del sistema en un nivel estable en presencia de perturbaciones

Es un enfoque de extremo a extremo que reúne tres áreas críticas:

- La seguridad de la información
- La continuidad del negocio
- La capacidad de recuperación de las redes de las empresas

Para garantizar que las organizaciones sigan funcionando durante los ciberataques [42].

A continuación se anexa un estudio global, donde muestran cuánto tiempo puede tolerar los negocios, compañías o proyectos a la hora de recibir un ataque:

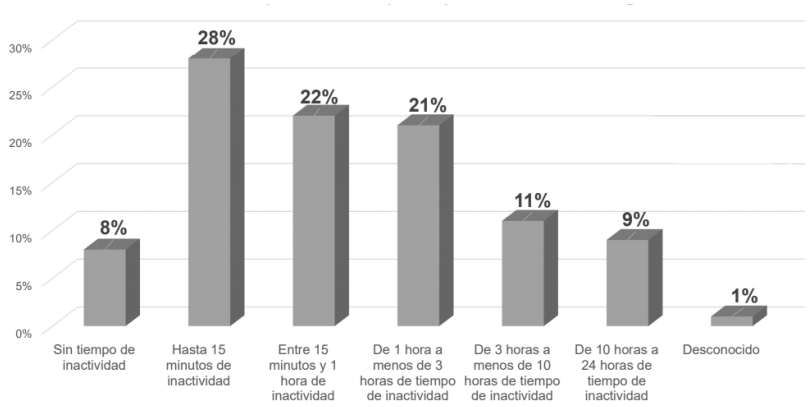

Ilustración 13 - ¿Cuánto tiempo de interrupción puede tolerar un negocio? Fuente: [42]

Como se ha podido observar en la gráfica anterior, un porcentaje de 28% para 15 minutos de inactividad en caso de que algo se genere y el sistema no responda, es un espacio muy amplio para acceder, robar y vulnerar miles de datos guardados, el margen de tolerancia debería ser menor, esto debido a la cantidad de metodologías que se podrían aplicar para evitar el riesgo, sin embargo en muchos casos no logra ser suficiente, no obstante han habido casos donde los accidentes o brechas de inseguridad han sido generado sin intenciones maliciosas del empleado, tomando este punto como sin el conocimiento adecuado también existe un riesgo. En muchos casos no se puede controlar algo que lleva planeado y estudiado por los diferentes métodos de robo de información que existen.

El número de vulnerabilidades de software está creciendo en órdenes de magnitud. Cerca de 15,000 nuevas vulnerabilidades fueron descubiertas en 2017, un 128% más que el año anterior [16].

De estos, más de la mitad (56%) fueron causados por códigos de programa inapropiados como la ejecución de código arbitrario, desbordamiento de búfer, inyección SQL e inclusión de archivos.

Los modelos que realiza o ejecuta dichos sistemas basados en la lógica programable pueden ser explotados por Ciber ataques. Estas amenazas han generado estrategias en la industria de dichos sistemas los cuales emplean técnicas de defensa activa para reducir o eliminar las causas que generen se activen canales o sistemas de ataque expertos desde afuera o adentro de la empresa.

Por consiguiente, es necesario entrar y revisar cada aspecto que integra la Ciber resiliencia en el marco que se trabaja, incluyendo lo más sencillo y que se maneja todos los días como son los Ciber ataques.

Se tiene identificado de acuerdo a un reciente estudio [42], que sucede un Ciber ataque cada 20 minutos y este puede llegar a costar millones para la compañía, hasta US $1 millón.

De acuerdo a [72] en su publicación relacionan los conceptos básicos que se deben entender para poder conocer y saber cómo tratar por ejemplo la Ciber resiliencia, no obstante en el artículo, señalan los complejos sistemas que se están desarrollando en la actualidad, desde maquinas complejas que hacen el trabajo de los humanos hasta sistemas de internet y navegación donde reside y se trabaja una cantidad de información exuberante, trabajando también con bases de datos y otras tecnologías para su “facilidad” sin embargo la grandeza de este sistema expone y crea también pequeñas brechas de riesgos.

Las organizaciones que desarrollan este tipo de sistemas, tienen la probabilidad de quedar bajo un Ciber ataque, generando no solo interrupción en sus operaciones sino también la perdida de información tanto de la empresa como de sus clientes ocasionando que el riesgo y el impacto sea mayor tanto económico el prestigio de la organización.

La información expuesta anteriormente se basa en los múltiples estudios y análisis que se han realizado como los descritos anteriormente en [16] y [72], donde se ha podido demostrar que estos riesgos que sean vuelto peligros en las organizaciones generando un costo anual de 550 mil millones de dólares a partir de los riesgos que no fueron evitados o tratados [72]. Poniendo a prueba no solo los sistemas que desarrollan sino toda la compañía en la manera como se maneja, puesto que existen muchos intereses personales en el medio.

Son muchas las técnicas y estrategias que se utilizan hoy por hoy para revenir y contrarrestar eventos que puedan generar algún riesgo o peligro para el sistema u organización que se trabaja, adicional de los simuladores expuestos anteriormente existe una "técnica" conocida con el nombre de Ciber-resiliencia que se ha venido utilizando los últimos años y que es necesario definirlo, exponerlo y argumentarlo para su compresión.

De acuerdo al departamento de ciencias de la computación de Estocolmo en su artículo *Cyber Resilience – Fundamentals for a Definition*. Infieren que la Ciber-resiliencia es "la habilidad de continuar por un resultado deseado a pesar de los eventos cibernéticos que se presentan" **Error! Reference source not found.**. Está definición se centrará en la explicación que se brinda para ciertas características, de las cuales permite describir y justificar no solo su definición sino la justificación de esta herramienta.

La Ciber resiliencia de acuerdo a**Error! Reference source not found.**, indica en sus texto que la ciber resiliencia podría considerarse como una investigación académica que aún está en su etapa más prematura, orientada en ciertos temas a académicos, por lo cual para temas de investigación y educación suele ser más eficiente y efectivo, no obstante, para negocios, compañías y sociedad se necesita tener más eficiencia y efectividad.

La definición determinada inicialmente, se puede considerar como un conjunto de varios niveles, donde cada nivel, el mismo contiene retos, métodos y controles concebibles en relación a la resistencia cibernética. Por lo tanto, para la parte de "la habilidad de continuar por un resultado" **Error! Reference source not found. Error! Reference source not found.** puede pertenecer desde empresas y negocios individuales o sistemas de tecnología

específicos sin embargo dicho sistemas deben abordarse temas integrales y que incluyan varios niveles de revisión.

A continuación, se presenta los niveles de la Ciber resiliencia.

Level	Description	Example
Supranational	CR for a confederation of nations	European Union
National	CR for a country or society	Sweden
Regional	CR for a region or city	Stockholm
Organizational	CR for an organization	Company, agency, council
Functional	CR for a business function	Division, process, capability
Technical	CR for a technical system	IT system, network

*Ilustración 14 - Diferentes niveles de la Ciber resiliencia, fuente****Error! Reference source not found.***

A continuación, se explicará brevemente como se determina la definición brindada por el grupo de expertos del departamento de ciencias de Estocolmo [73], en los cuales se define los siguientes:

- La noción de "continuar" palabra relacionada con la definición brindada previamente. En esta noción refiere a la capacidad de entregar u resultado aun cuando la operación presenta algún tipo de falla o incidente, y que el mismo este bajo las políticas de calidad establecidas en la organización, un ejemplo de esto podría ser un domicilio, en el cual un evento inesperado es la lluvia y sin embargo la entrega de la comida bajo la lluvia está garantizada. Esta noción también incluye la restauración de los mecanismos de entrega regulares después de los eventos que se presenten, y como idea principal esta cambiar o modificar de acuerdo a os eventos que se presenten es decir evitar que un evento se vuelva a presentar por el mismo riesgo.

- El resultado, está relacionado con la unidad de análisis (organización o sistema) que se utilizar para poder alcanzar o cumplir una meta mediante un proceso o servicio que presta la entidad.

- Para la última parte, a pesar de los eventos cibernéticos presentados puede ser utilizado para las diferentes acciones que realiza el hombre, generando impactos negativos en:
  - ✓ Disponibilidad
  - ✓ Integridad
  - ✓ Confidencialidad.

La definición citada en los párrafos anteriores es solo una de las tantas definiciones que tiene una de las técnicas más mencionadas en la actualidad como lo es la Ciber resiliencia.

Por ejemplo [43] en su texto, define la Ciber resiliencia puede referirse también a "*la capacidad del sistema para preparar, absorber, recuperarse y adaptarse a los efectos adversos, especialmente los asociados con los ciberataques."* Siendo de alguna forma similar a la definición anterior de **Error! Reference source not found.** (*la habilidad de continuar por un resultado deseado a pesar de los eventos cibernéticos que se presentan*), esto se debe a los múltiples usos y adaptabilidad que las personas pueden utilizar para poder implementar esta técnica dentro de sus sistemas y organizaciones.

Las características de la Ciber resiliencia se puedan agrupar en 5 sub-definiciones en dirección del conocimiento y entendimiento para lograr identificar la metodología objetiva. Conforme [74] en su informe de *Cyber-Resilience: Creating an Agenda for Future Research* dichas características se logran ver reflejadas en lo que ellos llaman "fases" las cuales se exponen de la siguiente manera, conforme [74].

- **Planificación**: Consiste en enfocarse en la definición de la pregunta guía, la cual debería siempre ser ¿La Ciber resiliencia incorpora en su data temas en relación al riesgo cibernético?

- **Investigación**: Esta fase consiste en identificar la información relevante en bases de datos donde la investigación fue realizada. Las palabras claves son importantes en esta fase y la información apropiada que arroja el documento en relación a los resultados que se incluyen en la investigación. El conocimiento que se encuentre y se adquiera será muy importante dentro del margen de la investigación por eso se requiere utilizar bases de datos educativas, académicas y científicas. El dominio de este conocimiento adquirido en relación a la Ciber resiliencia permitirá la tripleta del conocimiento, como se muestra en la siguiente imagen.

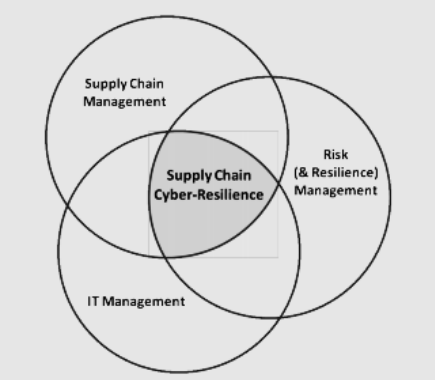

Ilustración 15- Principales dominios de conocimiento en la gestión del riesgo cibernético, Fuente: [74]

- **Selección**: Una vez realizada la búsqueda de la diferente documentación relacionada al tema, se procede a analizar los títulos y resúmenes de los documentos. Luego, más adelante el contenido de los volúmenes debe ser leído, incluido el contenido extendido entre otros.

