TRABAJO FIN DE MÁSTER

TÍTULO OFICIAL UNIVERSITARIO

CURSO ACADÉMICO: 2021 - 2022

CONVOCATORIA: NOVIEMBRE

AGILIDAD EN UN PROGRAMA DE CIBERSEGURIDAD APLICADO A UNA PYME EN PERÚ

APELLIDOS/NOMBRE ESTUDIANTE:

TAN NOZAWA JAIME MARTÍN

APELLIDOS/NOMBRE TUTOR:

LÓPEZ RAÚL

Fecha: agosto del 2022

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El presente trabajo final de máster propone el diseño de un programa de ciberseguridad para una pequeña empresa con el enfoque y la filosofía ágil. Además, tiene en consideración los modelos, marcos y controles de ciberseguridad de aplicación práctica, simples y técnicamente precisas.

La propuesta de valor sería brindarle una herramienta de utilidad a una pequeña empresa para que logre implementar un programa de ciberseguridad y que le brinde el mayor beneficio a su negocio en el menor tiempo posible.

Para ello, se ha planteado como objetivo principal la integración de estos dos conceptos, el de ciberseguridad y agilidad. Luego de ello, en un caso de aplicación, se procederá a probar el modelo y las herramientas propuestas en el proceso de diseño del programa en una PYME ubicado en Latinoamérica.

Palabras Clave:

Programa de ciberseguridad, agilidad, PYME, seguridad de la información, ciberseguridad, pequeña empresa.

I. INTRODUCCIÓN

1.1. Problema

Según S2 Grupo, las pequeñas empresas son el principal objetivo de amenazas cibernéticas, se le atribuye un 74% de afectación en incidencias en ciberseguridad. Por otro lado, la empresa Kaspersky menciona que el 40% de las PYMES tienen problemas para invertir en mejoras para la ciberseguridad de su organización. Usualmente, cuando se piensa en brindar seguridad de la información en una empresa, se recomienda la adopción de su estándar ISO constituido por 114 controles. Esta tarea es enorme y titánica para emprendimientos de pequeña o mediana escala. Alcanzar este objetivo podría tomarle años según la prioridad en la estrategia de la organización y la asignación del presupuesto. Si no se alcanza una gestión mínima de la ciberseguridad, una PYME no podría nunca alcanzar esa soñada transformación digital.

Los principales motivos de fracaso de la implementación de un Sistema de Gestión de Seguridad de la Información utilizando el estándar ISO 27001, es la planificación del proyecto, la falta de respaldo de la alta dirección y principalmente la mala concepción de que la seguridad es responsabilidad sólo del área de tecnología. Se resalta que el 40% de los controles de seguridad son atribuibles al área de TI, por lo tanto, su aplicación requiere a todas las áreas dentro de la organización (Tristancho Robles, L.A., 2015). Según este autor, la utilización de métodos tradicionales basado en estándares, que cambian cada 5 años o más, sería muy rígido, complejo y extenso. En su lado opuesto, para afrontar este reto es necesario manejar una propuesta con un modelo que implique el cambio constante, la agilidad en su diseño e implementación y sobre todo que brinde rápidos beneficios cuantificables al negocio.

El presente trabajo de investigación va a proponer un cambio en el paradigma de utilizar estándares internacionales de seguridad, por el de un diseño, desde su concepción, híbrido y ágil de un programa de ciberseguridad para una PYME.

1.2. Preguntas de la investigación

¿La integración y uso de métodos ágiles como Kanban y Scrum, en un programa de ciberseguridad, obtendrá un rápido retorno de inversión en seguridad en una

pequeña empresa? ¿Cuáles son los marcos de trabajo y controles de seguridad más adecuados para un programa de ciberseguridad ágil para una PYME?

1.3. Justificación

El propósito de desarrollar la presente tesis es construir una herramienta que permita implementar un programa de ciberseguridad ágil y eficaz, y con ello, mitigar el impacto de ciber amenazas, aumentar la ciber resiliencia y asegurar la continuidad de la operación de una pequeña empresa. El principal beneficiario sería la organización del caso de aplicación, los directivos y sus trabajadores. De igual forma, es adaptable a cualquier PYME de latino américa expuesta a ciber amenazas.

1.4. Hipótesis

Si se utiliza métodos ágiles en el diseño de controles ciberseguridad, entonces mejorará el seguimiento y control de un programa de ciberseguridad con un retorno de inversión en seguridad en el corto plazo y una mejora notable en su ciber resiliencia para una pequeña empresa.

1.5. Objetivo General

Desarrollar una propuesta de integración de marcos de trabajo, controles de ciberseguridad y aplicación de herramientas ágiles en un programa de ciberseguridad para una pequeña empresa.

1.6. Objetivos específicos

- Seleccionar los marcos de trabajo, controles de ciberseguridad aplicables para generar agilidad y adaptabilidad para una pequeña empresa
- Definir un cuadro de controles de ciberseguridad resultado del modelo y aplicados en el caso de aplicación.
- Definir una planificación ágil del programa de ciberseguridad del caso de aplicación.
- Definir una lista de herramientas de metodologías ágiles aplicado a la ciberseguridad de una pyme.
- Calcular el ROSI o retorno de inversión de seguridad de un control implementado del caso.

II. MARCO TEÓRICO

2.1.Ciberseguridad

Según la empresa especializada en seguridad informática Palo Alto Networks, define ciberseguridad como indica a continuación:

> *"[…] Ciberseguridad implica proteger la información y los sistemas contra amenazas cibernéticas importantes, como el ciber terrorismo, la guerra cibernética y el ciber espionaje."* (PALO ALTO, 2017)

Podemos confirmar este concepto propuesto por ISACA, que define la ciberseguridad de la siguiente forma:

> *"[…] La protección de los activos de información mediante el tratamiento de las amenazas a la información procesada, almacenada y transportada por sistemas de información conectados en red."* (ISACA, 2017)

2.2.Vulnerabilidad, Amenaza y Riesgo

Es posible definir estos tres conceptos básicos en seguridad informática tomando en consideración el *Glosario de términos de ISACA*:

- Amenaza, es cualquier cosa (por ejemplo, objeto, sustancia, humano) que sea capaz de actuar contra un activo de una manera que puede resultar en daño. Una posible causa de un incidente no deseado.
- Vulnerabilidad, una debilidad en el diseño, implementación, operación o el control interno de un proceso que podría exponer el sistema a amenazas adversas provenientes de eventos de amenaza.
- Riesgo, es la combinación de la probabilidad de un evento y sus consecuencias. (ISACA, 2017)

2.3.Conceptos básicos de amenazas cibernéticas

Adicionalmente, se mencionarán diferentes tipos de amenazas cibernéticas. Estos conceptos son obtenidos del glosario de términos de firmas de seguridad Panda Security y ESET.

- Botnet, red o grupo de ordenadores zombies, controlados por el propietario de los bots. El propietario de las redes de bots da instrucciones a los zombies. Estas

órdenes pueden incluir la propia actualización del bot, la descarga de una nueva amenaza o lanzar ataques de denegación de servicio, entre otras. (PANDA, 2022)

- Centro de Comando & Control (C&C o CnC o C2), servidor administrado por un botmaster que permite controlar y administrar los equipos zombis infectados por un bot, rootkit, gusano u otro tipo de malware, que integran la botnet. (ESET,2022)
- DDoS o Distributed Denial of Service, es un ataque distribuido de denegación de servicio. Se lleva a cabo generando un gran flujo de información desde varios puntos de conexión, por lo general a través de una botnet. (ESET, 2022).
- Exploit, es una técnica o un programa que aprovecha un fallo o hueco de seguridad existente en un determinado protocolo de comunicaciones, sistema operativo, o herramienta informática. (PANDA, 2022)
- Malware, cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. (PANDA, 2022)
- Phishing, consiste en el envío masivo de mensajes que, aparentando provenir de fuentes fiables, intentan conseguir que el usuario proporcione datos confidenciales. (PANDA, 2022)
- Ransomware, código malicioso usado para extorsionar a sus víctimas. El ransomware criptográfico cifra la información allí alojada; luego, el cibercriminal solicita dinero para devolver el poder sobre su equipo o sus datos. (ESET, 2022)

2.4.Estado de la ciberseguridad en el Perú y América Latina

Según el *Reporte Ciberseguridad del BID y la OEA* (BID, 2020), el Perú aún no cuenta con una estrategia nacional de seguridad cibernética, sin embargo, sí ha puesto en marcha iniciativas para una política y un comité de nacional en ciberseguridad. Las principales herramientas que posee, en el aspecto legal, se encontrarían el dictamen del proyecto de Ley de Ciberseguridad, que busca establecer el marco normativo en materia de seguridad digital (2019), La ley 29733 - Protección de datos personales (2011) y la ley 30096 - Delitos informáticos (2013).

Por otro lado, si se consulta el informe *ESET Security Report 2021*(ESET, 2021) podemos rescatar un conjunto de estadísticas de las principales ciberamenazas de los países en Latino América, y notaremos que el país del Perú se encuentra en un alto riesgo al ubicarse primero en la mayoría de sus categorías. Respecto al phishing, las empresas de Brasil fueron las más afectadas con el 26,4% de todas las detecciones,

según el informe, seguidas por Perú (22,8%), México (12%) y Colombia (9,1%). Respecto al malware para la minería de criptomonedas el país en la región con mayor porcentaje de detecciones fue Perú (10,1%) y Ecuador (5,1%). Sobre la amenaza de Ransomware a nivel empresas los países con mayores detecciones fueron Perú (30%), seguido por México (14.9%), Venezuela (13.2%), Brasil (11.3%) y Colombia (7.9%). Los principales controles de seguridad tecnológicos implementados para mejorar sus medias de protección, reflejan también la prioridad en la inversión en seguridad de las empresas. Los principales controles de las empresas serían el antimalware o antivirus tradicional (86%), firewalls (75%) y soluciones de respaldo de información (68%).

El Perú tiene más de 12 millones de usuarios de Internet, y esta cifra va en aumento con ello también el crecimiento de las amenazas de ataques cibernéticos.

2.5.Programa de Ciberseguridad

Si revisamos el *Modelo de Construcción de Capacidades de Ciberseguridad de la Cadena de Valor* que forma parte del Esquema Nacional de Seguridad Industrial o ENSI, define a un programa de ciberseguridad como indica a continuación:

> *"Un programa de ciberseguridad representa una suma de procesos, tecnología, políticas, gobierno, alineamiento con el negocio, actividades de concienciación y otros elementos necesarios para gestionar, de manera efectiva, la postura de ciberseguridad de la organización."* (INCIBE, 2019)

Así mismo la consultora A2Secure, menciona lo siguiente:

> *"El programa de ciberseguridad se encarga de desarrollar planes específicos, centrados en el cliente, con el propósito de controlar los riesgos de seguridad, y siempre adaptados a las posibilidades reales de nuestros clientes y al ecosistema en que se encuentran."* (A2secure, 2021)

Según el libro Building a Comprehensive IT Security Program (Wittkop Jeremy, 2016) menciona para definir un programa de ciberseguridad primero es necesario alinearlo al negocio, luego definir la inteligencia y las estrategias. Consecutivamente, las tácticas necesarias y tecnología a utilizar, para culminar con la capa de eventos. El negocio de la empresa u organización es la que debe

determinar cuáles son las necesidades de la urgencia y cuáles serían los eventos de seguridad que hay que mitigar y en lo posible evitar que ocurran.

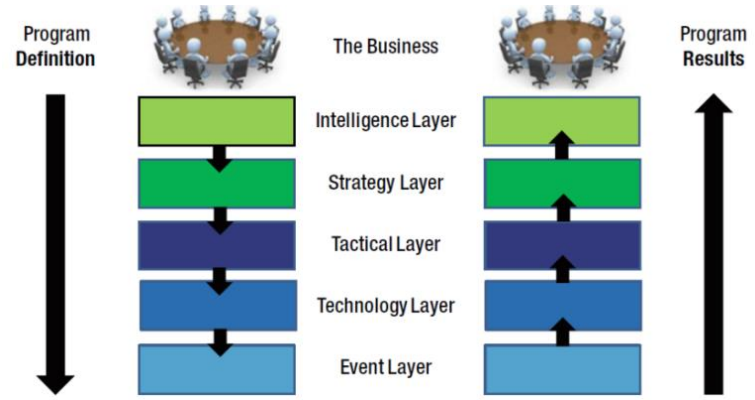


Figura 1. Modelo de Inteligencia de Seguridad

Nota. Gráfico del libro "Building a Comprehensive IT Security Program", Wittkop, 2016

2.6. Métodos y marcos ágiles

2.6.1. Kanban

Según Anderson, D.J. & Carmichael en su libro *Kanban Esencial Condensado,* define el término *Kanban* como sigue:

> *"Kanban es un método para definir, gestionar y mejorar servicios que entregan trabajo del conocimiento, tales como servicios profesionales, trabajos o actividades en las que interviene la creatividad y el diseño tanto de productos de software como físicos."* (Anderson, D.J. & Carmichael, 2016)

Según el libro *Kanban y Scrum, obteniendo lo mejor de ambos* (Kniberg, H. & Skarin, M., 2010) explica de forma muy resumida que es Kanban basado en sus características. Según estos autores, Kanban realiza lo siguiente:

- Visualiza el flujo de trabajo:
    - Divide el trabajo en bloques, escribe cada elemento en una tarjeta y ponlo en el muro.
    - Utiliza columnas con nombre para ilustrar dónde está cada elemento en el flujo de trabajo.
    - Limita el WIP (Work in Progress o trabajo en curso) - asigna límites concretos a cuántos elementos pueden estar en progreso en cada estado del flujo de trabajo.

- Mide el lead time (tiempo medio para completar un elemento, a veces llamado "tiempo de ciclo"), optimiza el proceso para que el lead time sea tan pequeño y predecible como sea posible.

2.6.2. Scrum

Como nos comenta Schwaber, K. & Sutherland, J. en su *Guía definitiva de Scrum*, este concepto puede definirse como indica a continuación:

> *"[…] Un marco de trabajo por el cual las personas pueden abordar problemas complejos adaptativos, a la vez que entregar productos del máximo valor posible productiva y creativamente. Scrum es: liviano, fácil de entender y difícil de dominar."* (Schwaber, K. & Sutherland, J., 2017)

En el libro *Kanban y Scrum, obteniendo lo mejor de ambos* (Kniberg, H. & Skarin, M., 2010), Scrum puede ser explicado en breves frases, éstas serían:

- Divide tu organización en equipos pequeños, interdisciplinarios y autoorganizados.
- Divide el trabajo en una lista de entregables pequeños y concretos. Ordena la lista por orden de prioridad y estima el esfuerzo relativo de cada elemento.
- Divide el tiempo en iteraciones cortas de longitud fija (generalmente de 1 a 4 semanas), con código potencialmente entregable y demostrado después de cada iteración.
- Optimiza el plan de entregas y actualiza las prioridades en colaboración con el cliente, basada en los conocimientos adquiridos mediante la inspección del entregable después de cada iteración
- Optimiza el proceso teniendo una retrospectiva después de cada iteración.

2.6.3. Historias de usuario

En la exploración del libro *Proyectos Ágiles con Scrum* podemos encontrar el origen del término como indica a continuación:

> *"[…] Las Historias de Usuario son especificaciones funcionales que invitan a la conversación para que el detalle sea consecuencia de esta última y no un remplazo"*. (Alaimo D.M, 2013)

Cabe mencionar que la *Project Management Institute* define historia de usuario:

> *"[…] Una breve descripción del valor entregable para un usuario específico. Es un compromiso de discusión a fin de aclarar detalles."* (PMI, 2017a)

2.6.4. Lista de Producto o Product Backlog

Los especialistas Schwaber, K. & Sutherland, J. nos indica en su *Guía definitiva de Scrum*, el concepto de Product Backlog:

> *"[…] La Lista de Producto es una lista ordenada de todo lo que se conoce que es necesario en el producto. Es la única fuente de requisitos para cualquier cambio a realizarse en el producto."*

El *Ciclo de Scrum* destaca la naturaleza de Scrum y su forma de trabajo. En la tercera edición del libro de *Scrum SBOK de SRUMstudy*, se explora su importancia:

> *"[…] El ciclo de Scrum empieza con una reunión de stakeholders, durante la cual se crea la visión del proyecto. Después, el Product Owner desarrolla una Backlog Priorizado del Producto que contiene una lista requerimientos del negocio y del proyecto por orden de importancia en forma de una historia de usuario."* (SCRUMstudy, 2017)

2.6.5. Planificación de liberaciones o sprints

Según el portal especializado *MuyAgile.com* la clave en la planificación se encuentra en el Backlog. En ese portal se afirma lo siguiente:

> *"[…] Todas las entradas dentro del Product Backlog deben estimarse de acuerdo con la definición acordada (por ejemplo, puntos de historia). Esta estimación se puede utilizar para priorizar las entradas del Backlog y para planear las entregas (releases)."* (MUYAGILE, 2021)

Este portal nos menciona, además, que el backlog es iterativo, dinámico y cambia en el tiempo.

Si toma en consideración la *Guía del PMBOK, Sexta edición* disponemos de una propuesta de planificación ágil de liberaciones (Release Planning):

> *"[…] La planificación ágil de liberaciones proporciona una línea de tiempo resumida de alto nivel del cronograma de liberación (normalmente 3 a 6 meses) en base a la hoja de ruta del producto y la visión de producto para su evolución. La planificación ágil de liberaciones también determina la cantidad de*

iteraciones o sprints de la liberación, y permite al responsable del producto y al equipo decidir cuánto es necesario desarrollar y cuánto tiempo insumirá tener un producto liberable sobre la base de las metas, dependencias e impedimentos del negocio." (PMI, 2017a)

2.6.6. Mapeo de Historias (Visual Story Mapping)

Según el SBOK, la técnica de mapeo de historias o Story Mapping se describe como sigue:

"[…] El mapeo de historias, conocido en inglés como Story Mapping, es una técnica para proporcionar un esquema visual del producto y sus componentes clave." (SCRUMstudy, 2017).

Mayor profundidad de esta técnica la encontramos en el libro *Proyectos Ágiles con Scrum* detallando los niveles de jerarquía:

*"[…] La teoría del Visual Story Mapping comienza en un nivel "humano" identificando los Objetivos que toda persona persigue y dividiéndolos en actividades para las cuales deben utilizarse Herramientas, resultando entonces en una jerarquía de Objetivos → Actividades → Herramientas"(*Alaimo D.M, 2013).

2.7.Análisis de costo – beneficio en CiberSeguridad.

Un análisis de costo beneficio es requerido para una correcta justificación financiera. Para ello, es necesario calcular la rentabilidad de un proyecto o adquisición mediante la comparación de sus costos con los beneficios. El ROI se calcula de la siguiente manera: *ROI = (Ingresos-Inversión)/Inversión x 100.*

Pero si hablamos de seguridad, disponemos del concepto de ROSI (Return on Security Investment). Es un concepto utilizado a nivel de gestión de la seguridad para justificar la implementación de sistemas que mitigan riesgos. El ROSI es un indicador financiero derivado del ROI. El cálculo se realizaría con la siguiente fórmula (ORMELLA, 2011): ROSI = *(Valor – Costo) / Costo.*

Una segunda propuesta de ROSI podemos encontrarlo en el modelo de Sonnenreich, Albanese y Stout (Sonnenreich, W, 2006). En su artículo publicado los autores

proponen una medición utilizando las variables de exposición al riego, porcentaje de riesgo mitigado y el costo de la solución. Considerando esta fuente, el cálculo se realizaría con la siguiente fórmula:

ROSI= ((Exposición al riesgo x % Riesgo Mitigado)-Costo de la solución)/(Costo de la Solución) x 100

2.8.Marcos, controles e iniciativas similares en Ciberseguridad.

2.8.1. Defensa en profundidad: Los 20 Controles CIS y Mejores prácticas CIS.

El CIS (*Center of Internet Security)* define sus propios controles como un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes *(CIS, 2019).* Las mejores prácticas de seguridad de CIS, que incluyen los controles de CIS y Benchmark CIS, son más que una lista de verificación de *"cosas buenas que hacer" o "cosas que podrían ayudar"*; en vez de ello, son un conjunto de acciones prescriptivas, priorizadas y altamente enfocadas que tienen una comunidad de apoyo para hacerlas implementables, utilizables, escalables y alineadas con todos los requisitos de seguridad gubernamentales o de la industria.

Son agrupados y desarrollados en Grupos de Implementación o IG. Los IG son categorías autoevaluadas para organizaciones basadas en atributos de ciberseguridad relevantes. Estos IG representan un corte horizontal a través de los controles CIS.

Grupo de implementación 1 (IG1): Sugerido para SOHOs, pequeñas y medianas empresas con equipos de TI y de Ciberseguridad limitado conocimiento o tiempo reducido. La sensibilidad de la información es baja y tiene una tolerancia a la indisponibilidad de sus servicios.

Grupo de implementación 2 (IG2): Tiene personal responsable y dedicado en administrar y proteger la infraestructura de TI. Pueden ser también pequeñas empresas, pero en obligación de cumplimiento normativo. Almacenan y procesan información confidencial de clientes o empresas y pueden soportar breves interrupciones del servicio.

Grupo de implementación 3 (IG3): Emplea expertos en seguridad que se especializan en las diferentes facetas de la ciberseguridad (gestión de riesgos, pruebas de penetración, seguridad de aplicaciones). Los sistemas y datos contienen información o funciones sensibles que están sujetas a supervisión regulatoria y de cumplimiento

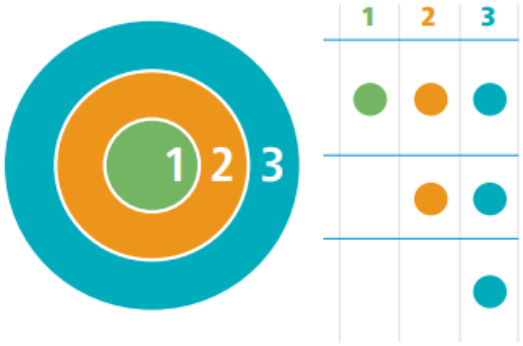


Figura 2. Grupos de implementación de los CIS Controls

Nota. Obtenido del documento "CIS Controls V 7.1 del ***Center*** *for Internet Security", 2019*

Para mayor detalle y conocer todos los controles CIS revisar la sección anexos. *Ver anexo F: Tabla de Controles CIS y grupos de implementación*

2.8.2. Marco de ciberseguridad NIST

Según la documentación oficial de la certificación Lead Cybersecurity Professional Certificate - LCSPC (Certiprof, 2019a), el marco NIST es un enfoque basado en el riesgo para gestionar el riesgo de ciberseguridad, y se compone de tres partes: El núcleo del marco, los niveles de implementación del marco y los perfiles del marco. Cada componente del marco refuerza la conexión entre los impulsores de negocio, la misión y las actividades de ciberseguridad.

- El Núcleo del Marco, es un conjunto de actividades de seguridad cibernética, resultados deseados y referencias aplicables que son comunes en todos los sectores de infraestructura crítica. El Núcleo del Marco consta de cinco Funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar.
- Los niveles de implementación del marco, proporcionan un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo. Los Niveles describen el grado en que

las prácticas de gestión de riesgos de seguridad cibernética de una organización exhiben las características definidas en el Marco (por ejemplo, consciente de los riesgos y amenazas, repetibles y adaptables). Los Niveles caracterizan las prácticas de una organización en un rango, desde *Parcial* hasta *Adaptable*.

N	TIPO	PROCESO DE GESTIÓN DE RIESGOS	GESTIÓN INTEGRADA DE RIESGOS	PARTICIPACIÓN EXTERNA
1	PARCIAL	Prácticas informales de riesgo, reactivo, enfoque de riesgo ad hoc	Conciencia institucional limitada. Gestión de riesgos en su lugar, pero irregular.	Carece de procesos para coordinar y colaborar
2	RIESGO INFORMADO	Práctica de gestión de riesgos aprobada, pero no en toda la organización. Prioridades informadas por las partes interesadas.	La organización tiene conciencia del riesgo de ciberseguridad, pero aún no tiene un enfoque institucionalizado	La organización no ha formalizado las capacidades
3	REPETIBLE	Prácticas de gestión de riesgos aprobadas formalmente, expresadas como políticas actualizadas regularmente	Enfoque de toda la organización para gestionar el riesgo. Las políticas, procesos y procedimientos sobre el riesgo se definen e implementan según lo previsto.	La organización comprende las dependencias y los socios reciben información que permite las decisiones de respuesta basadas en el riesgo
4	ADAPTATIVO	Se adapta según las lecciones aprendidas. Mejora continua, respuesta oportuna	Enfoque de riesgo organizacional con conciencia situacional integrada en la cultura	Comparte activamente con socios para aprender y beneficiar a la comunidad de manera proactiva

Tabla 1. Los cuatro niveles de implementación del marco

Nota. Adaptado del libro "Lead Cybersecurity Professional Certificate", por Certiprof LLC, 2019.

- Los perfiles del marco, se puede caracterizar como la alineación de estándares, directrices y prácticas con el núcleo del marco en un escenario de implementación particular. El análisis de brechas permite a las organizaciones crear una hoja de ruta priorizada.

FUNCIÓN	CATEGORÍA CIBERSEGURIDAD NIST	N1	N2	N3	N4
IDENTIFY (ID)	Asset Management (ID.AM)			X	
	Business Environment (ID.BE)		X		
	Governance (ID.GV)	X			
	Risk Assessment (ID.RA)				
	Risk Management Strategy (ID.RM)				
	Supply Chain Risk Management (ID.SC)				
PROTECT (PR)	Access Control (PR.AC)				
	Awareness and Training (PR.AT)				
	Data Security (PR.DS)				
	Information Protection Processes and Procedures (PR.IP)				
	Maintenance (PR.MA)				
	Protective Technology (PR.PT)				
DETECT (DE)	Anomalies and Events (DE.AE)				
	Security Continuous Monitoring (DE.CM)				
	Detection Processes (DE.DP)				
RESPOND (RS)	Response Planning (RS.RP)				
	Communications (RS.CO)				
	Analysis (RS.AN)				
	Mitigation (RS.MI):				
	Improvements (RS.IM):				
RECOVER (RC)	Recovery Planning (RC.RP)				
	Improvements (RC.IM)				
	Communications (RC.CO)				

Tabla 2. Las funciones del marco, sus categorías y niveles

Nota. Adaptada del libro "Lead Cybersecurity Professional Certificate", Certiprof LLC, 2019.

2.8.3. Modelo de amenazas STRIDE

El modelado de amenazas es una técnica de comprobación cuyo objetivo es ayudar a identificar y planificar de forma correcta, la mejor manera de mitigar las amenazas de una aplicación mediante un enfoque moderno de análisis de gestión de riesgos, y la implementación de medidas o controles que contribuyan a mejorar la seguridad. (Barba Olivares G.E., 2017)

STRIDE es un modelo de amenazas de seguridad informática, es el acrónimo de "Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege". El modelo de amenazas STRIDE se encuentra dividido en 6 categorías con sus correspondientes contramedidas.

CATEG	CONTRA MEDIDA	DESCRIPCIÓN
Spoofing	Autenticidad	Suplantación de identidad de usuario. Conjunto de técnicas que buscan un compromiso de la gestión de identidad, autenticación y autenticidad.
Tampering	Integridad	Manipulación no autorizada. Motivación de afectar a la integridad de los elementos del sistema, modificándolo de manera maliciosa.
Repudiation	No repudio	Cualidad de un sistema que permite tener certeza y validez sobre la demostración de autoría en una determinada acción.
Information disclosure	Confidencialidad	Exposición de información. Brecha o fuga de información de clasificación interna o superior de la organización.
Denial of service	Disponibilidad	Denegación de servicio. Ataques que buscan afectar la capacidad del sistema para ofrecer servicio de forma temporal o indefinida.
Elevation of privilege	Autorización	Escalada de privilegios. Motivación de realizar acciones para las que un usuario no está autorizado originalmente.

Tabla 3. Categorías de STRIDE y contramedidas

Nota. Tabla adaptada de categorías y contramedidas de STRIDE, artículo del portal Auditoriacodigo.com, publicado el año 2019. https://auditoriadecodigo.com/modelo-de-amenazas-stride-y-modelo-de-evaluacion-de-riesgos-dread/

2.8.4. ACAP o Plan de acción de ciberseguridad ágil

El Agile Cybersecurity Action Planning (ACAP) o Plan de acción de Ciberseguridad (John & Jo Link, 2015) platea un modelo de cultura de seguridad adaptativa al entorno de cambio y más flexible a la innovación. Utiliza los conceptos de metodologías ágiles, planificación estratégica adaptativa, mejora de procesos y gestión de riesgos. Del Flujo ACAP y sus etapas identifican y definen una estrategia de Ciberseguridad, las prioridades de activos a proteger y los parámetros de su desempeño.

N	ENTREGABLES ACAP
5.1	Defined Cybersecurity Vision & Mission Deliverable
5.2	Identified Cybersecurity Protection Priorities & Performance Parameters Deliverable
5.3	Baseline Cybersecurity Risk and Threat Profile Deliverable
5.4	Cybersecurity Policy Review and UpdateDeliverable
5.5	Cybersecurity Technology Update and Acquisition Strategy Deliverable
5.6	Cybersecurity Continuous Monitoring Plan Update Deliverable
5.7	Cybersecurity Response, Remediation and Continuity of Operations (COOP) StrategyDeliverable
5.8	Cybersecurity Staff Assessment and Staffing PlanDeliverable
5.9	Cybersecurity Knowledge Management PlanDeliverable
5.10	ACAP Implementation and Action Plan & Funding Request

Tabla 4. Tabla de entregables ACAP

Nota. Tabla obtenida del artículo *"Creating an Adaptive Cybersecurity Culture Through the Agile Cybersecurity Action Plan - ACAP"*, de VolvoXinc, por John W. Link & Jo Lee Loveland Link, 2015.