- **Extracción y síntesis**: Los documentos analizados y sintetizados que fueron utilizados para la documentación utilizando un formato, podría ser una hoja de cálculo que permita categorizar los documentos de acuerdo a la metodología investigada, contexto etc.

- **Reporte**: Se realiza un documento con los resultados encontrados en la información leída.

Una vez analizada la situación sobre cómo están ciertas organizaciones y cómo se trabaja en gran medida la resiliencia, se han realizado diferentes estudios e investigaciones importantes que no se pueden dejar pasar tan fácilmente para este tema, entre ellos, se tiene por ejemplo que el 68% de las organizaciones no tienen la capacidad de mantenerse resistente a raíz de un Ciber ataque. El 66% puede sufrir un Ciber ataque por una mala planificación o preparación insuficiente ante dicho riesgo, 75% tiene planes de respuesta para un Ciber ataque pero son inconsistentes, con niveles de información y solvencia flojos o incoherentes y por ultimo son alrededor de 191 días, en tiempo promedio que ocupan los hackers en los entorno de TI antes del ataque, descubrimiento o éxito de extracción de información [42].

CONTINUIDAD DEL NEGOCIO.

La continuidad del negocio proporciona la capacidad de reanudar las operaciones cuando un evento causa una interrupción del servicio. Los planes para la continuidad del negocio abordan catástrofes naturales, accidentes y ataques físicos deliberados; pero ahora, también deben apoyar la reanudación de las operaciones después de Ciber ataques [42]

Dentro de los procesos de gestión, para implementar protecciones a los diferentes ataques que se puedan materializan con éxito, se requiere de la opción de seguir con la operación con

el objetivo de no generar más afectaciones al negocio, siendo la continuidad del negocio parte de los procesos de protección.

Estas medidas correctivas, planes de continuidad de negocio, de recuperación de desastres y de gestión de crisis, también tienen el propósito de hacer disminuir el riesgo, y son de importancia vital en cualquier organización compleja.

La adecuada gestión del riesgo, la gestión del cambio y la implementación de medidas preventivas y correctivas en toda su extensión, incluyendo planes de continuidad de negocio y de recuperación frente a desastres, forman una parte capital de las herramientas para aumentar la ciber-resiliencia [75].

ORGANIZACIONES MÁS RESILIENTES.

El conjunto de capacidades tales como identificación, detección, cooperación, recuperación y mejora continua en las diferentes organizaciones de cualquier tamaño y sector frente a los distintos riesgos y amenazas, definen su disposición para construir y mantener la resiliencia [76].

Como meta y objetivo para la organización es encontrar las capacidades preventivas de gestión y respuesta para la recuperación, mejora y continuidad.

La Ciber resiliencia no pretende eliminar el riesgo; esto es imposible, pero un nivel de riesgo aceptable permite innovar, crear y desarrollar nuevas ideas [76]. Las organizaciones para lograr Ciber-resiliencia deberán alejarse de una seguridad fragmentada hacia una que sea integrada para toda la organización, que comparta la inteligencia sobre las amenazas y aproveche todos los servicios de seguridad. Establecer estrategias más sólidas y resistentes de forma proactiva, es estar preparado para proteger, detectar y responder a los riesgos y amenazas emergentes.

La resiliencia cibernética debe considerarse en el contexto de sistemas complejos no sólo físico e informativo, sino también dominios cognitivos y sociales **Error! Reference source**

not found.. Cyber Resilience garantiza que la recuperación del sistema se produce considerando los componentes interconectados de hardware, software y detección de infraestructura cibernética.

Por lo tanto, constituye un puente entre el mantenimiento de las operaciones del sistema y, al mismo tiempo, garantizar la ejecución de la misión [43].

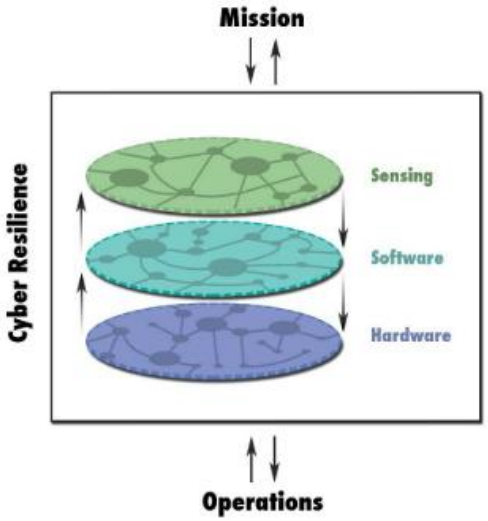

Ilustración 16- Dominios de la Ciber resiliencia comprenden componentes de detección, hardware y software que contribuyen colectivamente a mantener las operaciones del sistema. Fuente: [43]

Centralmente en las organizaciones más resilientes, se logra incluir el documento del consejo nacional de política económica y social (CONPES) 3854 de la república de Colombia, para en este caso hacer referencia al país el cual es perteneciente la institución educativa (Fundación Universitaria Los Libertadores), a cuál ejecuta este documento.

Dentro de los objetivos del CONPES 3854, está el siguiente enunciado, de acuerdo a [77]; "*Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos*"

Este objetivo específico busca desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y defensa para garantizar los fines del Estado. Al mismo tiempo que busca

mejorar la protección, preservar la integridad y la resiliencia de la infraestructura crítica cibernética nacional. Para esto, [77] adelantaría las estrategias que se describen a continuación.

- Fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital

Este plan de fortalecimiento permitirá al sector Defensa generar una autonomía cibernética conducente a identificar, detectar y atender posibles amenazas en contra del Estado y su infraestructura critica. Dicho plan se concentrará en la definición de mejores prácticas y estándares internacionales en los componentes operativos, administrativos, humanos, científicos, de infraestructura física y tecnológica para el CCOC (Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia) y las Unidades Cibernéticas de las Fuerzas Militares.

- Adecuar el marco jurídico para abordar la protección y defensa del entorno digital nacional

Diferentes entidades como el ministerio de defensa nacional, tecnologías de la información y comunicaciones, superintendencia de industria y comercio, además del DNI (Departamento Administrativo Dirección Nacional de Inteligencia) y la UIAF (Unidad de Información y Análisis Financiero de Colombia), se reunieron para adecuar el marco legal y regulatorio para abordar la protección y defensa del entorno digital en Colombia.

Bajo la adecuación del mencionado anterior, se debe buscar que esté acorde con las definiciones internacionales en lo relacionado con la gestión de incidentes, delitos informáticos, ciber crimen, entre otros. La adecuación del marco jurídico deberá buscar, además, el reporte obligatorio de incidentes cibernéticos a la col CERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) por parte de los propietarios u operadores de infraestructuras críticas cibernéticas nacionales y demás partes interesadas, con las previsiones respectivas de confidencialidad, privacidad, entre otros aspectos.

- Generar una estrategia de protección y defensa de la infraestructura crítica cibernética nacional

El Ministerio de Defensa Nacional llevará a cabo la actualización periódica del catálogo de infraestructuras críticas cibernéticas nacionales. A partir de esto, establecerá los contenidos de los planes de protección de la infraestructura crítica cibernética nacional, y los socializará en el marco de la agenda nacional de seguridad digital.

El grado de criticidad de las infraestructuras cibernéticas definido por el catálogo, será el insumo principal para diseñar la estrategia de protección y defensa de la infraestructura crítica cibernética nacional. Característica esencial en lo relacionado con seguridad digital, teniendo en cuenta la evolución permanente de las amenazas en el ciberespacio. En cada actualización se buscará vincular a los sectores y entidades que aún no hayan decidido participar en el catálogo, reiterando la invitación a hacer parte del grupo de trabajo de la primera instancia. Esto permitirá robustecer el catálogo, y, en consecuencia, la estrategia de protección y defensa

- Fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de las múltiples partes interesadas.

Se busca que el coordinador nacional de seguridad digital apoye la creación del objetivo anteriormente nombrado, los cuales permitirán la adecuada gestión de incidentes digitales en los diversos sectores de la economía.

El apoyo consistirá en identificar los sectores que no cuenten con dicho equipo de respuestas, motivarlos a participar de la comunidad CERT de Colombia, y pedirle al CSIRT (Equipos de Respuestas ante Incidentes de Seguridad en español) que considere pertinente que actúe como garante en el proceso de creación de estas instancias, adicional tendrán la capacidad de reacción ante incidentes especializados por sector y con capacidad real de interacción con los diferentes fabricantes, agencias de ley y otras agencias del gobierno como también, definirán prácticas adecuadas de gestión de seguridad en cada sector, asesorarán y acompañarán a las diferentes empresas.

- Fortalecer las capacidades de los responsables de garantizar la defensa nacional en el entorno digital

El Ministerio de Defensa Nacional diseñará contenidos educativos especializados y capacitará a las múltiples partes interesadas responsables de garantizar la defensa nacional en el entorno digital. El desarrollo y fortalecimiento de las capacidades de ciber defensa permiten afrontar las amenazas cibernéticas transnacionales, los desafíos y los retos que imponen los desarrollos tecnológicos y la convergencia de las telecomunicaciones en un mundo más globalizado e interconectado. Así mismo, mediante operaciones cibernéticas, se contribuye al desarrollo de las operaciones militares de tierra, mar, aire y espacio a fin de garantizar la superioridad militar en todo tiempo.

MÉTRICAS.

La Ciber resiliencia, con capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes, es la herramienta necesaria para afrontar cada tarea, y en su configuración se hace necesaria la definición y establecimiento de un marco de medición de indicadores dirigido a medir la capacidad de las organizaciones ante distintos ataques, amenazas o incidentes que puedan sufrir [50].

No obstante, sin importar los ataques que recibieran estos sistemas se deben diseñar para continuar con la disponibilidad y funcionalidad de sus operaciones, aun resistiendo a un Ciber ataque.

Para ese caso y todos los posibles casos que se presenten, se debe contar con algunas cosas claras, uno de ellos, refiere que la Ciber resiliencia es un área muy grande y con mucho trabajo por delante, en el cual, aun los científicos y personas que trabajan en este campo han identificado muchas limitaciones y para comenzar a llevar un resumen y control, han comenzado a utilizar métricas, partiendo del hecho que esta disciplina contiene limitaciones igual de importantes [78].

Se conoce como métrica, a la disciplina encargada de medir o dar a conocer e inclusive estimar tamaños o características de un software o sistemas de información, con el objetivo de realizar comparativas o generar una planificación de proyecto de desarrollo. De acuerdo a [79].

Una vez identificada la definición de métricas, se debe proceder a identificar las posibles formas de medir la información o data en un sistema Ciber resiliente, no obstante, para poder identificar dichas medidas se requiere que la organización o individuo que desarrollo el sistema tengan claro y presente dos puntos de medida que se requieren, las cuales son:

Adicional, el enfoque que las métricas a utilizar deben de tener para la Ciber resiliencia es importante, por lo cual una de sus funciones ha sido generar una red, la cual toma un conjunto de métricas como base para comenzar a evaluar el sistema, las mismas se han podido recopilar de acuerdo a [80] como las siguientes:

- Métricas multiusos: Apoyan decisiones operativas y de ingeniería
- Métricas aplicables a diferentes capas arquitectónicas: Como por ejemplo bases de conocimiento, comunicaciones, aplicaciones y tecnologías específicas.
- Métricas que reflejan diferentes características: Donde incluyen la puntualidad, capacidad y confianza.
- Métricas multiformes: Cuantitativas, semicuantitativas y cualitativas.

Algunas de las técnicas para las métricas, se encuentran en plantillas que utilizaran de acuerdo a la métrica escogida [80], se resumen en las siguientes;

- Un título, nombre o definición resumida de la métrica.
- Objetivos de resistencia cibernética (Anticipar - A, Resistir - W, Recuperar - R y / o Evolucionar - E); una X indica que la métrica puede ayudar a responder preguntas sobre qué tan bien se cumple la meta
- Objetivos de resiliencia cibernética; la métrica puede ayudar a responder preguntas sobre cómo los objetivos identificados se logran.
- Prácticas de resiliencia cibernética; la métrica puede ayudar a responder preguntas sobre la eficacia de la práctica que se aplica.

Las métricas de la Ciber resiliencia comparten una variedad de problemas con las métricas de seguridad [80], incluyendo:

- Uso de términos no especificados, indeterminados o posiblemente indeterminados en las descripciones de las métricas. Tales términos requieren interpretación. Por ejemplo, el momento en que comienza un ataque es indeterminado: lo que constituye un ataque es un asunto de juicio experto, y el inicio real de un ataque puede ser imposible de determinar. Los juicios de expertos pueden diferir, y en la práctica de evaluación de métricas a menudo involucra a no expertos

- Incapacidad para establecer valores objetivo, o incluso para indicar si un valor dado de una métrica es bueno, malo o indiferente. Un uso comúnmente deseado de las métricas de seguridad es la evaluación del cumplimiento (con requisitos o con estándares de buenas prácticas). Sin embargo, la propiedad que motiva la definición métrica puede ser una para la cual los objetivos no se pueden identificar claramente, debido a la falta de un cuerpo común de conocimiento. En ese caso, definir requisitos y evaluar el cumplimiento puede ser un ejercicio de ficción en lugar de ingeniería

Innumerables herramientas y métodos comercializados como evaluaciones de resiliencia existen ahora, pero toman formatos muy diferentes [43]. Algunos métodos son tan simples como una lista de comprobación, sin embargo, otros son visualizaciones geoespaciales de métricas cuantificables, como también existen métodos que utilizan otros métodos para el modelado de red, pero sin forma generalizada, están creados a medida para cada aplicación.

Los resultados de estas herramientas o métodos para métricas cuantificables son similares a los métodos que se utilizan, puesto existe tal variedad que se puede manejan diferentes instrumentos para un efecto exitoso como mapas, puntuaciones y gráficos de tiempo de proceso etc. [43]. Los desarrolladores de las herramientas abarcan una amplia gama de entidades, como, por ejemplo:

- Incluyendo académicos y privados, por ejemplo, consultoría.
- Patrocinadores de programas, por ejemplo, fundaciones y agencias.

- Organizaciones de límites que se unen a través de los reinos de investigación, políticas y profesionales, y los usuarios potenciales Sí mismos.

Los usuarios potenciales incluyen administradores estatales y municipales, administradores de procesos de la industria y operadores de servicios públicos, muchos de los cuales carecen de la experiencia para elegir entre los productos que se acumulan rápidamente en este campo emergente.

Aunque existen niveles diferentes de complejidad en la matemática que se aplica, los desafíos científicos están en abordar los procesos a nivel de sistema y adaptar las metodologías a las necesidades específicas [43]. Se han centrado varios esfuerzos en el desarrollo de métricas aplicables a una variedad de sistemas, incluidos los sociales, ecológicos y técnicos.

Avances en análisis de decisiones y la valoración social y económica de los beneficios ofrecen formas de abordar estos desafíos, con métodos para evaluar el impacto de la negociación de los atributos de resiliencia (por ejemplo, flexibilidad, redundancia) con valores actualmente considerados en el proceso de toma de decisiones (por ejemplo, costo, impacto ambiental, reducción de riesgos) para diversas alternativas de inversión. Una mayor investigación sobre este tema puede beneficiar en gran medida tanto las decisiones de gestión como de inversión para la resiliencia del sistema.

Los enfoques basados en modelos se centran en una representación del mundo real y una definición de resiliencia utilizando conceptos matemáticos o físicos.

El modelado requiere el conocimiento de las funciones críticas de un sistema, misión, los patrones temporales de un sistema, umbrales y memoria y adaptación del sistema [43].

Los modelos de proceso requieren una comprensión detallada de los enfoques físicos dentro de un sistema para simular los impactos de eventos y la recuperación del sistema y son

difíciles de construir y consumen información. Los enfoques estadísticos requieren alternativamente una gran cantidad de datos sobre el rendimiento del sistema. Los modelos bayesianos combinan características de procesos y modelos estadísticos. Los modelos de red requieren una presentación del sistema como redes interconectadas cuya estructura depende de la función del sistema.

Alternativamente, el enfoque teórico/basado en agentes del juego se centra en el rendimiento del modelo del sistema basado en un conjunto limitado de reglas definidas por los modeladores. Con estos enfoques, se puede definir la resistencia, pero la utilidad de muchos modelos avanzados está limitada debido a los requisitos de uso intensivo de datos [43].

Los parámetros de resiliencia (función crítica, umbrales, tiempo y memoria) serán la base para identificar y describir las propiedades de red relevantes. Este cambio en las herramientas de pensamiento y evaluación es necesario para fomentar la adaptabilidad y la flexibilidad, además de evaluar adecuadamente las compensaciones entre la redundancia y la eficiencia que caracterizan una evaluación de la resiliencia útil.

Se han desarrollado múltiples herramientas para abordar la resiliencia en sistemas en ambos grupos metodológicos, como se puede observar en la siguiente figura:

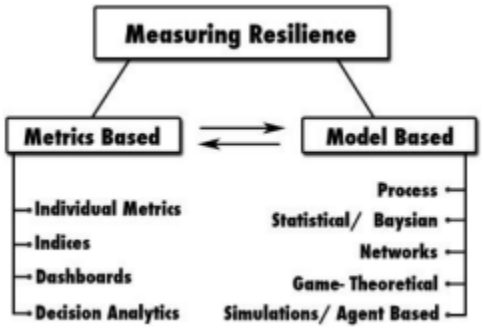

Ilustración 17 - Enfoques basados en métricas y modelos para la evaluación de la resiliencia. Fuente: [43].

Múltiples herramientas se han desarrollado para abordar la resiliencia en sistemas en ambos grupos metodológicos.

INDICADORES

Un indicador es la representación estadística de los datos de una característica relevante, relacionado con al menos una dimensión con el fin de permitir comparaciones significativas [50]. Esta es una medida de resumen relacionada con una cuestión clave o fenómeno y derivado de una serie de hechos observados. Permiten comparaciones en el tiempo entre, por ejemplo, países y regiones, y de esta manera ayudar en la recolección de "pruebas" para la toma de decisiones.

MÉTRICAS EN RELACIÓN A LA CIBER SEGURIDAD

Todas las estrategias de la Ciber seguridad tienen el mismo objetivo principal, el cual se base en proteger el Ciber espacio contra adversarios y mejorar la Ciber resiliencia [81].

Sin embargo, el panorama de amenazas cibernéticas, las condiciones sociopolíticas, las tendencias de seguridad, las tradiciones, el nivel de conciencia cibernética del país, han traído variaciones significativas en los enfoques de Ciber seguridad de los países, Sobre todo los que han sido seleccionados en algún momento para realizar estudio sobre la Ciber seguridad como EE. UU, Canadá, Australia, Nueva Zelanda, Estonia, Japón, UK, Alemania, Austria, Israel, Holanda, Finlandia, Francia, España y república checa entre otros.

A continuación, se describen un conjunto de métricas que se ha desarrollado para llevar a cabo la comparación de las estrategias de seguridad cibernética.

- Cronología de desarrollo (Año en que se publicó la estrategia o política de Ciber

- seguridad para un país en particular)
- Objetivos estratégicos en el documento de estrategia
- Comprensión de los principales términos clave. (Ciber espacio y Ciber seguridad)
- Nivel de priorización asignada a la Ciber seguridad nacional
- Percepción del país de las amenazas cibernéticas.
- Visión general de la organización: es decir, las principales organizaciones y actores públicos responsables de mantener el estado de la seguridad cibernética a nivel federal,
- Crítica sectores e infraestructura sin salidas enumerados en la estrategia
- Capacidades de respuesta a incidentes: es decir, si existen o no sistemas de alerta temprana cibernética, enfoques de intercambio de información sobre amenazas, equipos de respuesta a emergencias informáticas (CERTS), etc.
- Medidas legales: que abarcan los mecanismos de evaluación y revisión de la estrategia.
- Creación de capacidad: incluye el esfuerzo del país para la investigación y el desarrollo (I+D), el desarrollo de la fuerza de trabajo cibernética, la concienciación cibernética, etc.
- Colaboraciones para la Ciber seguridad (interestatal, intraestatal e internacional)

METODOLOGIAS PARA EL DESARROLLO DE WEB SEGURO MEDIANTE LA CIER RESILIENCIA.

Después de que se ha podido embarcar y profundizar un poco en cada parte que componen la Ciber resiliencia y la Ciber seguridad durante la fase de investigación. Por lo que ahora, se procede con el planteamiento de una metodología que estará basado en el conocimiento previamente adquirido durante el correr de las páginas anteriores.