Tener en consideración que el Plan ACAP, sería el documento existente más cercano y similar a la presente investigación desarrollada por este autor. Sin embargo, es un artículo que propone indicaciones generales sin mayores especificaciones de que pasos a seguir o cómo podría implementarse. Aun así, es de alta relevancia y será utilizado en la propuesta de alineamiento en la integración de conceptos de ciberseguridad ágil.

III. DESARROLLO DE LA INVESTIGACIÓN: PROGRAMA DE CIBERSEGURIDAD ÁGIL

3.1.Presentación de un Programa de Ciberseguridad aplicando filosofía ágil

En esta sección se realiza la propuesta general de cómo utilizar principios de agilidad en un programa de ciberseguridad.

Al desplegar un programa de ciberseguridad, al tener una naturaleza temporal, con un inicio, un fin y con un resultado concreto, sería considerado como un proyecto. A pesar de ello, luego de ser entregado al área responsable de su monitoreo, dejará de considerarse un proyecto, para que sea calificado como un programa, que no sería más que un proceso continuo dentro de la operación en la organización. Es la forma correcta de cómo debe afrontarse la ciberseguridad dentro de una empresa, como un proceso y no como un producto. Para la propuesta de diseño del programa ciberseguridad, se utilizará como herramienta principal uno de los principales artefactos que es independiente a la metodología o marco de trabajo ágil. Nos referimos a la *historia de usuario*.

La *historia de usuario* sería el equivalente a los requisitos funcionales de un producto, que serían a su vez los requisitos por implementar según las capacidades de seguridad solicitadas en nuestro programa de ciberseguridad. Cuando una historia de usuario no es posible realizarse en tiempo y esfuerzo en un único sprint es agrupado en entidades de mayor tamaño llamado *Épicas* y estos a su vez agrupados en *Temas*. Estos niveles superiores llamado *Épicas*, calzan en perfecto alineamiento para la agrupación de los controles de seguridad CIS (ver 2.8.1). La utilización de las *Épicas* e *Historias de Usuarios* se visualizarán de forma concreta en el documento de planificación de liberaciones o sprints para el programa de ciberseguridad. Otra herramienta esencial por utilizar en el diseño sería el Product Backlog, un artefacto dinámico que contiene todos los requerimientos del cliente en un instante del tiempo. Adicionalmente, según la PMBOK, cuando utilizamos estos conceptos adaptativos podemos utilizar métricas de seguimiento y de cumplimiento. Entre ellos se encuentran el Diagrama de Flujo Acumulado (FDA) y el Diagrama Burn-up, que permite visualizar la evolución y el avance del trabajo del equipo.

Luego de describir de forma resumida la aplicación de artefactos ágiles, a continuación, se describirán diferentes propuestas adicionales de integración:

- Como primera herramienta propuesta es una matriz de autoevaluación e identificar si es aplicable la utilización de métodos ágiles.
- La segunda herramienta propuesta relaciona el diseño de un programa de ciberseguridad usando el *Modelo de Inteligencia de Seguridad* con algunos métodos ágiles que podrían aplicarse en el proceso de diseño y elaboración.
- La tercera herramienta propone, en formato de ejemplo, una tabla con el contenido de historias de usuario y el desglose a detalle en sus tareas.
- La última herramienta es la principal y unifica todos los conceptos. Alínea los niveles de agrupación de épicas e historias de usuario con la Inteligencia de Seguridad, Controles CIS y ACAP.

3.1.1. Herramienta de autoevaluación de complejidad del entorno

A continuación, se propone una herramienta de auto evaluación y de fácil aplicación.

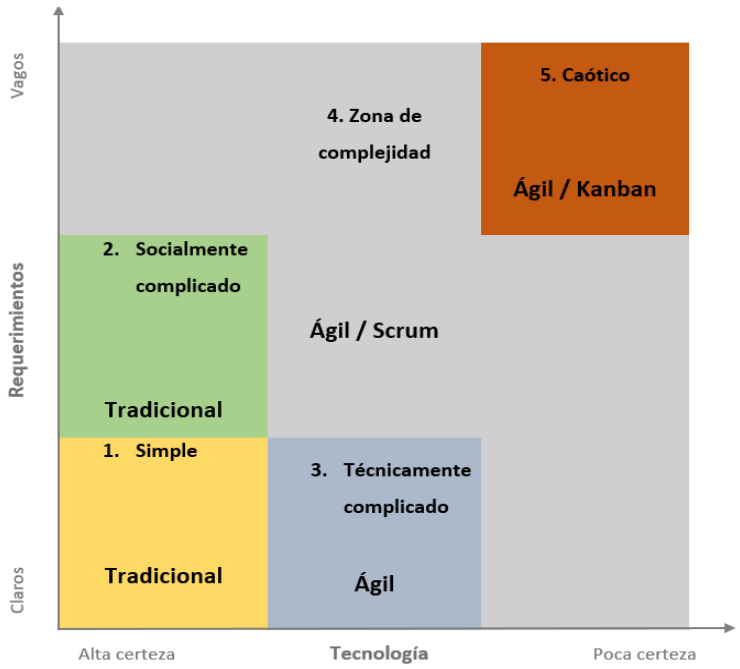


Figura 3. Matriz de Stacey

Nota. Adaptada de la matriz original de Ralph D. Stacey (Stacey, 2011)

Esta herramienta será de mucha utilidad para identificar si es que el entorno de la organización se encuentra en un entorno cambiante, con requerimientos vagos o de alta incertidumbre. O caso contrario, se encuentra en un entorno conocido, con requerimientos claros y con situaciones o eventos de alta certeza. El motivo principal de usar la matriz es que el enfoque ágil no es aplicable a por ejemplo entornos de alta certeza o de situaciones simples o baja complejidad. En ese escenario es mejor aplicar una metodología tradicional o un estándar internacional.

De esta matriz de puede desprender las siguientes preguntas de auto evaluación:

- Según la situación que actualmente se encuentra:
  - A nivel tecnológico y herramientas, ¿tiene poca o alta certeza? ¿son de simple o compleja aplicación?
  - A nivel de requerimientos del negocio, ¿son vagos o muy claros?
- Identificar en qué cuadrante de la matriz se ubica, y con el resultado determinar si se encuentra en una zona tradicional y simple, en una zona complicada, compleja o caótica.
- Decidir, por último, si es necesario la aplicación de métodos o marcos ágiles en el diseño de su programa de ciberseguridad para su empresa u organización.

3.1.2. Programa de Ciberseguridad y aplicación de métodos ágiles

Según el modelo de Inteligencia de Seguridad, en la capa de negocio se determina cuáles son las necesidades de seguridad en la empresa y su nivel de urgencia. Es posible aplicar un enfoque ágil en este nivel ya que conserva la esencia de varios de los doce (12) principios. En este caso, se hace énfasis sobre el enfoque al cliente y sus necesidades, así como la participación del mismo cliente en el equipo de trabajo.

La capa de inteligencia determina los activos críticos por proteger y su uso aceptable de ellos. En posible aplicar Scrum en el inicio de la construcción del Product Backlog que contiene los requerimientos necesarios. Cabe mencionar, que al delimitar los activos críticos estamos indirectamente construyendo nuestro producto mínimo viable o MVP. Todos estos requerimientos pueden

expresarse en formato de historias de usuario, que expresan un mayor entendimiento y conserva el principio ágil de simplicidad.

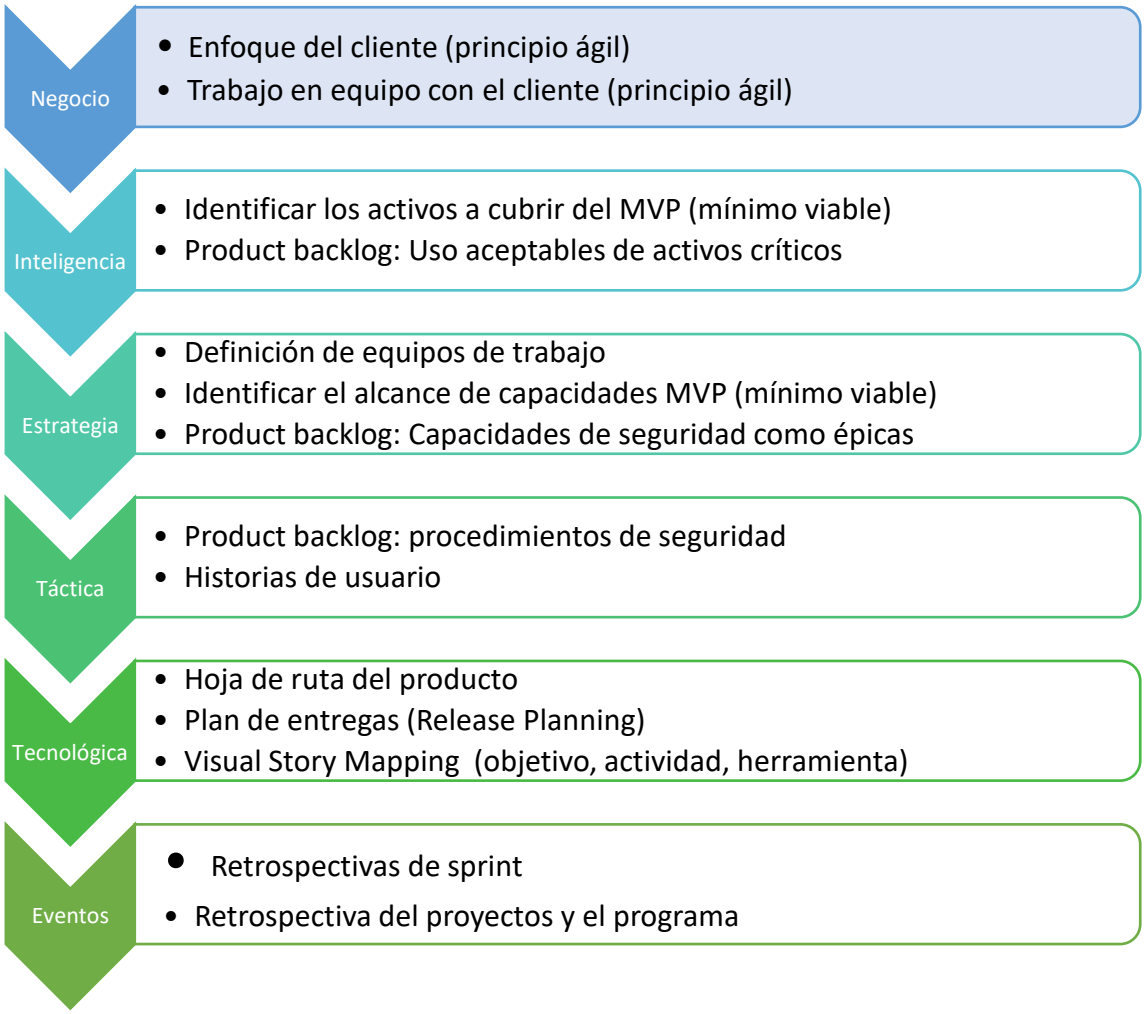


Figura 4. Programa de ciberseguridad y métodos ágiles

Elaboración Propia

En la capa táctica, se determina los procedimientos de seguridad cubriendo las siguientes áreas tácticas: gestión de aplicaciones, gobierno y políticas, priorización de eventos, gestión de incidentes, informes y analítica. Esta capa táctica nos ayudará a detallar los requerimientos a mayor profundidad descritas en las historias de usuario y a disponer una primera estimación de tiempo. Pero a su vez, también sería parte del plan de entregas, debido a que los procesos y procedimientos de seguridad serían parte de estos entregables de los primeros sprints del plan.

En la capa de tecnología se implementa las herramientas según las necesidades del negocio. Aquí se propone la aplicación de un Visual Story Mapping y el Release Planning. La primera técnica puede utilizarse para realizar una trazabilidad desde la necesidad, el objetivo, la actividad o procedimiento y la herramienta a implementar. Así mismo, es altamente probable que la capa tecnológica cubra gran parte de los entregables de programa de ciberseguridad. Por lo tanto, es el momento adecuado de construir el Plan de Entregas (Release Planning) divididos en sprints según el marco Scrum.

La capa de eventos son todos los eventos que ocurren en la organización. Por lo tanto, dentro de la programación de entregas de los sprints debe considerarse las capacidades de identificar y categorizar los eventos de seguridad. Por último, esta última capa nos puede brindar una retroalimentación de mejora continua, como controles de seguridad que posiblemente no hemos considerado en el programa inicial o corrección sobre los procedimientos o afinamiento de configuración en las herramientas tecnológicas implementadas.

3.1.3. Historias de usuario para la ciberseguridad

En esta sección se realiza una propuesta de historias de usuario aplicado a ciberseguridad. Las historias de usuario son los requisitos descritos en primera persona por el mismo usuario que incluye sus necesidades y motivaciones de lo que solicita. La siguiente tabla se explora en formato de ejemplo:

ID	Como… (Rol)	Necesito… (Objetivo)	Para… (Motivación)	Criterios de aceptación
1	Gerente producto	El sitio web esté disponible ante ataques DDoS	Los clientes pueden realizar las compras y continúe brindando ingresos a la empresa	- Soporte ataques volumétricos de 10 Gbps o superior. - Panel de gestión y visualización.
2	Área Legal	Backups de clientes estén protegidos	Evitar responsabilidades relacionadas a brechas de datos.	- Backup cifrado con AES256. - Política de derecho a olvido aplicado.

Tabla 5. Historia de usuario y ciberseguridad

Elaboración Propia

Seguidamente, se desarrolla, en formato de ejemplo, la descomposición de una historia de usuario en tareas a trabajar por cada equipo o equipos de trabajo:

- Característica (Capacidad): Resiliencia ante ataques DDoS
- Historia de usuario: Como gerente de producto necesito que el sitio web esté disponible ante ataques DDoS, para que los clientes pueden realizar las compras y continúe brindando ingresos a la empresa.
- Tareas: Convocatoria y selección de solución de mitigación DDoS, Implementación de la capa de red, BGP, túneles y ruteo, etc.

3.1.4. Alineamiento de los modelos de ciberseguridad en épicas e historias de usuario.

En esta última sección, se realiza la unificación de todos los conceptos. Según esta herramienta se determina que, para nuestra planificación ágil, los niveles superiores sean las llamadas *Épicas* y las *historias de usuario* el detalle a desarrollar por el equipo de trabajo.

Con ello se aplicaría un alineamiento en los niveles de estratégico, táctico y tecnológico del modelo de *Inteligencia de Seguridad*, en la agrupación de controles y de sub-controles CIS.

La idea desarrollada a continuación es una simplificación audaz que brinda una comprensión general unificada para realizar la gestión del proyecto, el diseño del programa ciberseguridad o del seguimiento del avance de la implementación tecnológica.

En la figura a continuación (ver figura 5) se resume la propuesta de este alineamiento:

- Nivel Épica:
    - Capacidad de seguridad, Control CIS, ACAP entregable.

- Nivel Historia de usuario:
    - Procedimiento de seguridad, Tecnología de seguridad, Sub-Control CIS, Actividad ACAP.