Esta metodología de proyecto busca encontrar las mejores estrategias para la planificación de tareas y actividades que surjan durante el desarrollo del proyecto de investigación como también, la mejor practica que reúna las fases y características de la Ciber resiliencia. En caso que se presenten, la metodología del proyecto busca también saber cómo gestionar los incidentes o errores que se manifiesten antes, durante y en dado caso después.

Con el objetivo de buscar efectividad, asertividad y demás características resilientes para aplicarlo a un sistema web seguro.

A continuación, se mostrarán algunas metodologías relacionadas a la Ciber resiliencia en relación al desarrollo de software seguro.

METODOLOGÍA DE REQUISITOS DE SEGURIDAD CIBERNÉTICA (CYBER SECURITY REQUIREMENTS METHODOLOGY)

Una metodología es la Cyber Security Requirements Methodology, que por sus siglas en ingles se conoce como CSRM, el mismo traduce a *Metodología de Requisitos de Seguridad Cibernética.* CRSM busca soportar y mejorar las técnicas que se utilizan en la actualidad para el diseño y desarrollo de un sistema web [82], mediante un proceso donde reúne también los requisitos y mejores prácticas de la cibernética del sistema

El CSRM para los sistemas físicos cibernéticos está basado en el riesgo [83]. El riesgo está determinado por las consecuencias que ocurrirían si se produce un escenario de ataque cibernético en particular y la probabilidad de que ese escenario realmente ocurra. Las consecuencias pueden ir, por ejemplo, desde lesiones humanas o pérdida de vidas, a la pérdida de control, a la corrupción o retrasos de la información de concienciación de la situación, a la denegación de una operación del sistema.

El CSRM reconoce que los propietarios, operadores y usuarios de un sistema son la comunidad adecuada de personas para considerar y priorizar las posibles consecuencias que deben evitarse.

El CSRM también reconoce que los atacantes cibernéticos (adversarios) son la comunidad de personas que priorizan y determinan en última instancia la probabilidad de ataques cibernéticos específicos que ocurren [83].

Debido a la naturaleza del sistema, la cual incluye Ciber resiliencia y mejores prácticas de desarrollo, se necesita identificar los requisitos en una etapa preliminar a la finalización de la fase de diseño y arquitectura. Una vez identificado estos requisitos se aplica unas consideraciones que se basan en:

- Separación y aislamiento del hardware y software que soportan las funciones que maneja el sistema

- Selección de productos estándar, que representan los diferentes ataques cibernéticos que se han presentado y detectado

- Soluciones específicas que actuaran como defensa una vez el sistema tenga la capacidad y maduración en la web.

- Requisitos de diseño y rendimiento para las capacidades relacionadas a la resiliencia a lo largo del ciclo de vida del sistema.

- Realizar experimentos rápidos en la creación de prototipos y herramientas relacionadas donde se pueda poner a prueba la resiliencia del sistema.

- Donde dentro del proceso de desarrollo del nuevo sistema para enfocar el mayor énfasis y los recursos correspondientes con respecto a los procesos de desarrollo de software (herramientas de aseguramiento de calidad, pruebas, habilidades de desarrollo, soporte de ciclo de vida, etc.),

La metodología traba entra la coordinación de los tres equipos que se ven involucrados en los 6 pasos de desarrollo [82], los cuales son:

1. **SE (Systems Engineering)**, consiste en un grupo de personas que trabaja con las habilidades técnicas y de la operación basados en su experiencia adquirida. Ellos requieren tener unas bases sólidas de habilidades análisis que usaran como herramientas. Es responsable de la gestión coherente del proceso de esta metodología, donde como otra habilidad es ir actualizando las descripciones de los sistemas para dar nuevas soluciones a medida que surgen algún incidente en el sistema.

2. **Blue team**, trabajan en la operación. Tienen conocimiento sobre las prácticas operativas y sus propósitos para los sistemas están relacionados con el sistema en desarrollo. Su foco esta relacionando a las consecuencias ocasionadas por los riesgos y amenazas que se presentes, dando prioridad a las diversas funciones del sistema y evitar que los riesgos se materialicen generando consecuencias peores. Este equipo recibe apoyo del equipo SE.

3. **Red team**, Este equipo se centra en las identificaciones de todos los posibles ataques cibernéticos que se puedan presentar, con o sin una solución potencial para aplicar. Dicho equipo proporciona una visión priorizada sobre la defensa y resiliencia desde un punto objetivo. Se espera que los miembros presentan diversas soluciones y alternativas al impacto correspondiente a un ataque. Tiene una unión de expertos en Ciber seguridad y Ciber ataque que juntos desarrollan alternativas de solución y evaluaciones a las probabilidades de un ataque.

La metodología CSRM presenta un diagrama de flujo donde describe el trabajo de cada equipo durante el desarrollo de un sistema web, con un esquema iterativo, que se presenta a continuación.

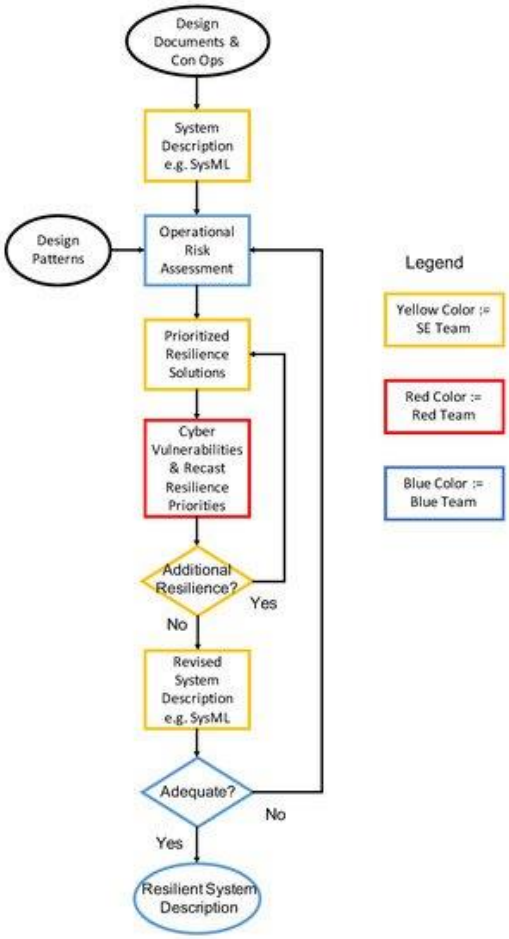

Ilustración 18 - Procesos que se manejan en el desarrollo utilizando la metodología CSRM, fuente: [82]

CSRM comienza de acuerdo con **Error! Reference source not found.** el esquema inicia con una descripción del sistema de alto nivel producida por el equipo de SE y luego se procede a realizar o ejecutar de una manera iterativa haciendo uso de los diversos equipos y su experiencia, descritos anteriormente. A continuación, se describe cada ítem representado en la imagen.

1. Descripción del sistema de alto nivel, se basa en herramientas producidas por el equipo de SE, incluida la arquitectura básica del sistema y la descripción funcional en un medio como el lenguaje de modelado de sistemas (SysML) a través de

diagramas de requisitos, diagramas de actividad, diagramas de definición de bloques y diagramas de bloques internos.

2. Equipo azul, Evalúa el riesgo operacional, cuya entrega es una lista priorizada de resultados funcionales indeseables, y un análisis de consecuencias basado en la descripción del sistema. Esto es similar, por ejemplo, a un análisis de riesgos funcionales de la comunidad de seguridad de la aviación.

3. Equipo SE: Obtiene las soluciones de resiliencia potencial priorizadas basadas en los resultados de la evaluación del riesgo operacional.

4. El equipo rojo, se basa en la experiencia con amenazas de ciberataques, soluciones de defensa cibernética COTS y GOTS (y el uso de herramientas analíticas para la confirmación de supuestos relacionados con ataques), prioriza soluciones de ingeniería de software, soluciones de defensa cibernética y soluciones de resiliencia.

5. Equipo de SE, Realiza ajuste de la descripción del sistema SysML para tener en cuenta las recomendaciones del equipo rojo y los resultados rápidos de creación de prototipos / simulación para su presentación al equipo azul. Tenga en cuenta que esto puede desencadenar otra iteración del proceso si las prioridades de refundición requieren un análisis adicional.

6. Equipo azul, responde a las recomendaciones del equipo rojo y los resultados de la simulación con su consecuencia revisada de priorización de soluciones, lo que permite al equipo de SE proporcionar un debate de diseño de sistema integrado para los responsables de la toma de decisiones relacionadas con los requisitos que incluiría consideraciones de costo y reducción de riesgos. Nuevamente, este paso puede desencadenar otra iteración a través del proceso.

Generar u obtener la descripción del sistema implica un esfuerzo de colaboración entre la SE y los equipos azules y rojos para acordar el propósito general, la funcionalidad y la misión del sistema.

El uso de una herramienta como SysML ayudó a comunicar diversas complejidades en las descripciones del sistema que pueden ser ambiguas o difíciles de transmitir utilizando un lenguaje natural.

La evaluación del riesgo operacional involucró principalmente un ejercicio de obtención liderado por el equipo SE, pero dirigido a capturar el conocimiento del equipo azul. El equipo de SE realizó el análisis de las consecuencias, lo que permitió que la información del equipo azul capturado se modelara en una forma interpretable Error! Reference source not found..

ESTANDARIZACIÓN DE BAJO NIVEL

Se deben manejar unos conceptos que deben sentar los estándares de la definición de los indicadores a bajo nivel incluyen los siguientes [50]. Aunque su prioridad no es la medición de Ciber-resiliencia, sino más bien la medición de la efectividad de la implementación de un ISMS que por sus siglas en ingles Information Security Management Systems.

A continuación, se describen los conceptos de acuerdo [50].

- **Objetivos**: Son de bajo nivel establecidos para el grupo de indicadores/indicador en concreto.

- **Ámbito**: Refiere a las áreas de implicación del modelo, en general el mismo se conforma por el concepto metodológico del universo y los entornos en los que se analiza, desarrolla e implanta el modelo, los cuales son:

  - ✓ Universo: conjunto de elementos o sujetos que se pretende estudiar.

- ✓ Ámbito Geográfico: Localización de los activos de recogida de datos.
- ✓ Ámbito Temporal: período temporal de recogida de información y continuidad en la recogida de datos, éste puede ser:

    - ➢ Transversal o longitudinal
    - ➢ Periódico o puntual
    - ➢ En tiempo real o diferido.