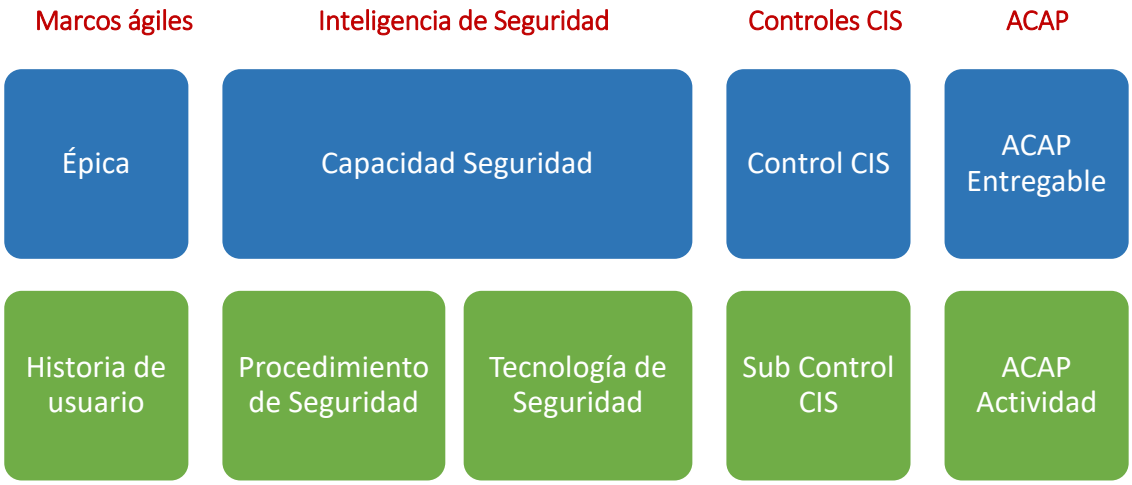


Figura 5. Alineamiento de Marcos de Ciberseguridad y Métodos ágiles

Elaboración Propia

3.2. Equipos de Trabajo y Planificación del programa de Ciberseguridad

3.2.1. Equipo de trabajo

En la siguiente tabla, se realiza una propuesta de identificación de los roles que define Scrum y los roles definidos en el Modelo de Inteligencia de Seguridad. Con ello utilizamos Scrum en el diseño de nuestro programa de ciberseguridad:

Roles del marco ágil Scrum	Roles del Security Intelligence
Interesados (Stakeholder)	Grupo de Gobierno
Dueño del producto	Delegado del grupo de gobierno
Scrum Máster	--
Equipo Scrum	Grupo de trabajo

Tabla 6. Roles Scrum y del Modelo de Inteligencia de Seguridad

Elaboración Propia

Por lo tanto, se propone que para el diseño del programa de ciberseguridad debe determinarse los siguientes roles clave:

- Grupo de Gobierno, el grupo de gobierno debe de encontrarse el principal patrocinador del proyecto, los tomadores de decisiones asociados al presupuesto y los líderes del proceso clave del negocio relacionados a los activos críticos identificados.

- Dueño de producto, el delegado del grupo de gobierno que se convertirá en el producto owner según el modelo de inteligencia de seguridad. Este rol debe disponer de capacidad técnica y de autonomía suficiente para definir las características detalladas de cada procedimiento y capacidad en seguridad.
- Equipo de desarrollo, serían los grupos de trabajo y estarían conformados usualmente por el área de seguridad, el área de TI y los proveedores especializados en la implementación.
- Scrum Máster, según scrum, es un guía y facilitador que apoya al equipo en todo momento, elimina impedimentos y hace que el ambiente de trabajo sea el adecuado. (Certiprof, 2019b)

3.2.2. Planificación del Diseño del programa de ciberseguridad en liberaciones

Con el apoyo del marco teórico del presente documento, procederemos a utilizar la herramienta de Planificación de Liberaciones (Release Planning). Si nos encontramos ante un proyecto de mediano o gran alcance sería necesario construir, además, una hoja de ruta del producto entre 3 a 6 meses, alineadas a su visión, según recomendaciones del PMI en su Guía Práctica de Ágil y el PMBOK. Para este entregable definiremos una planificación de liberaciones agrupado en versiones del producto en una línea de tiempo. La primera versión propuesta sería el MVP o Producto Mínimo Viable para el programa de ciberseguridad que se diseña.

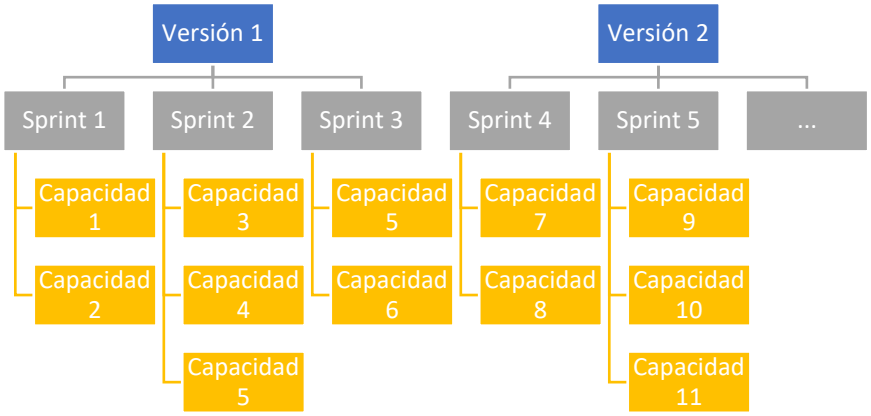


Figura 6. Modelo del plan de liberaciones

Elaboración Propia

3.3. Propuesta de controles tecnológicos por capas de seguridad

En el siguiente diagrama, este autor propone a nivel tecnológico, la seguridad en profundidad basada en capas. Iniciando desde la capa de protección en nube hasta la de seguridad en el mismo equipo final o host. En cada capa, se identifican controles de seguridad tecnológicos tanto de uso común y de índole muy especializados.

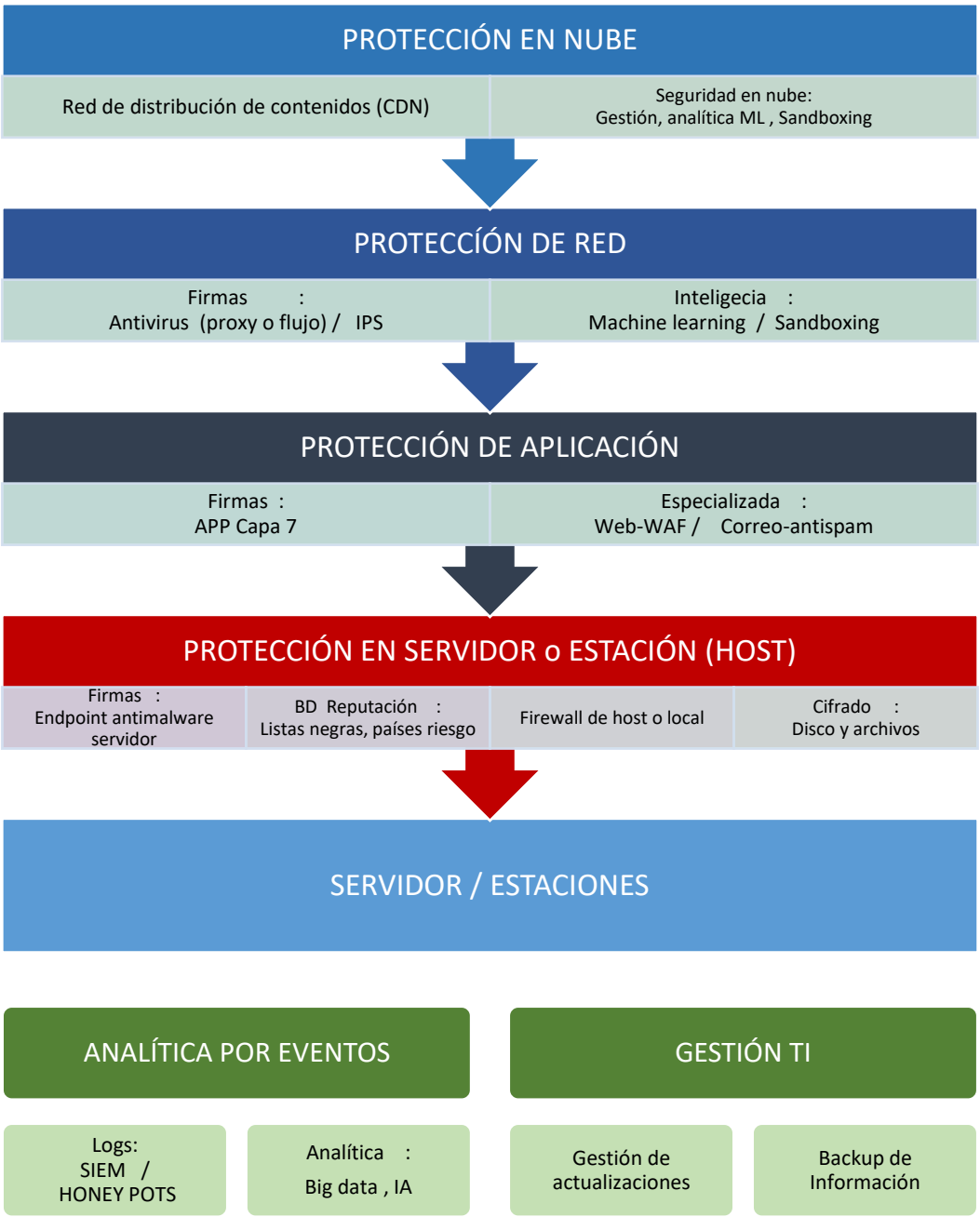


Figura 7. Protección tecnológica basada en capas

Elaboración Propia

Explicación por capas de seguridad tecnológica:

- Protección en nube
  - Red de distribución de contenidos (CDN): Es una red distribuida de servidores que aloja una copia del contenido, usualmente de un portal web, que permite generar mayor eficiencia en los tiempos de carga. También puede ser utilizado como mitigación contra ataques DDoS.
  - Seguridad en nube: los actuales proveedores de seguridad manejan una capa de gestión de analítica de datos en la nube cuya principal característica tecnológica es la utilización de técnicas como el *sandboxing* y el *machine learning*.

    El machine learning es una rama de la inteligencia artificial que a través de detección de patrones complejos, utilizando grandes volúmenes de datos (big data) y algoritmos de aprendizaje automático, para el caso de la ciberseguridad, permiten reconocer patrones de ataques cibernéticos, y con ello consiguen una alta detección y mitigación automática de la amenaza. El Sandboxing es un entorno aislado y controlado de simulación en diferentes entornos, que permite explotar y probar software potencialmente malicioso.

- Protección de red
  - Basado en firmas: este control de protección tradicional basada en firmas que serían los antivirus en red y un sistema de protección IPS. Aquí pueden utilizarse Firewall con funciones avanzadas de IPS y antivirus, o equipos de propósito específico de tipo IPS y/o de función antimalware.
  - Basado en inteligencia: este control de seguridad estaría basado en Machine Learning y Sandboxing. Serían las mismas definiciones explicadas en la capa de protección en nube.

- Protección en aplicación
  - Basado en firmas: este sería el control de protección basado en capa 7 o basado en firmas que detectan las aplicaciones en red. Los firewalls de capa 7 o firewalls de siguiente generación permiten detectar aplicaciones, y luego de ello relacionar una regla para permitir o bloquear el tráfico.
  - Especializada: esta capa usualmente está basada en proxy inverso, serían los controles de antispam especializado y protección web o WAF. El antispam

especializado, son soluciones a medida para protección de correo electrónico entrante y saliente. Por otro lado, el WAF o firewalls web, son soluciones a medida para protección de portales web, principalmente en el protocolo HTTP. Manejan capas basadas en firmas y basadas en inteligencia.

- Protección en servidor o estación (Host)
  - Basado en firmas: serían los antivirus o antimalware locales que se encuentran instalados en los servidores o estación.
  - BD de reputación: aquí se encuentran las bases de datos de reputación, en el cual podríamos considerar las RBL o listas negras de spam, fuerza bruta, malware, lista de países, entre otros. El comportamiento y configuración de seguridad puede diferir según su origen y naturaleza de la empresa.
  - Firewall local: sería el control más básico y esencial. Permite ingreso o salida de tráfico de puertos de red. También existe el firewall especializado para permitir o bloquear aplicaciones.

- Analítica por eventos
  - Security Information and Event Management (SIEM) registra, captura y almacena todos los eventos, registros de auditoría y los logs de los equipos de red, de seguridad y de los propios dispositivos. Realiza además un análisis a través de la correlación de eventos y genera información de valor.
  - Honeypots o señuelos, es una herramienta que simula la exposición de un equipo servidor vulnerable. Es muy útil para conocer el origen de redes atacantes, conocer el nivel de exposición a las amenazas e identificar las formas de operación de los cibercriminales.

- Gestión TI
  - Gestión de actualizaciones o parches, es un control fundamental en nuestro ecosistema tecnológico de protección. Permite mantener actualizado los equipos ante ataques cibernéticos que exploten vulnerabilidades de seguridad y evitar en la medida de lo posible la vulneración de nuestros sistemas.
  - Los Backups o respaldo de información, permite recuperar los datos en un punto anterior del tiempo, ante cualquier contingencia que ocurra en nuestros equipos.

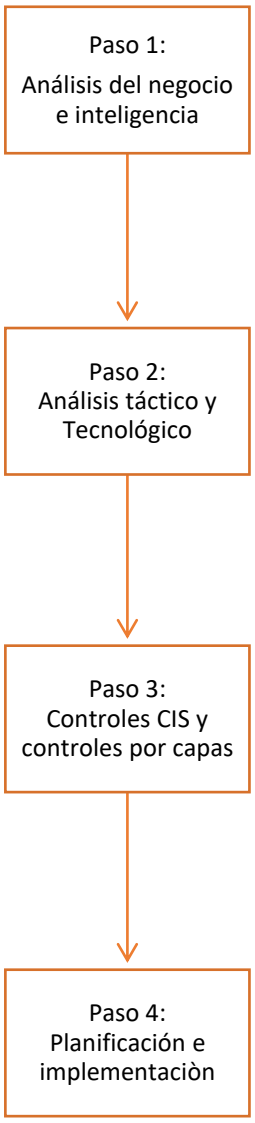
3.4. Implementación: Caso de aplicación

3.4.1. Resumen y explicación esquemática del desarrollo del caso

A continuación, se realiza una explicación resumida de cómo se aborda el caso y se aplican las herramientas propuestas como artefactos en el desarrollo de un programa de ciberseguridad ágil. Antes de comenzar, es necesario evaluar si es aplicable o no, un modelo ágil para la problemática en nuestra organización.

El caso de la empresa ABC fue seleccionado por principal interés debido a que según la evaluación con la Matriz de Stacey (Ver 3.1.1) esta organización se encuentra en un entorno de incertidumbre y de cambio constante.