- ✓ Ámbito Tecnológico: qué tecnologías se ven implicadas en el proceso de medición y cuáles serán utilizada

- **Definición de métricas**: Consiste en la correspondencia del dominio empírico en el campo real de la Ciber-resiliencia en su abstracción formal matemática. En el cual se debe incluir la definición nominal del atributo o fenómeno estudiado, la tipología del fenómeno medido y las escalas de medida asociadas al fenómeno.

- **Definición de indicadores**, se relaciona al deber de definir el método de cálculo y la estimación del concepto medible.

- **Asociación Indicador ↔ Dominio Seguridad**, Donde se debe incluir la asociación del indicador con alguno de los dominios de seguridad definidos en el análisis de dominios de Ciber-resiliencia. Una vez definido el dominio, dentro de este apartado se puede añadir la correspondencia del propio indicador contra los controles de los estándares de seguridad y estándares de medición de la seguridad para obtener un mapa con dos vías de análisis: por indicadores, o por controles.

- **Método de cálculo**, cuál es el método de cómputo del indicador, y si es un indicador compuesto o simple.

- **Valor**, Se requiere de establecer el tipo de valor resultante del indicador (absoluto o relativo). Dentro del tipo de valor se pueden establecer los rangos de valor, si fuera necesario establecer límites y márgenes sobre los que fijar valoraciones del mismo.

- **Contraste**, En la medida de lo posible, y siempre que existan datos de test, se realizará un contraste de hipótesis para valorar el indicador, juzgando la propiedad de si es medible la Ciber-resiliencia y si es significativo el valor resultante del indicador contra lo observado en una muestra de la población, normalmente de fuentes de referencia externa.

- **Muestra**, Consiste en la definición de los datos recogidos para analizar y tamaños de las muestras.

- **Recogida de la información**, Cómo se va a realizar la recogida de la información para dicho indicador, procedimiento, responsables, almacenamiento.

- **Tratamiento de la información**, En este ítem busca indicar si será necesario los procesos de depuración, normalización, etc.

- **Otros**, Donde se podrá Indicar los procesos de difusión interna y/o externa.

METODOLOGÍA PARA EVALUAR LOS INDICADORES DE MEJORA DE LA CIBER RESILIENCIA

También conocida como Methodology for Assessing Cyber-Resilience Improvement Indicators en inglés.

El objetivo de esta metodología en los sistemas de control industrial es ayudar a todas las partes interesadas en la mejora de sus capacidades de la Ciber resiliencia y proporcionar un procedimiento para entender el nivel de madurez de sus controles para anticipar, resistir, recuperarse y evolucionar después de sufrir condiciones adversas, estrés o ataques contra los recursos cibernéticos de la organización [84].

Esta metodología está diseñada en su principal para sistemas de control industrial (ICS). Se utiliza en casos de amplia dispersión geográfica, cuando se requiere monitoreo y control centralizados. Tiene una arquitectura compuesta por subsistemas encargados de controlar los procesos localizados.

Este modelo está destinado a todas las empresas del sector industrial como una herramienta que les permite analizar sus capacidades de Ciber resiliencia. [84].

Los usuarios interesados en una organización pueden ser cualquier persona, grupo o empresa que forma parte o se ve afectada por ella obteniendo algún beneficio de acuerdo a sus propios intereses. El modelo presentado en este documento tiene por objeto satisfacer las diferentes necesidades de cada una de ellas, tal como se indica a continuación, teniendo en cuenta tanto las partes interesadas internas y externas más relevantes.

Partes interesadas	Necesidades	Función del modelo
Interno		
Gobierno	Saber de la Ciber resiliencia al nivel de ICS	Mejora continua de la resiliencia
Operación	Mejorar la Ciber resiliencia al nivel de ICS	Mejora continua de la resiliencia

Gerente de seguridad	Un modelo para medir el nivel de Ciber resiliencia del ICS	Mejora continua de la resiliencia
Externo		
Accionistas	Saber de la Ciber resiliencia al nivel de ICS	Información acerca de la Ciber resiliencia
Socios	Mejorar la continuidad del negocio a través de los socios o asociados Ciber resiliencia	Información sobre las capacidades de Ciber resiliencia de los socios o asociados

Tabla 1 - Necesidades de las partes interesadas y utilidad del modelo, Fuente: [84].

Modelo de evaluación.

Sobre la base del marco conceptual anterior, se ha diseñado un modelo para evaluar el nivel de Ciber resiliencia de un servicio esencial. Este marco conceptual consiste en los siguientes elementos [84]..

Las cuatro metas principales de acuerdo a [84]**.**

- ✓ **Anticipar (A)**: Mantiene un estado de preparación con el objetivo de evitar comprometer un servicio esencial por los Ciber ataques.
- ✓ **Resistir (T):** Busca continuar con los servicios esenciales a pesar de que ocurra un Ciber ataque. Exitoso o no exitoso.
- ✓ **Recuperar (R):** Restaura los servicios esenciales en la mayor posible medida después de la ejecución exitosa o no de un Ciber ataque.
- ✓ **Evolucionar (E)**: Para cambiar las funciones y capacidades, apuntando a un rediseño de la estrategia, con el fin de minimizar los impactos negativos de los Ciber ataques reales o futuros.

Adicional maneja nueve dominios funcionales, agrupados por objetivo de acuerdo a [84].**:**

- ✓ Política de Ciber seguridad (CP): Teniendo una política establecida en los requerimientos de la Ciber resiliencia. Aborda los riesgos de la Ciber seguridad, asigna responsabilidades y se comunica en toda la organización.

- ✓ Gestión del riesgo (RM): Identifica, analiza y mitiga los riesgos que impactan en los activos de la organización y que podrían impactar negativamente en el funcionamiento de la operación y prestación de servicios

- ✓ Capacitación de Ciber seguridad (CT): Promover el desarrollo de conocimientos y habilidades individuales, que apoyan sus tareas, permite el logro y mantenimiento de la protección operativa y la Ciber resiliencia.

- ✓ Gestión de la vulnerabilidad (VM): identifica, analiza y gestiona las vulnerabilidades sobre los activos que apoyan la prestación del servicio esencial

- ✓ Supervisión continua (CS); Colecta, compila y distribuye información acerca del comportamiento y actividades de los sistemas e individuos para soportar el continuo proceso de identificar y analizar los riesgos de la organización que impacta los servicios esenciales y puede perturbar negativamente su funcionamiento y entrega.

- ✓ Gestión de incidentes (IM): Establece procesos para identificar, analizar eventos, detectar incidentes, determinar e implementar una respuesta organizativa adecuada.

- ✓ Gestión de servicio continuo (SCM): determina como la organización realiza las actividades de planificación para asegurar la continuidad de los servicios esenciales en un evento de un incidente presentado.

- ✓ Gestión de configuración y cambios (CCM): Establece procesos para mantener la integridad de todos los activos (tecnología, información e instalaciones) necesitando proveer los servicios esenciales.

- ✓ Comunicación (CM); Establece procesos que garanticen las comunicaciones entre quienes, tanto internos como externos a la organización, participan en el funcionamiento de servicios esenciales

La agrupación de dominios dentro de los objetivos se puede ver en la siguiente tabla:

Anticipar	
Mantener un estado informado de preparación, con el fin de evitar comprometer los servicios esenciales por los ciberataques	Política de Ciber seguridad
	Gestión del riesgo
	Capacitación en Ciber seguridad
Resistir	
Continuar los servicios esenciales a pesar de la ejecución exitosa del ciberataque	Gestión de vulnerabilidad
	Supervisión continua
Recuperar	
Restaurar los servicios esenciales en la mayor medida posible después de la ejecución exitosa de un ataque cibernético.	Gestión de incidentes
	Gestión de servicio continuo
Evolucionar	
Cambiar funciones y capacidades, apuntando a un rediseño de la estrategia, con el fin de minimizar los impactos negativos de los ciberataques reales o futuros.	Gestión de configuración y cambios
	Comunicación

Tabla 2- Marco de referencia de la Ciber resiliencia, Fuente: [84].

EVALUACIÓN DE LA METODOLOGÍA

Para poder realizar una evaluación correcta de la metodología en cada empresa se desarrollan las siguientes etapas.

- Delinear el alcance del análisis.
- Realizar una prueba de autoevaluación o cuestionario.
- Implementar una serie de medidas correctivas dentro del ámbito.
- Repetir la consulta para analizar la eficacia de las medidas.

Etapa 1	
	Delinear el alcance del análisis.
	Seleccione un servicio esencial donde la interrupción tenga un impacto importante
Etapa 2	
	Realizar la prueba de autoevaluación
Etapa 3	
	Analizar medidas correctivas
	Aplicar los más adecuados para la organización
Etapa 4	
	Repita la prueba para evaluar el nuevo nivel de Ciber resiliencia

Tabla 3- Enfoque general de la metodología de evaluación, Fuente: [84].

La aplicación de las medidas correctivas que debe llevar a cabo la organización, que la Ciber resiliencia está en estudio, está fuera del ámbito de aplicación de este modo. [84].

Se describen los pasos de la metodología a continuación, conforme indica [84]:

- **Etapa 1 - Esquema de alcance**

El primer paso para aplicar el modelo es determinar el servicio esencial a ser evaluado. Dentro de este contexto, el alcance es definido con respeto a la prestación específica de un servicio esencial cuya interrupción puede tener un gran impacto en la organización. Por lo tanto, cada organización que le gustaría pasar por este modelo debe determinar el alcance de su propio cuestionario.

Como pauta general, el cuestionario debería completarse con respecto a la prestación específica de al menos un servicio esencial cuya interrupción presumiblemente tendría un impacto significativo. El cuestionario puede completarse para más de un servicio esencial, obteniendo así un valor de Ciber resiliencia para cada uno de los servicios considerados esenciales por el demandado. La realización de un análisis exhaustivo que incluya varios servicios permitirá a las partes interesadas localizar sinergias que permitan una mejora general en la Ciber resiliencia de la organización

- **Etapa 2 - Realización de autoevaluación**

Una vez identificado el servicio esencial, que es el objeto del análisis, el cuestionario de autoevaluación debe completarse evaluando las métricas seleccionadas según su propio grado de vencimiento. La consulta se lleva a cabo mediante el uso de una herramienta con una sección para cada objetivo: Anticipar, Resistir, Recuperar y Evolucionar. Para cada sección, la empresa debe insertar la medida tomada para las diferentes métricas. Cada una de estas métricas podría implementarse en la empresa con un nivel de madurez que debe elegirse. Los niveles de madurez se adaptan para cada métrica, y deben corresponder a uno de los ofrecidos por la herramienta, como se muestra en el ejemplo en la siguiente tabla:

L0	L1	L2	L3	L4	L5
L0	No se han establecido los requerimientos para la ciber resiliencia				
L1	Se ha iniciado la identificacion de los requerimientos para la ciber resiliencia				
L2	Se establecen los requerimeintos pero no hay documento oficial				
L3	Se establecen los requerimientos y se documenta				
L4	Los requerimientos han sido gestionados y verificados				
L5	Se aplican acciones de mejora en la definicion de los requerimientos de la metodologia				

Tabla 4 - Niveles de madurez en la metodología, Fuente: [84].

Una vez seleccionado el nivel de madurez correspondiente a cada una de las métricas, se obtendrá un resultado para cada objetivo. El ejemplo (Tabla 4) muestra cómo se podrían representar estos resultados como un diagrama de barras.

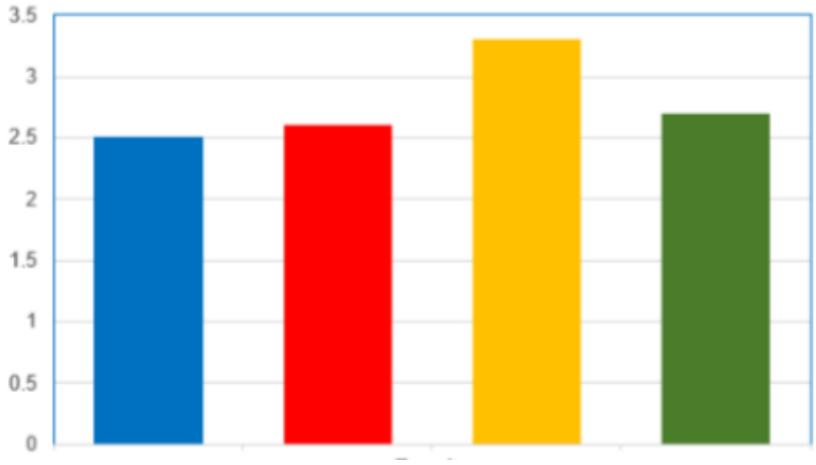

Ilustración 19 - Ejemplo de consulta Resultados, fuente: [84].

Donde:

- Azul refiere a Anticipar

- Rojo refiere a Resistir
- Amarillo refiere a Recuperarse
- Verde refiere a Evolucionar

Opcionalmente, para cualquier otro servicio esencial identificado en el punto anterior, se puede hacer otra consulta, obteniendo así el valor de Ciber resiliencia de cada servicio esencial identificado cuyo deterioro o fallo causa un gran impacto [84].

- **Etapa 3- Implementación de medidas correctivas**

Una vez realizada la consulta de autoevaluación, la empresa debe implementar las medidas correctivas. Estas medidas se podrían ver reflejadas en un documento mejoras de indicadores de la Ciber resiliencia que la empresa en cuestión manejaría.

A continuación, se puede mostrar un ejemplo de análisis de una acción correctiva.

Análisis		
Medida Objetiva		
Indicador	Valores positivos	Los valores que tienden al indicador L5 que las categorice la organización y priorice las vulnerabilidades que afectan un servicio esencial, para lo cual se lleva a cabo una encuesta. El nivel de criticidad debe estar basado en el objetivo de criterio.
	Medidas correctivas	Establecer un mecanismo para categorizar y priorizar las vulnerabilidades que afectan un servicio esencial. Por ejemplo, establecer la siguiente vulnerabilidad como prioridad de solución
		No tomar ninguna acción

		Resolver inmediatamente (Por lo general para actualizaciones o cambio de fabricante)
		Desarrollar e implementar la estrategia de resolución de vulnerabilidad
		Realizar investigación o análisis adicionales
		Referir vulnerabilidad a la gestión de riesgo para considerarse como un posible riesgo formal.

Tabla 5- Ejemplo de acciones correctivas, Fuente: [84].

Para la organización que lleva a cabo la consulta el estudio de la idoneidad de la aplicación, de las medidas correctivas propuestas, u otras más apropiadas, así como su proceso de implementación está fuera del alcance de este modelo.

- **Etapa 4 - Repita la consulta periódicamente**.

La evaluación de la Ciber resiliencia es un proceso que permite a las partes interesadas conocer su capacidad para anticiparse, resistir, recuperarse y evolucionar a partir de incidentes de Ciber seguridad. Es importante llevar a cabo estos análisis periódicamente para evaluar la eficacia de las medidas correctivas adoptadas y, por lo tanto, tratar de mejorar aquellos aspectos que necesitan mejoras, aumentando así la Ciber resiliencia de los servicios considerados esenciales.

NIST CYBER SECURITY FRAMEWORK (NIST CSF)

Esta metodología consiste en tener unos estándares, pautas y mejores prácticas para gestionar los riesgos relacionados a la Ciber seguridad. Cyber Security es flexible, prioriza y tiene un enfoque rentable que ayuda a promover la protección y resiliencia de las infraestructuras críticas y otros sectores importantes en la economía y seguridad digital [85].

El ciclo de vida de Ciber resiliencia de IBM permite a las organizaciones mejorar su robustez cibernética en cinco fases, de acuerdo a [42]:

- **Identificar** definiendo una hoja de ruta y un plan de acción para construir o mejorar el plan de Ciber resiliencia de la organización.
- **Proteger** a la organización de ataques descubriendo vulnerabilidades antes de que sean explotadas.
- **Detectar** amenazas desconocidas con análisis avanzados.
- **Responder** efectivamente a los brotes cibernéticos.
- **Recuperar** el acceso a datos y aplicaciones críticas.

A continuación, se presenta la imagen que representa al ciclo de vida de dicha metodología con cada fase integrada y en el orden correspondiente, de acuerdo a [86]

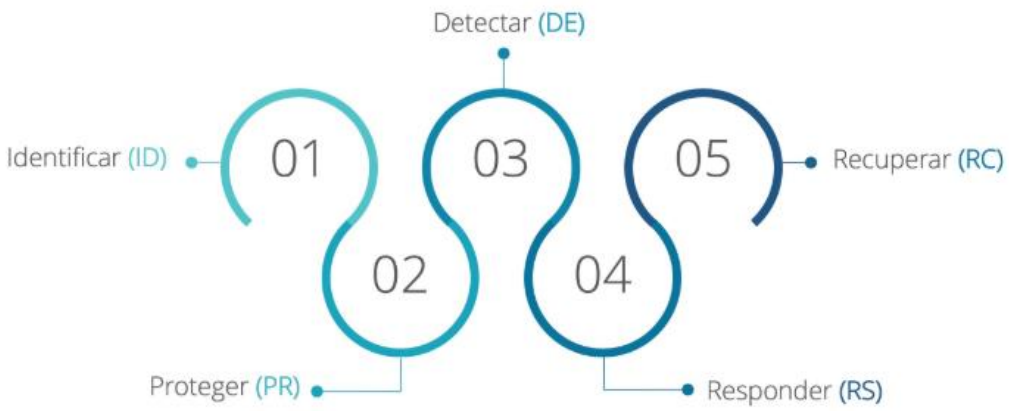

Ilustración 20 - Fases de NIST Cyber Security Framework, Fuente: [86]

Para lograr operaciones comerciales continuas, las organizaciones necesitan soluciones de recuperación de desastres y recuperación de incidentes cibernéticos que pasen de métodos manuales a modelos de automatización y orquestación.

IBM Cloud Resiliency Orchestrator (CRO), se ha mejorado para utilizar backup/datos replicados con Air Gap para proteger contra cortes cibernéticos**Error! Reference source not found.**, en la siguiente imagen se muestra el flujo de la metodología de resiliencia en producción;

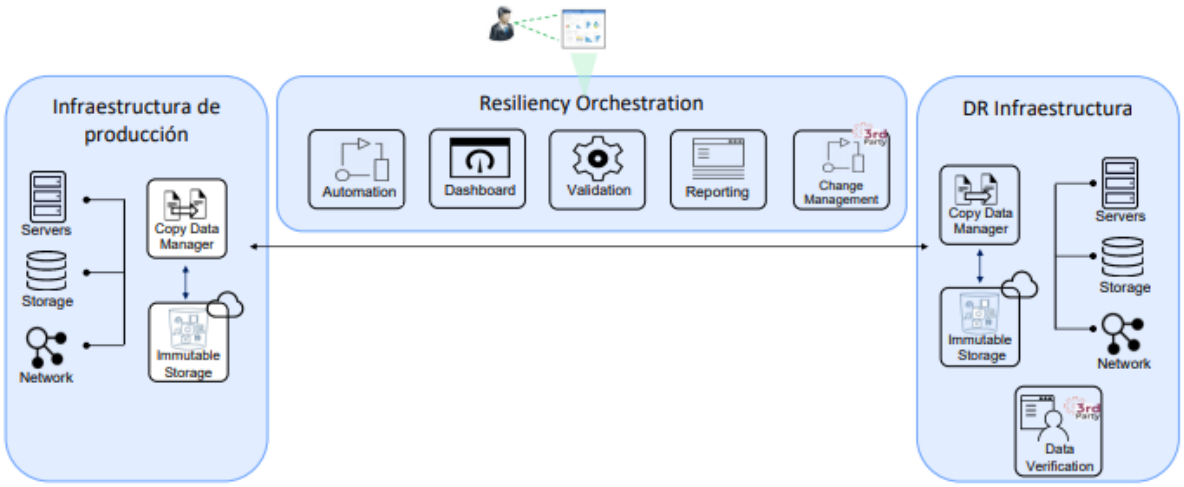

Ilustración 21- Flujo de la metodología, Fuente: [42] ***Error! Reference source not found.***

A continuación, se puede visualizar como está diseñado el flujo de las fases de la metodología, donde las fases nombradas anteriormente corresponden a “las funciones”, las categorías corresponden a subdivisiones de una función en grupo. Las subcategorías dividen una categoría en resultados, muy específicos y por último referencias informativas refiere a secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura critica que ilustran en un método para lograr los resultados asociados con cada subcategoría, El flujo es de acuerdo a

Ilustración 22- Diagrama de flujo de las fases de la metodología Cybersecurity Framework, Fuente: [87]

Características principales de la metodología. [87]

- El acceso vía Air-Gap reduce el riesgo de corrupción del backup.
- La recuperación rápida reduce el tiempo de inactividad y garantiza el RPO mínimo
- Recuperación eficiente en un punto en el tiempo con tecnologías de gestión de datos de copia.
- Almacenamiento inmutable para evitar la corrupción de la copia de seguridad

Recuperación de la configuración de plataformas ante Ciber incidentes.