El primer paso, es analizar el negocio donde se evalúa los objetivos estratégicos de la organización y cuáles serían los activos digitales más importantes a proteger. Con todo ello se alinea los objetivos de seguridad organizacional. La capa de inteligencia define los activos críticos y sus riesgos y las capacidades de seguridad a alcanzar.

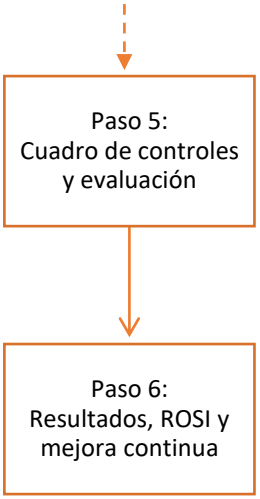


Como paso dos, se desarrollan los procedimientos de seguridad (táctico) y las tecnologías a implementar (tecnológico). Todas asociadas a cada capacidad de seguridad obtenida del paso 1. Las capacidades son Épicas, los procedimientos y tecnologías son Historias de Usuario dentro del MVP (Ver 3.4.3).

Como paso tres, se determina un perfil objetivo de controles de seguridad CIS (Ver 2.8.1) y los controles tecnológicos por capas (Ver 3.3). Para el caso de aplicación se determinó alcanzar los primeros 6 controles mínimos CIS en el nivel IG1. Se agrega al backlog del MVP como *Épicas e Historias de Usuario* (Ver 3.4.4).

Como paso cuatro, se realiza la planificación usando artefactos ágiles. Para el caso de aplicación se han utilizado el User Story Map y el Product RoadMap. Con todo ello, se implementa las Historias de Usuario descritas en el paso uno, dos y tres (Ver 3.4.5)

Como paso cinco, la herramienta más útil dentro de un programa de ciberseguridad podría considerarse el Cuadro de Controles de Seguridad. Este cuadro nos sirve para realizar un seguimiento del avance, del progreso y el monitoreo constante (Ver 3.5 y 3.6.1).



Como último paso, se realizan proyecciones y se analizan los resultados. Se calcula el ROSI o ROI de seguridad. Cabe mencionar es momento oportuno para realizar una retroalimentación y definir los siguientes pasos de la mejora continua. (Ver 3.6.4)

3.4.2. La empresa ABC

La empresa ABC, es una empresa peruana dedicada a brindar servicios de telecomunicaciones y de valor agregado por Internet. Se creó en el año 2008 e inició operaciones en el año 2009. Su visión es liderar la creación de valor e identidad para sus clientes. Y como misión busca es brindar identidad y competitividad mediante soluciones creativas e innovadoras, inspiradas en las necesidades de las personas y las empresas. Cuenta con dos unidades estratégicas de negocio; la de empresas y la de "en línea", cada una de ellas cuenta con una cartera de clientes y con un modelo de negocio específico. El modelo la unidad "en línea" de la empresa ABC, es la unidad de negocio que atiende al mercado masivo y permite a sus clientes, de forma sencilla y segura, adquirir y gestionar productos sobre Internet, lo que contribuirá al desarrollo de sus negocios o emprendimientos. Los productos y servicios que vende son los siguientes: alojamiento web, de correo y dominios. El portal, que denominaremos, abc.pe cuenta con un único medio de venta, su portal web. A través de esta interfaz los clientes acceden a la oferta, realizan la selección de los productos y tienen la opción de pagarlos por pasarelas de pago. Entre los activos relevantes de esta unidad de negocio podemos encontrar el portal web de venta y los mismos servidores de alojamiento web, donde se almacena y resguarda la información de clientes.

El Web Hosting es un servicio en el que un proveedor ofrece el alojamiento de sitios web de comercio electrónico de empresa a consumidor (B2C). Se utilizan servidores y aplicaciones compartidos o dedicados de propiedad del vendedor y controladas

desde las instalaciones del proveedor. El proveedor de Hosting es responsable de todas las operaciones diarias y el mantenimiento. El cliente es responsable del contenido. Un sitio web (Website) hace referencia a una colección de archivos a los que se accede a través de una dirección web, que cubre un tema o temas en particular y que son administrados por una persona u organización. Mientras que un Nombre de Dominio (Domain Name) es un identificador único para un sitio de Internet que consta de al menos dos segmentos separados por puntos (GARTNER, 2022). El alcance del programa de ciberseguridad para el caso es solo aplicable a la unidad de negocio en línea y ha sido desplegado el año 2021.

3.4.3. Aplicación del modelo de Inteligencia de Seguridad

Caso de aplicación: Capa de Negocio

La situación actual del negocio se obtuvo del documento del plan estratégico y de las reuniones con la gerencia general o delegado asignado. En ella, se determinaría los puntos principales relacionados a la seguridad por parte del negocio. Aquí se propuso una dinámica simple que consta de pregunta y respuesta que fueron mencionadas en reunión.

Anexo A. Cuestionario de la capa de negocio del caso de aplicación.

Del plan estratégico se reconocieron los siguientes objetivos estratégicos para la empresa ABC, como meta para el año 2025:

- Alcanzar 300 mil clientes en la región
- Lograr situarse en el “top of mind” del consumidor latinoamericano.

Por ende, según las entrevistas y los objetivos estratégicos, se puede deducir que la reputación e imagen en el rubro en la región latinoamericana será de gran importancia en los siguientes 3 años. El activo más importante, sería la información de clientes. Éstas deben de mantenerse en línea el mayor tiempo posible con el máximo aceptable de 2 horas en una situación crítica y extrema. En el caso del portal web de venta, la gerencia solicita evitar verse afectado por alguna intrusión o alguna caída de larga duración, con ello, la imagen no se vería mermada.
Estos serían los objetivos de Seguridad propuestos y acordados:

- Mantener la disponer de disponibilidad servicio a clientes superior al 99.9%
- Mantener la disponer del portal web en 99.9%, en un máximo de 2 horas
- Resguardar y proteger el portal web, contra las incidencias en brechas de seguridad al mínimo.

Caso de aplicación: Capa de Inteligencia

Se procede a establecer de forma clara los dos (2) activos críticos:

- Información del cliente : Servicio Alojamiento clientes
- Portal Web : Servicio de venta en línea

A continuación, se construye un árbol de activos y con ello determinar sus dependencias.

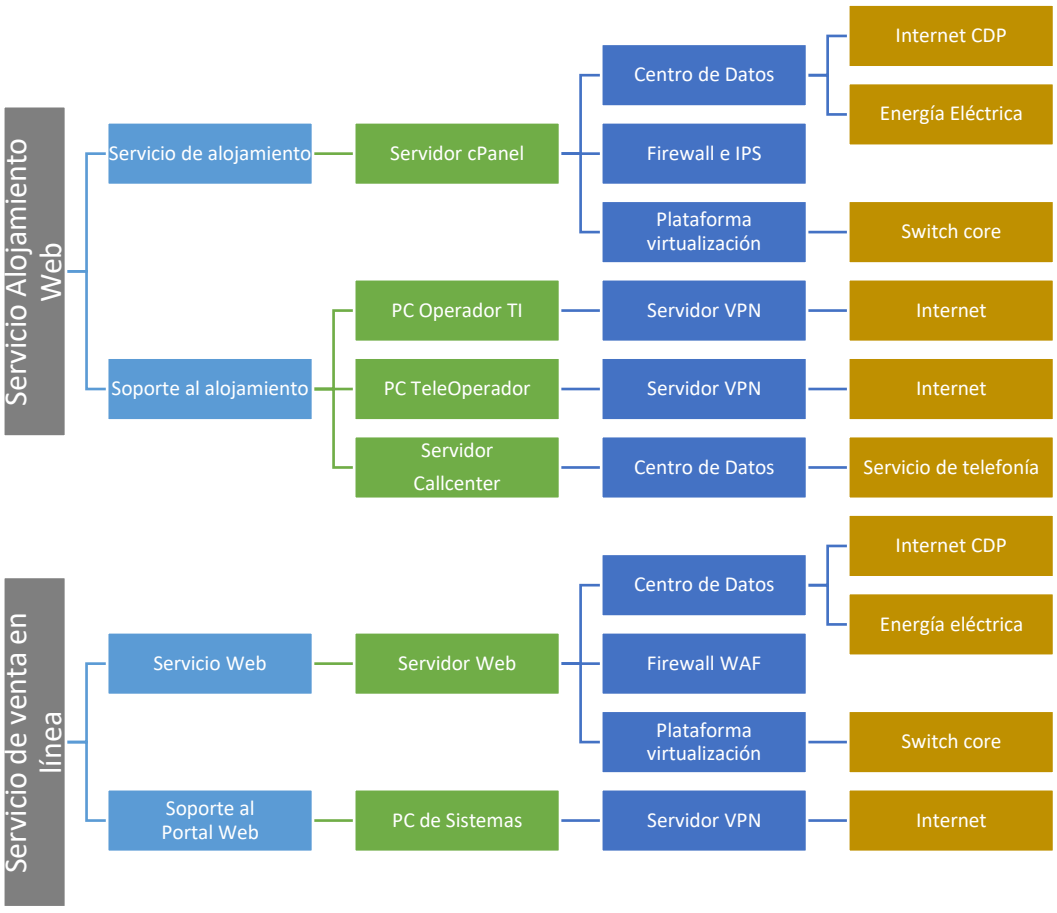


Figura 8. Árbol de Activos y dependencias

Elaboración Propia

De este diagrama anterior, podemos desglosar una nueva tabla de activos críticos con el cual vamos a trabajar en el programa de ciberseguridad. Notar que se han sombreado los activos principales y críticos.

N	ACTIVOS CRÍTICOS	CATEGORÍA
1	Información de clientes	Información
2	PC Sistemas	Hardware
3	PC Operador TI	Hardware
4	PC Teleoperador	Hardware
5	Servidor Web	Hardware
6	Servidor cPanel	Hardware
7	Servidor Callcenter	Hardware
8	Servidor VPN	Equipo de red
9	Firewall IPS	Equipo de red
10	Firewall WAF	Equipo de red
11	Switch Core	Equipo de red
12	Plataforma Virtualización	Software
13	Portal Web de venta	Software
14	cPanel	Software
15	Servicio de alojamiento Web	Proceso / Sistema
16	Servicio Venta en línea	Proceso / Sistema
17	Personal de CallCenter	Personal
18	Personal de Sistemas	Personal
19	Personal de TI	Personal
20	Servicio Telefonía	Servicio
21	Suministro Eléctrico	Servicio
22	Servicio de Internet CPD	Servicio
23	Centro de Datos Principal	Sitio

Tabla 7. Activos Críticos

Elaboración Propia

Caso de aplicación: Capa de estrategia

En primera instancia, esta etapa se determina los roles con sus responsabilidades y las capacidades de seguridad.

Según el modelo de Inteligencia, en esta etapa, además, se determina unos de los puntos fundamentales en nuestro programa de ciberseguridad que son las Capacidades de Seguridad. Esta primera propuesta de historias de usuario del Mínimo Viable (MVP) contendría las capacidades, pero a su vez deben alinearse a

las necesidades de seguridad que nos indica el negocio y a la protección de los activos críticos de Seguridad. Para mayor detalle ver los siguientes anexos:
Anexo B. Cuadro de roles de la capa de estrategia del caso de aplicación.
Anexo C. Cuadro de capacidades de seguridad del caso de aplicación.

Caso de aplicación: Capa Táctica

En esta sección se determinan los procedimientos técnicos. En este punto, nos encontramos con equivalencias específicas.

Una Épica o agrupación de Historia de Usuario sería una capacidad de Seguridad de la capa de estrategia. Un procedimiento técnico, sería una historia de usuario, que es a su vez requisito funcional del programa de ciberseguridad. El desarrollo completo de los procedimientos de seguridad para el caso práctico agrupado por Épicas (capacidades de seguridad), y categorizado por área táctica. Para mayores detalles del desarrollo ver el siguiente anexo:

Anexo D. Cuadro de procedimientos de seguridad e historias de usuario del caso de aplicación.

Caso de aplicación: Capa Tecnológica

Similar a la capa táctica, que se logra ubicar los procedimientos técnicos necesarios, en esta sección se determinan las tecnologías a implementar. De igual forma, una Épica o agrupación de Historia de Usuario sería una capacidad de Seguridad y una tecnología para implementar, sería una historia de usuario. Cabe señalar, es recomendable también que cada tecnología a implementar disponga de un procedimiento, si no se ubica alguno, tendría que crearse uno según sea necesario. Las tecnologías de seguridad podrían categorizarse en herramientas basadas en el contenido, en el contexto y las de monitoreo.

Este autor propone que todas las historias de usuario que implica procedimientos y tecnologías de seguridad, sea un único artefacto. Éste sería nuestro Product Backlog inicial para el MVP. Así mismo, se propone que el resultado final de este modelo no sólo debería considerar el Modelo de Inteligencia de Seguridad, sino también

utilizar las otras fuentes que serían la identificación del perfil objetivo a un nivel de implementación de los controles CIS y los controles tecnológicos que ya han sido propuestos. El cuadro a detalle que desarrolla las tecnologías a aplicar, se determinan en el siguiente anexo:
Anexo E. Cuadro de tecnologías e historias de usuario del caso de aplicación.

3.4.4. Establecer el perfil objetivo según nivel y grupo de implementación CIS.

Siguiendo con la aplicación de métodos ágiles en la empresa ABC, se prosigue con la utilización de los controles CIS, antes ya justificados, y luego definir un perfil objetivo según nivel de implementación del grupo de controles CIS.

Los controles más esenciales de *ciber higiene*, denominado y referidos por la misma organización CIS, son el subconjunto de los primeros seis (6) de su lista. Por consiguiente, el Producto Mínimo Viable (MVP) va a considerar los primeros 6 controles del grupo IG1. En los siguientes sprints, procederíamos a implementar los controles restantes de este mismo grupo CIS de implementación. En nuestra planificación de Product Roadmap consideraríamos, como objetivo a mediano plazo, para nuestro perfil de seguridad lograr cumplir los sub-controles del segundo grupo CIS de implementación o IG2.

Control crítico #1: Inventario y control de activos hardware				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**IG 1**
1.4	Equipos	Identificar	Mantener un inventario de activos detallado	X
1.6	Equipos	Responder	Gestionar los activos no autorizados	X
Control crítico #2: Inventario y control de activos software				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	
2.1	Aplicaciones	Identificar	Mantener un inventario de software autorizado	X
2.2	Aplicaciones	Identificar	Asegurar que el software tenga soporte del fabricante	X
2.6	Aplicaciones	Responder	Gestionar el software no aprobado	X

Control crítico #3: Gestión continua de vulnerabilidades				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	
3.4	Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches del sistema operativo	X
3.5	Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches de software	X
Control crítico #4: Uso controlado de privilegios administrativos				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	
4.2	Usuarios	Proteger	Cambiar contraseñas por defecto	X
4.3	Usuarios	Proteger	Asegurar el uso de cuentas administrativas dedicadas	X
Control crítico #5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	
5.1	Aplicaciones	Proteger	Establecer configuraciones seguras	X
Control crítico #6: Mantenimiento, monitoreo y análisis de logs de auditoría				
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	
6.2	Red	Detectar	Activar registros de auditoría	X

Tabla 8. Controles y sub-controles CIS del MVP

Nota. Elaboración Propia. Adaptado de los Controles y Sub-controles CIS.

3.4.5. Planificación del Producto y de Sprints.

En esta parte importante del diseño del programa de ciberseguridad, vamos a utilizar las herramientas: Product RoadMap y User Story Mapping, antes ya abordado y detallado a profundidad. Para el MVP, se ha considerado los 6 primeros controles CIS de ciber higiene, la identificación de activos críticos, las capacidades, procedimientos y tecnologías de seguridad enfocados para una pequeña empresa. Ante de proceder a la planificación, se debe tener en consideración las siguientes equivalencias en los niveles y jerarquías de agrupación de requisitos, para mayor detalle revisar la propuesta de alineamiento en el capítulo.

Product RoadMap, es una vista de planificación del producto de alto nivel. Debido a ello, se considerarán agregar las funcionalidades que serían las épicas para la perspectiva de Scrum.

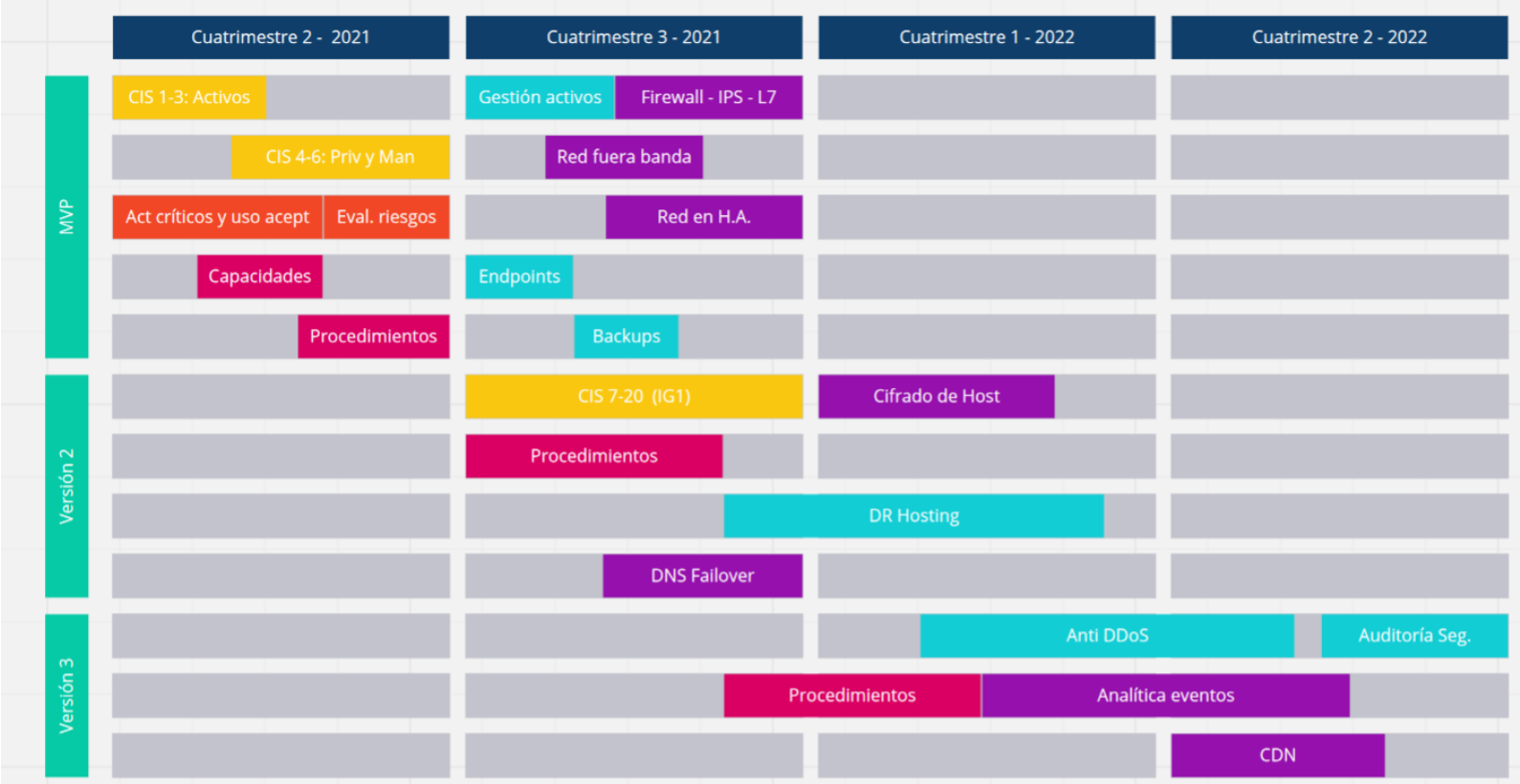
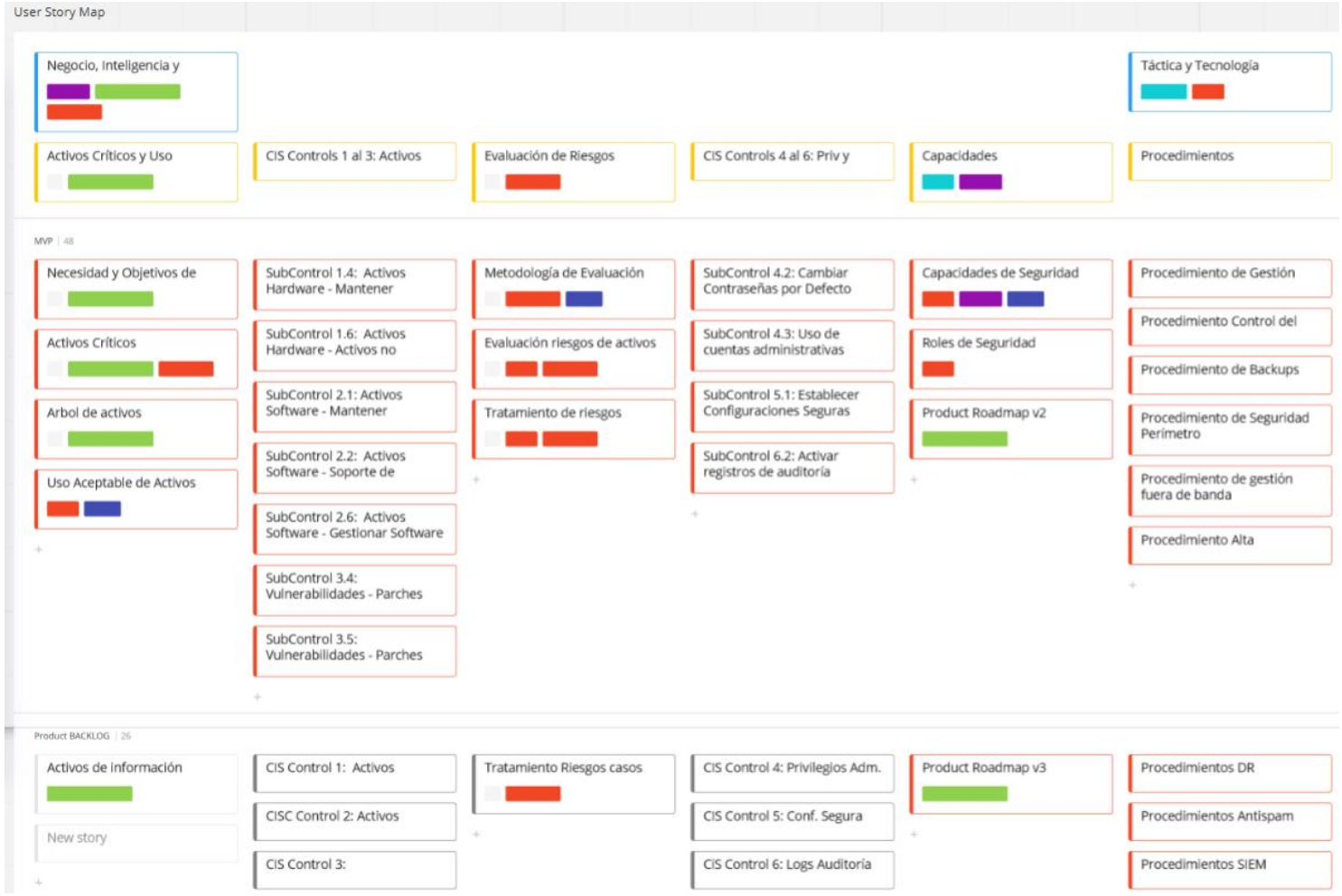


Figura 9. Product Roadmap del Diseño del Programa de Ciberseguridad

Nota. Elaboración propia. Nótese que el Anti DDoS no fue priorizado en esta planificación. Desarrollado en la aplicación Miro. https://miro.com

User Story Map, puede desarrollarse de forma más detallada desplegándose hasta la historia de usuario.



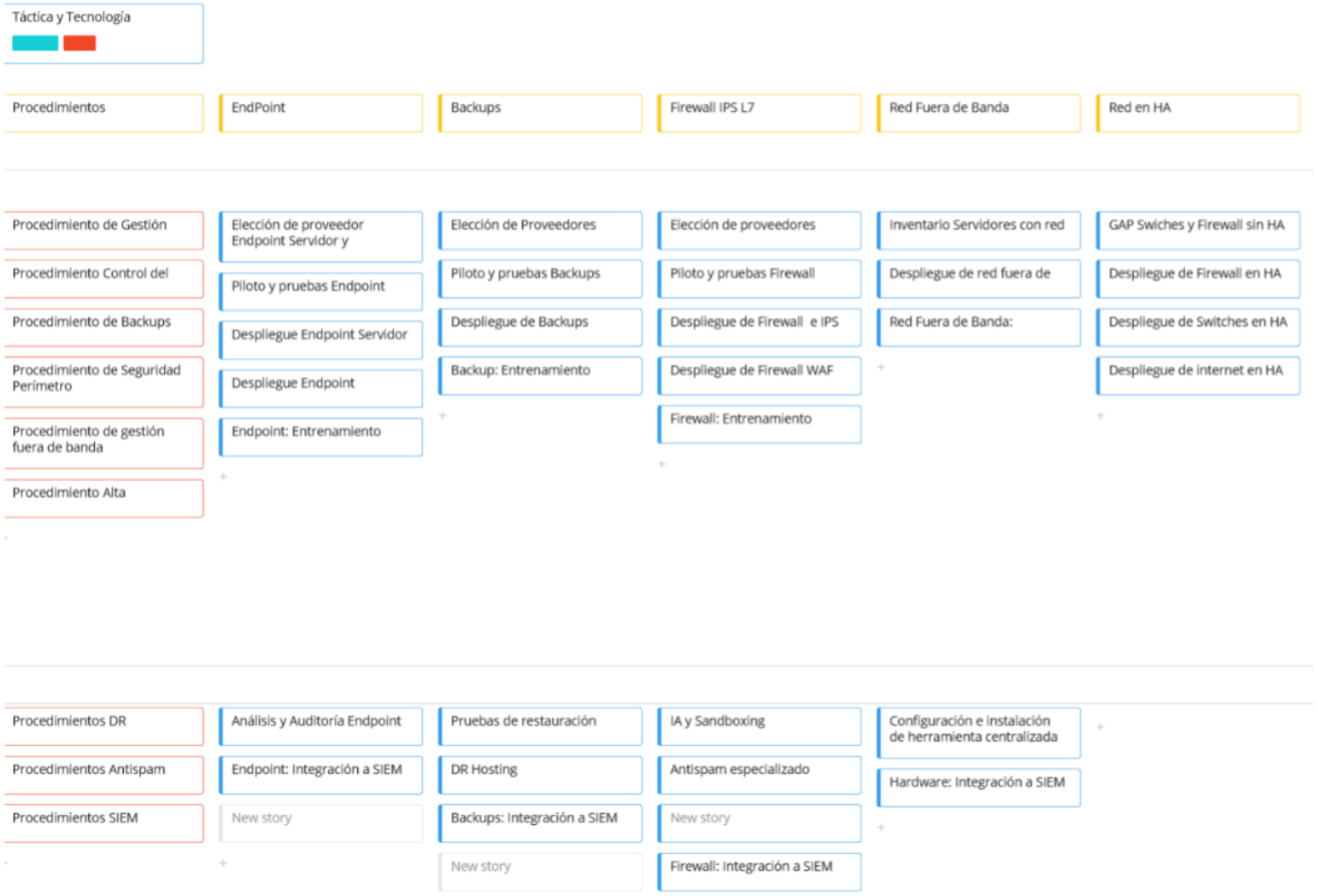


Figura 10. User Story Map del Diseño del Programa de Ciberseguridad (MVP)

Nota. Elaboración propia. Desarrollado en la aplicación Miro. https://miro.com

3.5. Cuadro de Controles de Seguridad por estado y por progreso

	CONTROL	CIS	MR	SPA	AVANCE	ESTADO
1	Inventario y control de activos hardware	CIS1	-	-	90%	
2	Inventario y control de activos software	CIS2	-	-	80%	
3	Gestión continua de vulnerabilidades	CIS3	-	SPA8	10%	
4	Uso controlado de privilegios administrativos	CIS4	-	-	50%	
5	Configuración segura para hardware y software en dispositivos	CIS5	-	-	50%	
6	Mantenimiento, monitoreo y análisis de logs de auditoría	CIS6	-	SPA9	50%	
7	Endpoint en servidores (Defensa contra malware)	CIS8	-	SPA1	10%	
8	Backups (Capacidad de recuperación de datos)	CIS10	-	SPA2	95%	
9	Firewall IPS L7 (Defensa de borde)	CIS12	-	SPA3	95%	
11	Equipos de red en HA	CIS12	-	SPA4	60%	
12	Protección anti DDoS	-	R1	SPA5	33%	
13	Respuesta ante incidentes y DR (DDoS y/o indisponibilidad)	CIS19	R2	SPA6	10%	

Tabla 9. Cuadro de controles de Seguridad por estado.

Nota. Elaboración propia. Las siglas CIS, MR y SPA, hace referencia a la procedencia de la fuente del control.