Características principales de acuerdo a [87]

- Protección de configuraciones de dispositivos mediante Air-gap, copia de máquinas virtuales y sistemas bare metal a Inmutable Storage con IBM Resiliency Orchestration replication.

- La identificación temprana de anomalías en la configuración de la plataforma permite responder de inmediato y orquestar la recuperación con la inteligencia incorporada de Resiliency Orchestration (CRO)
- Restauración rápida de las configuraciones del dispositivo en la infraestructura de producción por CRO
- Restauración rápida de las configuraciones de máquina virtual y bare metal server en infraestructura de producción limpia
- Funcionalidad de pruebas inmediatas, para probar la solución con frecuencia sin afectar la producción
- Proporcionar visibilidad e informes en el proceso para garantizar el grado de cumplimiento y conformidad normativa.

Recuperación de datos frente a Ciber incidentes

Características principales de acuerdo a [42] **Error! Reference source not found.**

- Protección de máquinas virtuales y datos mediante herramientas de Copy Data Management y almacenamiento inmutables
- La detección de anomalías en los datos mediante la integración de múltiples herramientas propias o de terceros, reduce significativamente los daños causados
- Rápida recuperación de copias limpias en la infraestructura de recuperación de desastres
- Además, se pueden restaurar copias limpias en infraestructura de producción opcionalmente
- Proporcionar visibilidad e informes en el proceso para garantizar el cumplimiento y la preparación
- Proporcionar visibilidad e informes en el proceso para garantizar el grado de cumplimiento y conformidad normativa

Niveles de implementación del NIST Cyber Security Framework

Los niveles de implementación le permiten a la organización catalogarse en un umbral predefinido en función de las prácticas actuales de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones de la propia empresa [87]

Los rangos de los niveles de implementación son los siguientes:

- **Nivel 1** – Parcial (Partial): En este nivel las prácticas de gestión de riesgos de Ciber seguridad no están formalizadas (ad-hoc) y actúan por lo general de forma reactiva. La priorización de actividades no se encuentra alineada con los objetivos de riesgo organizacionales, el entorno de amenazas ni con los requerimientos de negocio. Se cuenta con una mínima participación externa en términos de colaboración y compartición de información

- **Nivel 2 –** Riesgos informados (Risk Informed): En este nivel las prácticas de gestión de riesgo están aprobadas por la Dirección, pero pueden no estar establecidas como una política global. Se cuenta con procedimientos y procesos definidos e implementados y con personal cualificado. La participación externa se realiza de manera informal.

- **Nivel 3** – Repetible (Repeatable): En este nivel las prácticas formales de gestión de riesgo son actualizadas regularmente como parte de la aplicación de análisis en cambios en requerimientos de negocio, amenazas o tecnologías. Se ha establecido un marco de colaboración formal con terceros.

- **Nivel 4** – Adaptativo (Adaptive): Las prácticas de Ciber seguridad están basadas en lecciones aprendidas e indicadores predictivos derivados de actividades previas y actuales de Ciber seguridad, a través de un proceso de mejora continua de adaptación a los cambios. Estas tareas hacen parte de la cultura organizacional. Se colabora de forma activa con terceros, compartiendo información de eventos de Ciber seguridad.

CONCLUSIONES

La elaboración del estado del arte hace parte de la investigación documental cuyo objetivo es alcanzar el conocimiento critico necesario en relación al nivel de comprensión que se tiene sobre un fenómeno, que para esta situación, se indago acerca de los diferentes ecuánimes que se deben contemplar a la hora de desarrollar un tipo de software seguro orientado a la web, contemplando la seguridad del mismo y la resiliencia que precisara para salvaguardar la información, calidad y funcionalidad del sistema implementado.

A lo largo del proceso de investigación, se contempló la revisión, el análisis y la profundidad de diferentes autores y opiniones acerca del tema, se consiguió tener un panorama más amplio, con base a la relación que debe existir para obtener un nivel de ciber seguridad adecuado y que además se debe de contemplar a la ahora de implementar un producto de software seguro, además se identificaron y presentaron los diferentes tipos de delitos informáticos, tales como por ejemplo ingeniería social, phishing y ransomware entre otros, orientados para que los participantes del grupo de diseño tengan en cuenta y puedan crear sistemas que prevengan y detecten en caso de que se llegara a presentar un evento de estos en el software seguro deseado.

Adicionalmente, se contempló el ciclo de vida que debe cumplir, por diferentes entes nombrados como Microsoft y los diferentes estándares que existen en el mercado para su mejor desarrollo entre ellos, la ISO 9126, ISO 27001 y compendios especiales que los diferentes gobiernos de cada país buscan implementar para su mejor productividad, por ejemplo, en Colombia el CONPES 3854.

Otro punto importante, es la medición de la calidad, basándose en la diferentes métricas y sistemas de evaluación de los sistemas, como de igual forma los riesgos y amenazas que se deben examinar a la hora de diseñar un sistema. Se indago también sobre las metodologías que permitirán un mejor desarrollo, diseño e implementación del mismo, entre ellas están los siete puntos de contacto de McGraw, Team Software Process, Oracle software security Assurance entre otros para poder generar que los sistemas sean robustos en los tres principios

del sistema de gestión de la seguridad de la información, los cuales son integridad, disponibilidad y confidencialidad.

Para finalizar, se tomó en cuenta una de las metodologías expuestas para el desarrollo de software seguro orientado al web basado en la ciber resiliencia, teniendo en cuenta que para que la metodología sea un éxito no se debe tener solo en cuenta la documentación que existe de la misma, sino contemplar todo lo anterior expuesto en el documento desde la ciber seguridad, ciber resiliencia, estrategias, metodologías etc.

BIBLIOGRAFIA

[1] C. G. a. M. H. Luis Baquero, «The Usability and Accessibility as Quality Factors of a Secure Web Product,» International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 23 (2018) pp. 16288-16294, Bogotá D.C., Colombia., 2018.

[2] A. Matei, «Guía para el desarrollo de Software Seguro,» Universidad Politécnica de Madrid Escuela Técnica Superior de Ingenieros Informáticos, Madrid, España, 2015.

[3] M. R. D. R. F. E. Norma Barrios Fernández, «La definición de funciones en la gestión de la calidad de los procesos universitarios,» 01 07 2016. [En línea]. Available: http://scielo.sld.cu/scielo.php?pid=S2073-60612016000200005&script=sci_arttext&tlng=pt. [Último acceso: 2019].

[4] J. P. C. Ana Villalta, «Modelos de calidad de software: Una revisión sistemática de la literatura,» Fundación Consorcio Ecuatoriano para el desarrollo de Internet Avanzado, MASKANA, CEDIA, 2015.

[5] S. M. BecerraPaola, «Revisión de Estado del Artedel Ciclo de Vida de Desarrollo de Software Seguro,» 01 06 2015. [En línea]. Available: http://revistas.unisimon.edu.co/index.php/identic/article/view/2474/2367.

[6] E. D. M. R. Dawam Dwi Jatmiko Suwawi, «Evaluation of academic website using ISO/IEC 9126,» IEEE, Nusa Dua, Bali, 2015.

[7] L. B. a. M. H. Celio Gil, «A Conceptual Exploration for the Safe Development of Mobile Devices,» International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 18, Bogotá D.C., Colombia, 2018.

[8] E. Editorial, «Reporte Digital,» 03 09 2018. [En línea]. Available: https://reportedigital.com/seguridad/vectores-de-ataque-activos-digitales/. [Último acceso: 2019].

[9] I. Ramos, «Patrones de Ataque y de Seguridad como guía en el,» Universidad Tecnológica Nacional, Facultad Regional Santa Fe, Argentina, Argentina, 2015.

[10] M. S. K. S. Donna Dodson, «Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework,» NIST CYBERSECURITY WHITE PAPER (DRAFT), 2019.

[11] V. Figueroa, «Secure Software Development Life Cycle,» OWASP, 2016.

[12] Y. Narváez Vallejo, «GESTIÓN DE SEGURIDAD EN EL PROCESO DE DESARROLLO DE SOFTWARE,» Universidad Piloto de Colombia, Bogotá, Colombia, 2016.

[13] M. J. |. G. S. M. |. L. H. P. Blas, «Especificación de la calidad en software-as-a-service: definición de un esquema de calidad basado en el estándar ISO/IEC 25010,» SEDICI, 2016.

[14] D. C. L. Roberto, «Desarrollo de software seguro,» Universidad piloto de Colombia, Bogotá, Colombia.

[15] ISO, «ISO,» 01 06 2017. [En línea]. Available: https://www.iso.org/standard/44378.html. [Último acceso: 2019].

[16] Y.-H. H. M. A. H. N. S. U. Leah Winkfield, «A Study of the Evolution of Secure Software Development Architectures,» Journal of The Colloquium for Information System Security Education, 2018.

[17] M. D. Sguerra, «Diseño de software seguro,» http://52.0.140.184/typo43/fileadmin/Revista_119/Uno.pdf, Bogotá, Colombia, 2018.

[18] OWASP, «Guía de Seguridad en Aplicaciones para CISOs,» OWASP, 2015.

[19] INCIBE, «INCIBE,» 20 03 2017. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian. [Último acceso: 08 10 2019].

[20] U. N. d. Luján, «Seguridad informatica,» 01 06 2018. [En línea]. Available: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12. [Último acceso: 08 10 2019].

[21] MINTIC, «Seguridad y privacidad de la informacion,» https://www.mintic.gov.co/, Bogotá, Colombia, 2016.

[22] Proteje, «Proteje,» 01 09 2015. [En línea]. Available: https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/. [Último acceso: 08 10 2019].

[23] G. Robalino, «Iniciando en Desarrollo seguro,» OWASP, 2017.

[24] D. M. T. S. y. A. C. Baquero., «Sistema de Control de Versiones para el Desarrollo de Software Seguro,» Fundación Universitaria los Libertadores. Pasantía Investigativa., Bogotá, Colombia, 2016.

[25] G. McGraw, software security building security in, Raleigh, NC, USA: IEEE, 2006.

[26] W.WatsonaD.G.KouriebL.Cleophas, «Experience with correctness-by-construction,» ScienceDirect, 2015.

[27] OWASP, «OWASP,» 16 08 2016. [En línea]. Available: https://www.owasp.org/index.php/CLASP_Concepts. [Último acceso: 22 10 2019].

[28] S. L. K. a. M. N. b. Mahrin, «Secure Software Development Practice Adoption Model: A Delphi Study,» Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, MALAYSIA., 2018.

[29] M. A. O. S. M. K. Amjad Hudaib1, «A Survey on Design Methods for Secure Software Development,» University of Jordan, King Abdullah II School for Information Technology, Computer Science Department,, Jordan, 2017.