CIS: Procedencia de Controles CIS. MR: Procedencia de la matriz de riesgo y priorización del negocio. SPA: Procedencia de la Propuesta de Seguridad en pequeñas empresas

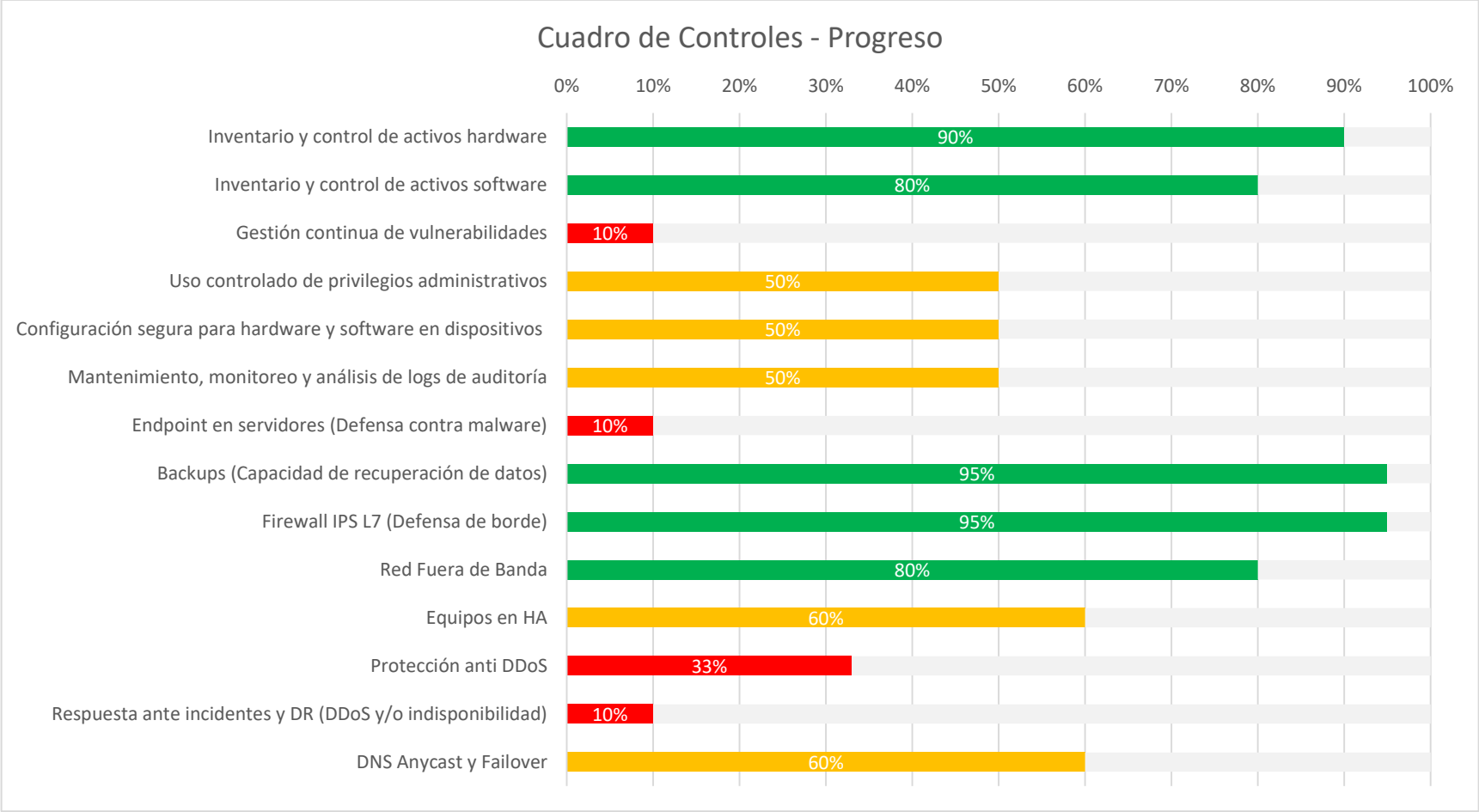


Figura 11. Cuadro de progreso de Controles de Seguridad

Nota. Elaboración Propia. El porcentaje indica el progreso de avance por control. Nótese en este cuadro ya se prioriza el Anti DDoS y los procedimientos de respuesta ante incidentes y DR

3.6.Resultados.

En esta sección se recopilarán los diferentes resultados logrados principalmente en el desenvolvimiento y ejecución del mínimo viable (MVP) del programa de ciberseguridad. Cabe mencionar, que ocurrieron sucesos inesperados, que no fueron considerados en la etapa inicial de la planificación como las siguientes:

- En las reuniones de necesidades del negocio y en la evaluación de riesgos, se encontró la necesidad de priorizar la capacidad de protección ante ataque DDoS que no se encontraba en el MVP. Fue agregado a la lista de actividades y entregables del Backlog del mínimo viable.
- En las reuniones de necesidades del negocio, se encontró la necesidad de priorizar una solución de Recuperación ante Desastres o DR. Se acordó además que, para el MVP, sólo abarcaría como alcance el servicio a clientes Cpanel, que es el aplicativo principal que brinda servicio a los clientes de la empresa. Además la solución de DR, se debería documentar un procedimiento de respuesta ante incidentes, con énfasis a ataque DDoS y caídas de red.
- Se observó que el programa de ciberseguridad no estaba siendo considerado dentro del plan estratégico. Se pudo hacer la corrección respetiva y se agregó a los OKR y metas del plan 2021 desde el cuatrimestre dos (2) del 2021. Al lograr ingresarlo al plan estratégico, se pudo evidenciar una considerable mejora del avance desde el mes de mayo.
- En el transcurso del año 2021 fue lanzado la nueva versión de los controles CIS, la versión 8.0. A pesar de ello, se decidió continuar con el uso de la versión 7.1 para el MVP del programa de ciberseguridad.

Para consolidar los resultados del caso práctico se ha generado los siguientes diagramas e indicadores:

- Velocidad del avance por ciclo de entrega (DFA)
  Mediante un Diagrama de Flujo Acumulado veremos la estabilidad del avance de los equipos de trabajo y la eficacia del trabajo.
- Proyección de tiempo para la finalización del MVP (DFA)

Utilizando el recurso de líneas de tendencia en el gráfico, podemos determinar la proyección de la finalización del MVP. En este caso, se utilizó tendencia lineal.

- Incidentes de Ciberseguridad por año, que determina la cantidad de incidentes según las amenazas usando el modelo STRIDE. Se evidenciará una reducción de eventos por infraestructura de red y un aumento en ataques DDoS.
- El retorno de inversión en seguridad o ROSI, de una solución implementada. Se aplicó en temporalidad mensual y para la solución Anti DDoS.

3.6.1. Velocidad del avance del trabajo por ciclo de entrega (DFA).

En el Backlog del MVP de disponen de un total 65 actividades para inicios de año, y en setiembre del año 2021, se disponía de 72 actividades por realizar. Entre las principales priorizadas y agregadas se encuentra la solución AntiDDoS. Cada sprint fue trabajado con una duración de 3 semanas y la semana adicional se repartió el tiempo en análisis, estimación de tiempo, retroalimentación de interesados y presentaciones internas de avances. Con ello, cada ciclo duró exactamente 1 mes. A continuación, se muestra el diagrama de flujo acumulado, notar la mejora del progreso desde el mes de mayo.

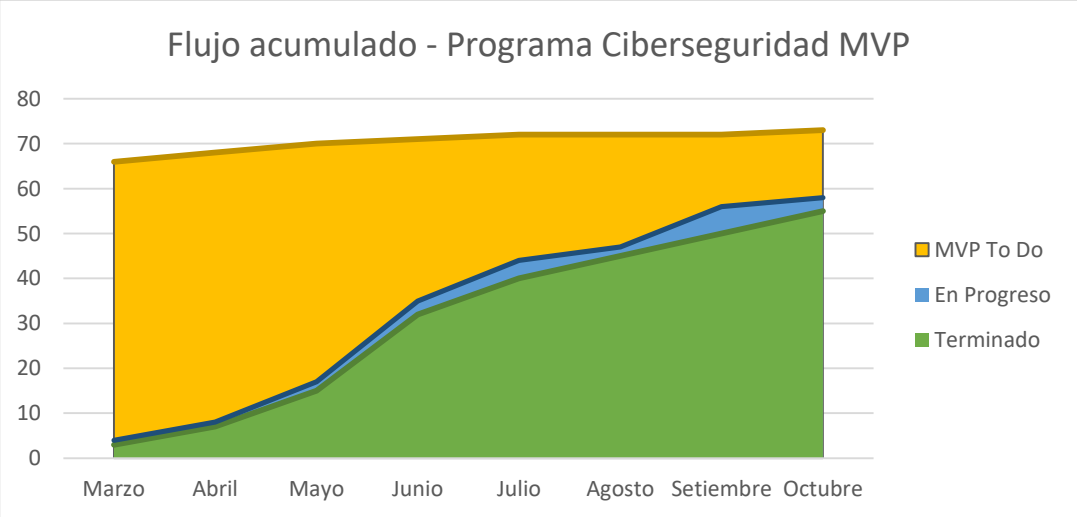


Figura 12. Diagrama de Flujo Acumulado del MVP

Nota. Elaboración Propia. Indica el avance de tareas e historias de usuario terminadas, en progreso y por hacer del MVP. El eje Y indica la cantidad de tareas, el eje X el tiempo.

3.6.2. *Proyección de tiempo para la finalización del MVP.*

Utilizando el mismo diagrama de flujo acumulado del diseño e implementación del MVP programa de ciberseguridad de puede generar líneas de proyección lineal, y con ello poder calcular el tiempo para la finalización del MVP.

Según el siguiente diagrama, se estaría culminando el MVP del programa de Ciberseguridad para diciembre del presente año.

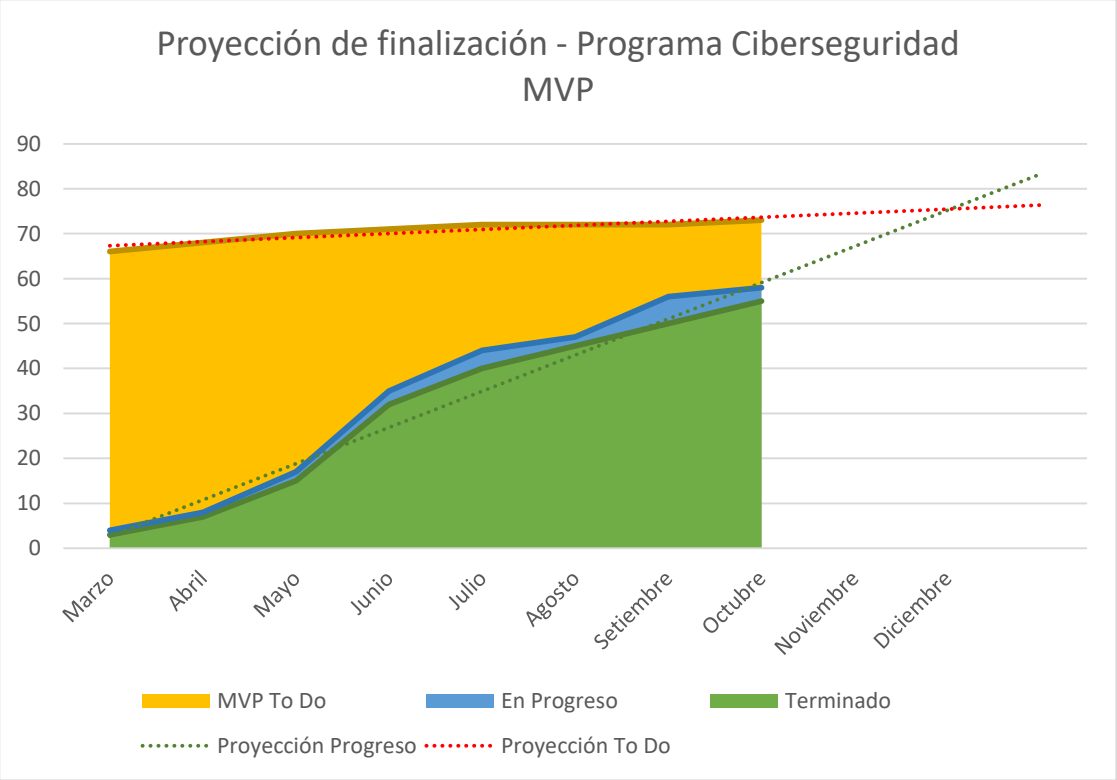


Figura 13. DFA del MVP con proyección lineal.

Nota. Elaboración Propia. El eje Y indica la cantidad de tareas, el eje X el tiempo. Se agregó la línea de tendencia lineal. Se agregó en el eje X, tres meses adicionales.

3.6.3. *Eventos e incidentes de Ciberseguridad por año.*

Se recopiló la cantidad de eventos de ciberseguridad en los últimos 5 años y se categorizó por tipo de amenazas según el modelo STRIDE (Ver 2.8.3). Se puede apreciar en la figura 14 que los principales eventos que ha sufrido la empresa del caso práctico han sido por disponibilidad o de tipo *Denial of Service* según el modelo STRIDE.

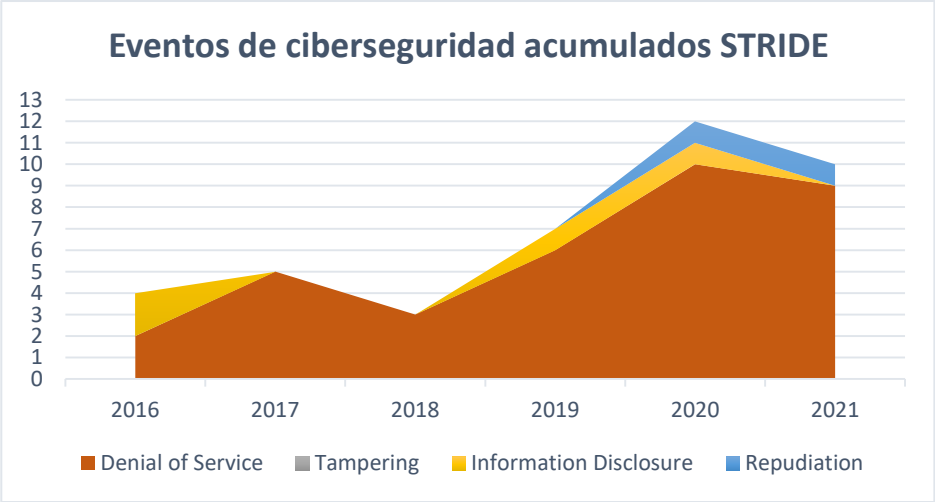


Figura 14. Eventos e Incidentes de ciberseguridad por año acumulados.

Nota. Elaboración Propia.

Para poder apreciar en mayor detalle, se ha divido en dos categorías los eventos de ciberseguridad asociados a la disponibilidad. Se dividió la categoría Denial of Service en los de tipo ataques DDoS y por evento de infraestructura de red.

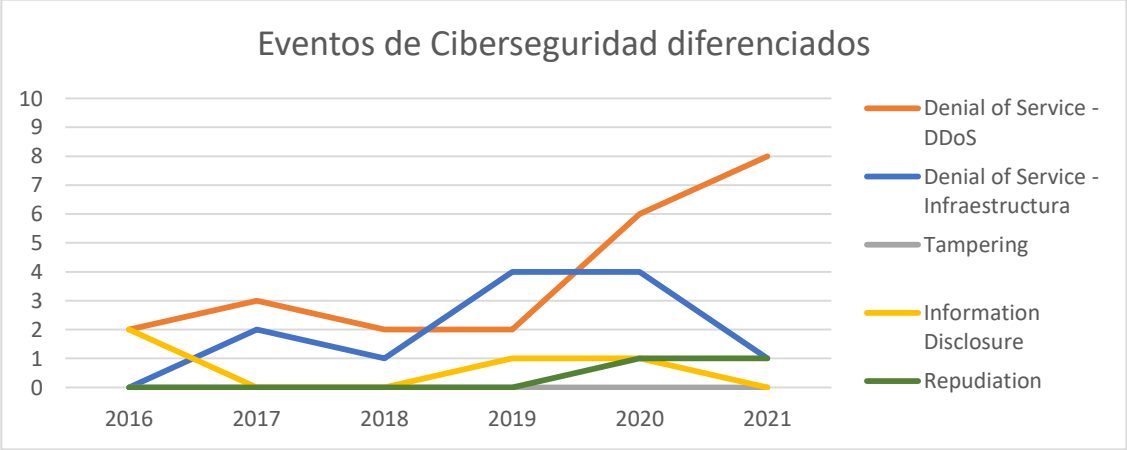


Figura 15. Eventos e Incidentes de ciberseguridad por año diferenciado.