[30] k. Publications, «INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY,» https://rajpub.com/, Punjab, India, 2019.

[31] P. Chandr, «Software Assurance Maturity Model,» OWASP, 2017.

[32] M. R. I. M. R. P. O. D. E. C. A. Díaz Sánchez Dulce Yadira, «Team Software Process,» Fernando Arciniega, 2017.

[33] ORACLE, «ORACLE,» 01 01 2019. [En línea]. Available: https://www.oracle.com/co/corporate/security-practices/assurance/. [Último acceso: 23 10 2019].

[34] R. Hughes, «Introduction to Alternative Iterative Methods,» Science Direct, 2016.

[35] F. B. N. M. D. M. A. S. Z. M. z. Y. M. A. M. R. Haslina Mohd, «A Secured e-Tendering Model Based on Rational Unified Process (RUP) Approach: Inception and Elaboration Phases,» School of Computing, Universiti Utara Malaysia, Sintok, Kedah, Malaysia., 2016.

[36] Ž. C. y. A. C. Hrvoje Belani, «RUP-Based Process Model for Security Requirements Engineering inValue-Added Service Development,» University of Zagreb, Faculty of Electrical Engineering and Computing Department of Telecommunications, Zagreb, Croatia, s.f..

[37] Dr. Francisco José García Peñalvo, «INGENIERÍA DE SOFTWARE I,» Departamento de Informática y Automática Universidad de Salamanca, Salamanca. España., 2018.

[38] L. Sharma, «TOOLSQA,» 17 04 2016. [En línea]. Available: https://www.toolsqa.com/software-testing/waterfall-model/. [Último acceso: 21 10 2019].

[39] M. Jorge Izaguirre Olmedo, «Análisis de los ciberataques realizados en América Latina,» INNOVA Research Journal,, Ecuador, 2018.

[40] G. Shah, «Detection and Prevention of System against Cyber Attacks,» International Journal for Scientific Research & Development| Vol. 5,, Vadodara, India, 2017.

[41] L. B. a. C. G. Miguel Hernández, «Approach to the State of the Art of Ciberdelincuence in Colombia,» International Journal of Applied Engineering Research ISSN 0973-4562, Bogotá D.C., Colombia, 2018.

[42] I. services, «Recuperación ante desastres y Ciber Resiliencia,» IBM Resiliency Orchestration, 2018.

[43] A. Kott, «Fundamental Concepts of Cyber Resilience: Introduction and Overview,» Springer, U.S. Army Research Laboratory, 2018.

[44] G. A. C. M, «Universidad del Cauca,» 01 05 2017. [En línea]. Available: http://fccea.unicauca.edu.co/old/siconceptosbasicos.htm. [Último acceso: 17 07 2019].

[45] E. A. D. González, «ESTAFA INFORMÁTICA DEL ARTÍCULO,» Universidad De Sevilla, 2017.

[46] D. J. Howard, «Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents,» University of South Florid, Florida, US, 2018.

[47] J. A. E. K. Mukesh Chinta, «A Study on Social Engineering Attacks and DefenceMechanisms,» Special Issue International Journal of Computer Science and Information Security (IJCSIS, Vijayawada, Andhra Pradesh, India, 2016.

[48] A. Bradbury, «Network Defense and Team Cognition: A Team-Based Cybersecurity Simulation,» ARIZONA STATE UNIVESRIT, Arizona, US, 2016.

[49] A. v. m. L. M. l. M. Reza Arghandeh, «On the definition of cyber-physical resilience in power systems,» California institute for energy and environment electrical engineering and computer science department, California, US, 2016.

[50] J. D. P. Á. y. M. G. H. Héctor R. Suárez, «Ciber Resiliencia aproximacion a un marco de medicion,» INCIBE, s.f..

[51] D. Acosta, «metodos de evaluacion de riesgos,» 25 03 2014. [En línea]. Available: http://metodosdeevaluacionderiesgos.blogspot.com/2014/03/metodologias-de-evaluacion-de-riesgos.html. [Último acceso: 11 10 2019].

[52] I. Excellence, «SGSI,» 16 03 2015. [En línea]. Available: https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/. [Último acceso: 15 10 2019].

[53] M. Hurtado, «GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT,» Universidad Piloto de Colombia. Hurtado. Metodología de Análisis de Riesgo, Bogotá. Colombia., 2016.

[54] 2. C. R. B. Helena Alemán Novoa, «Metodologías Para el Análisis de Riesgos en los SGSi,» Fundación Universitaria Juan de Castellanos, Facultad de Ingeniería, Tunja, Boyacá, Colombia, 2015.

[55] E. O. Numpaque Pineda, «ANÁLISIS DE RIESGOS: PROCESO, REGULACIONES Y METODOLOGÍAS,» Universidad Piloto de Colombia, Bogotá, Colombia, s.f..

[56] G. BSI, «The British Standards Institution 2019,» 14 11 2018. [En línea]. Available: https://www.bsigroup.com/es-CO/gestion-de-riesgo-iso-31000-/. [Último acceso: 15 10 2019].

[57] R. Management, «ENISA,» 01 01 2019. [En línea]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_riskwatch.html. [Último acceso: 15 10 2019].

[58] R. Management, «ENISA,» 01 01 2019. [En línea]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_riskwatch.html. [Último acceso: 15 10 2019].

[59] J. N. R. Pinzon, «Metodologia para identificacion y valoracion de riesgos y salvaguardas en una mesa de ayuda tecnologia,» Universidad Piloto de Colombia, Bogotá, Colombia, s.f..

[60] R. Management, «Riskwatch,» ENISA, 2019.

[61] A. A. A. R. L. Dante Carrizo, «PROPUESTA DE UN MODELO DE PLAN DE CONTINUIDAD: UN ESTUDIO DE CASO,» Memorias de la Décima Quinta Conferencia Iberoamericana en Sistemas, Cibernética e Informática, Copiapó, Chile, 2016.

[62] G. -. U. R. -. P. A. -. B. R. -. P. L. Pizarro, «Sistemas de información en ciencias de la computación,» Repositorio Institucional de la Universidad Politécnica Salesiana, Ecuador, 2017.

[63] A. P. A. M. I. F. H. M. M. S. M. E. M. M. P. M. A. Gabriela, «Plan decontingenciainformático,» Universidad Autónoma de San Luis Potosí, 2015.

[64] J. T. F. T. Initiative, «Guide for Conducting Risk Assessments,» NIST, 2012.

[65] J. F. S. R. Y. R. W. Richard A. Caralli, «Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,» Software Engineeringinstitute, 2007.

[66] ISO, «ISO /IEC 27001,» 01 07 2017. [En línea]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Último acceso: 15 10 2019].

[67] R. Management, «ENISA,» s.f. s.f. s.f.. [En línea]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html. [Último acceso: 15 10 2019].

[68] J. C. y. J. A. M. Miguel Angel Amutio Gómez, «MAGERIT – versión 3.0Metodología de Análisis y Gestiónde Riesgos de los Sistemas de Información,» Ministerio de Hacienda y Administraciones PúblicasSecretaría General TécnicaSubdirección General de Información,Documentación y PublicacionesCentro de PublicacionesColección: administración electrónicaNIPO: 630-12-171-8, Madrid, España, 2014.

[69] SANS, «The CIS Critical Security Controls for Effective Cyber Defense,» SANS, 2015.

[70] G. c. G. Morales, «Gestión de la Ciberseguridad según el ISO/IEC 27032:2012,» ENISA, 2017.

[71] P. Jorge E. Olaya T., «Estándar ISO 22301: nueva versión 2019 para Continuidad del Negocio,» 2019.

[72] G. T. P. L. Z. J. Czajkowskiac, «Cyber risk and insurance for transportation infrastructure,» Science Direc, 2019.

[73] J. S. J. Z. F. B. Martin Henkel, «Cyber Resilience – Fundamentals for a Definition,» Department of Computer and Systems Sciences,, Kista, Sweden , 2015.

[74] O. Khan y D. A. Sepúlveda Estay, «Supply Chain Cyber-Resilience: Creating an Agenda for Future Research,» Creating an Agenda for Future Research. Technology Innovation Management Review, 2015.

[75] L. d. S. Carrasco*, «CIBER-RESILIENCIA,» IEEE, 2015.

[76] A. Pinilla, «Resiliencia en la Seguridad Informática,» Universidad Piloto de Colombia, Bogotá, Colombia, s.f..

[77] M. d. D. N. D. N. d. I. D. N. d. P. Ministerio de Tecnologías de la Información y las Comunicaciones, «CONPES 3854,» CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, Bogotá, Colombia, 2016.

[78] M. C. L. M. a. M. B. Richard Ford, «Toward Metrics for Cyber Resilience,» Florida Institute of Technology University of California at Davis, California, US, s.f..

[79] ECURED, «Métrica de software,» s.f. s.f. s.f.. [En línea]. Available: https://www.ecured.cu/M%C3%A9tricas_de_software. [Último acceso: 14 06 2019].

[80] R. G. L. L. P. K. A. R. J. B. Deb Bodeau, «Cyber Resiliency Metrics,,» Approved for Public Release: 12-2226., s.f..

[81] A. M. Narmeen Shafqat, «Comparative Analysis of Various National CyberSecurity Strategies,» International Journal of Computer Science and Information Security, Rawalpindi, Pakistan, 2016.

[82] S. A. 1. B. 2. S. 1. B. 1. H. 1. a. F. 1. Bryan Carter 1OrcID, «A Preliminary Design-Phase Security Methodology for Cyber–Physical Systems,» https://doi.org/10.3390/systems7020021, 2019.

[83] P. B. C. F. a. T. Barry Horowitz, «Cyber Security Requirements Methodology,» Technical Report SERC-2018-TR-110, 2018.

[84] INCIBE, «Methodology for Assessing Cyber-resilience Improvement Indicators,» INCIBE CERT, España, 2019.

[85] NIST, «CYBERSECURITY FRAMEWORK,» NIST, 2019.

[86] G. G. Morales, «¿Qué es el Cybersecurity Framework de NIST de los Estados Unidos?,» 30 04 2019. [En línea]. Available: https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/. [Último acceso: 06 08 2019].

[87] N. C. F. (CSF), «NIST Cybersecurity Framework (CSF),» U.S. General Services, 2019.

[88] M. A. S. y. M. K. Amjad Hudaib, «A Survey on Design Methods for Secure Software Development,» 1University of Jordan, King Abdullah II School for Information Technology, Computer Science Department,, 2017.