Nota. Elaboración Propia.

Se puede notar en la figura una reducción de eventos de caída por infraestructura de red. El principal motivo fue la renovación tecnológica y mejora de configuración de equipos de networking en alta disponibilidad. En su contraparte, los eventos relacionados a la amenaza DDoS aumentaron considerablemente, ya que solo el total de eventos acumulados hasta octubre del 2021 superó su máximo del período anterior. Cabe señalar que no se visualiza

aún una reducción de los incidentes asociado a los eventos de tipo DDoS. A la fecha que se redactaba este documento, la plataforma de mitigación contra esta amenaza se encontraba aún en proceso de implementación.

3.6.4. ROSI o Retorno de inversión en Seguridad del AntiDDoS

Entre los cálculos a evaluar, se determinará el ROSI o retorno de inversión en seguridad, para una solución de ciberseguridad en implementada. Para el caso de aplicación la alta dirección solicitó en principal el interés el ROSI de la solución de protección ante ataques DDoS.

La siguiente fórmula determina el cálculo del ROSI por incidente de seguridad:

$$ROSI = \frac{(Exposición\ al\ Riesgo * \%\ Porcentaje\ de\ mitigación) - Costo\ de\ Solución}{Costo\ de\ Solución}$$

Exposición al riesgo: es el producto del costo estimado por un incidente por el número de incidentes declarados durante el mes.
% Porcentaje de mitigación: es el indicador de incidentes mitigados declarados en un año o hasta la fecha.
Costo de Solución: es el valor o pago de la solución mensual.

ROSI de la solución Anti DDoS

Hechos setiembre del 2021

- Costo de solución de seguridad $US 1800
- Número de incidentes declarados 3
- Porcentaje de Mitigación 70%

Supuestos setiembre del 2021

- Horas hombre por incidente $US 900
- Desafiliación de clientes por indisponibilidad $US 1200
- Costo total estimado por incidente $US 2100

ROSI = (($2100*3 * 70%) - $1800) / $1800

Basados en los hechos y supuestos se realiza un cálculo del ROSI para la solución AntiDDoS de empresa del Caso práctico, el cual tiene un valor de:

ROSI = 145%

3.6.5. Evaluación de resultados con la hipótesis inicial

Hipótesis:

Si se utiliza métodos ágiles en el diseño de controles ciberseguridad, entonces mejorará el seguimiento y control de un programa de ciberseguridad con un retorno de inversión en seguridad en el corto plazo.

Resultados:

- Al emplear marcos ágiles, permitió de forma rápida y simple agregar nuevos requerimientos críticos al negocio. En este caso, se aplicó un cambio de adición de dos nuevos controles en el MVP. Para más detalles de los controles de ciberseguridad ver *Tabla 9. Cuadro de controles de Seguridad por estado*.

- El programa de ciberseguridad permite un mejor seguimiento y control del programa utilizando diferentes herramientas ágiles, como el User Story Map y el diagrama de flujo acumulado. Ver el subcapítulo *Planificación del Producto y de Sprints.*

- Para el retorno de inversión en seguridad, se puede apreciar un retorno en corto tiempo con un valor de ROSI en 145%, para la implementación de la solución Anti DDoS. Para más detalles sobre el ROSI ver el subcapítulo 2.7 *Análisis de costo – beneficio en CiberSeguridad.*

- Se puede apreciar una mejora en la ciber resiliencia con una reducción de eventos de ciberseguridad por caídas por infraestructura de red. Fue el primer ítem implementado en el MVP y que logró buenos resultados en plazos inmediatos. Para más detalles ver *Eventos e incidentes de Ciberseguridad por año.*

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Si se utiliza marcos ágiles y buenas prácticas que se encuentren alineados al objetivo del negocio, la ciber resiliencia de una empresa se verá mejorada en el corto plazo y con beneficios de retorno visibles a la alta dirección. El ROSI es muy útil para justificar y priorizar la inversión según el riesgo para la empresa.

La utilización de herramientas ágiles en la ciberseguridad apoya de forma considerable en el seguimiento continuo del estado del programa y del avance del trabajo. Además permite gestionar los cambios, como agregar y quitar requerimientos sin mayor dificultad.

El negocio es quien prioriza realmente que controles de ciberseguridad debe primero implementarse. La seguridad de la organización no es sólo trabajo del área de TI, sino de toda la organización, con el compromiso total del gerente general o de la alta dirección.

4.2. Recomendaciones y propuesta gerencial

La empresa del caso, ha intentado por múltiples años implementar un sistema de gestión de seguridad basado en el estándar ISO 27001. Luego múltiples intentos nunca pudo desarrollar un programa o sistema integral, sólo se desplegaron iniciativas aisladas de las áreas técnicas.

Con la presente investigación se armoniza las necesidades de la alta dirección con la implementación técnica. Los objetivos de ciberseguridad se alinean a los OKR y las metas del plan estratégico. Las gerencias de las áreas críticas disponen de una herramienta de control y monitoreo de los riesgos cibernéticos a través de controles de seguridad tecnológico y táctico.

Este caso es aplicable, además, a muchas otras empresas en Latinoamérica en situación similar que requieren mecanismos que brinden beneficios en el corto plazo y con poca inversión, priorizando la necesidad y riesgo del negocio. La utilización del ROSI y el DFA, la agrupación del trabajo en sprint y disponer de un mínimo viable en ciberseguridad, le brinda a un gerente de una empresa en plena transformación digital, una posición única y de mayor capacidad de reacción, característica esencial en los negocio de hoy en día.

BIBLIOGRAFÍA

- ALAIMO, D.M. (2013): *"Proyectos ágiles con scrum",* Ediciones Kleer, Buenos Aires Argentina.
- ANDERSON, D.J. (2010): *"Kanban: Cambio Evolutivo Exitoso Para su Negocio de Tecnología"*, Sequim, WA: Blue Hole Press.
- ANDERSON, D.J. & CARMICHAEL, A. (2016): *"Kanban, esencial condensado"*, Lean Kanban University Press, Seattle-Washington, Estado Unidos.
- BARBA OLIVARES G.E. (2017): *"Modelo de amenazas, una técnica de análisis y gestión de riesgo asociados a software y aplicaciones"* [En línea], Artículo, Universidad Piloto de Colombia. Recuperado en marzo del 2021 de http://repository.unipiloto.edu.co/handle/20.500.12277/2646
- BID (2020): "CIBERSEGURIDAD: Riesgos, avances y el camino a seguir en América Latina y el Caribe", Banco Interamericano de Desarrollo, OEA, USA.
- KOHNFELDER, L. & PRAERIT, G. (1999): *"The threats to our products",* Paper, Microsoft Corporation.
- CERTIPROF (2019a): "*Lead Cybersecurity Professional Certificate (LCSPC)*", libro de certificación, Certiprof LLC, Estados Unidos.
- CERTIPROF (2019b): "*Innovation Management Certified Professional (IMCP)*", libro de certificación, Certiprof LLC, Estados Unidos.
- CIS (2019): "*CIS Controls V 7.1"*, **Center** for Internet Security, Inc.®, Nueva York USA.
- JOHN & JO LINK (2015): *"Creating an Adaptive Cybersecurity Culture Through the Agile Cybersecurity Action Plan - ACAP"*, VolvoXinc, John W. Link & Jo Lee Loveland Link, Virginia USA
- KNIBERG, H. & SKARIN, M. (2010): *"Kanban y Scrum – obteniendo lo mejor de ambos"*, InfoQ, C4Media Inc., Estados Unidos.
- ISACA (2017): "*Guía de Estudio de Fundamentos de Ciberseguridad, 2ª edición*", ISACA, Schaumburg, IL EE. UU.
- ISACA (2022): *"Glossary"* [En línea], recuperado en línea en setiembre del 2022 de https://www.isaca.org/pages/glossary.aspx
- OEA (2019): *"Ciberseguridad, Marco NIST - Un abordaje integral de la Ciberseguridad" [en línea], OEA,* recuperado en marzo del 2021 de

https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

- ESET (2021): “ESET Security Report. Latinoamérica 2021”, ESET Latinoamérica, Argentina.
- ESET (2022): *“Glosario WeLiveSecurity en español”* [en línea], ESET recuperado en setiembre del 2022 de https://www.welivesecurity.com/la-es/glosario/
- GARTNER (2022): “”
- PANDA (2022): *“Glosario de Panda Security”* [En línea], recuperado en setiembre del 2022 de https://www.pandasecurity.com/peru/homeusers/security-info/glossary/
- PALO ALTO (2022): *“Cyberpedia”* [En línea], recuperado en setiembre del 2022 de https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security
- Ormella, C. (2011). *“ROSI: EL ROI de la Seguridad de La Información”, Revista LAN & WAN.*
- PMI (2017): *“Guía Práctica de Ágil”,* Project Management Institute, Inc, Independent Publishers Group, Chicago, IL EE. UU.
- SCHWABER, K. & SUTHERLAND, J. (2017): *“La Guía de Scrum” [en línea]*, Attribution Share-Alike license of Creative Commons, Scrum.Org and Scrum Inc., recuperado en marzo del 2021 de *https://scrumguides.org/download.html*
- Sonnenreich, W (2005): *“Return On Security Investment (ROSI) – A Practical Quantitative Model”, Journal of Research and practice in Information Technology, Miami, USA.*
- STACEY (2011): *“Strategic Management and Organisational Dynamics”*, Pearson Education Limited, Pensilvania, EE. UU.
- TRISTANCHO ROBLES, L.A (2015): “*¿POR QUÉ FRACASAN LOS PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN?”* [En línea], Artículo, Universidad Piloto de Colombia. Recuperado en marzo del 2021 de http://repository.unipiloto.edu.co/handle/20.500.12277/2855
- WITTKOP, JEREMY (2016): *"Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices: Practical Guidelines and Best Practices"*, Springer Science + Business Media, Colorado, USA

ANEXOS

A. Cuestionario de la capa de negocio del caso de aplicación.

CUESTIONARIO – CAPA DE NEGOCIO	
Participantes del negocio: Participantes del proyecto: Fecha de reunión:	
¿Cuál cree usted, es el componente más importante en el negocio o unidad de negocio?	Nivel 1: El sistema de gestión y los datos de nuestros clientes finales.
¿En orden de prioridad, cuál cree sería el segundo en su lista?	Nivel 2: Sistema de venta (Portal web)
¿Este componente, evaluado en pérdidas económicas o por reputación, podría detenerse 5 minutos, 1 hora o 1 día?	Componente 1: Ideal, sin caídas. 1 hora caída (Máx. aceptable)
	Componente 2: Ideal, sin caídas 5 horas caída (Max. aceptable)
¿Este componente en riesgo de pérdidas económicas o por reputación, podría aceptarse tener una fuga o robo de información?	Componente 1: Intromisión a la información de un grupo de clientes no es aceptable. ejemplo: todo un servidor
	Componente 2: Una intrusión total en el sistema, que afecte la reputación corporativa.

B. Cuadro de roles de la capa de estrategia del caso de aplicación.

ROLES INTELIGENCIA DE SEGURIDAD	ROL SCRUM	Roles asignados	Responsabilidades
Grupo de Gobierno	Cliente / Interesados	**Comité de Seguridad:** - Gerente General - Área Legal - Gerente de Producto - Gerente de TI/Operaciones - Jefe área de transformación digital.	- Determina las necesidades del negocio - Solicita capacidades de seguridad - Determina los objetivos de seguridad. - Estipula el nivel mínimo de aceptación - Participan en la gestión de crisis. - Supervisa los OKR de seguridad.
Delegado del grupo de gobierno	Product Owner	Jefe del área de Transformación digital (E1, E3) Gerente de TI/Operaciones (E2)	Product Owner lidera cada equipo
Grupo de trabajo	Equipo de trabajo	**Equipo E1:** Equipo Políticas y Procesos **Equipo E2:** Equipo DDoS, DR y HA **Equipo E3:** Equipo Soporte TI – controles CIS	Se conformaron tres (3) equipos de trabajo: • El equipo de procesos y políticas, quien documentará además los procedimientos. • El equipo que trabajaría la solución DDoS, habilitar la función de HA en los equipos de networking y la solución de DR de Cpanel. • El último equipo de Soporte de TI, quien hará cumplimiento a los primeros 6 controles CIS.

C. Cuadro de capacidades de seguridad del caso de aplicación.

N	Activo Crítico	DCI	Como… (Rol)	Necesito la capacidad … (Objetivo)	Para… (Motivación)	Criterios de aceptación
1	Servicio Hosting	D	Gerente General	E1. Protección contra ataques DDoS.	Mejorar la experiencia con una mejor disponibilidad y reducir las desafiliaciones de clientes.	Protección 3x o más de tráfico de ataques DDoS historial
2			Gerente general	E2. Infraestructura altamente disponible.	Reducir las caídas por red, mantener a nuestros clientes y tener una disponibilidad de clase mundial	Disponibilidad de 99.9%. Equipos de networking en H.A.
3		C	Área Legal	E3. Datos (backups) de clientes protegidos	Evitar responsabilidades relacionadas a brechas de datos.	Cifrado y con política de derecho a olvido aplicado.
4	Servicio de Venta en línea	D	Gerente de producto	E1. Sitio web esté disponible ante ataques DDoS	Los clientes pueden realizar las compras ante eventos de este tipo.	Ataque mayor a 50 Gbps y que se active de forma automática.
5			Gerente de producto	E2. Infraestructura altamente disponible.	Reducir las caídas por el sistema, así el volumen de compras de clientes no es afectado.	Sistemas y portal web en H.A.

Nota: La columna DCI hace referencia a una dimensión de la seguridad: D de Disponibilidad, la C es la Confidencialidad y la letra I es la Integridad. La Épica 3, E3 Datos de clientes protegidos, no está incluido en el MVP, pero se haría el mayor esfuerzo para incluirlo.

D. Cuadro de procedimientos de seguridad e historias de usuario del caso de aplicación.

N	Activo Crítico	Área	Como… (Rol)	Necesito el procedimiento o documento… (Objetivo)	Para… (Motivación)	Criterios de aceptación
Épica 1 (E1): **Protección contra ataques DDoS**						
1	Servicio Hosting y Servicio Venta en línea	GA	Gerente de TI	Diagrama de arquitectura de la solución AntiDDoS	Documentar, conocer y comprender la solución de seguridad	Se requiere HLD (alto nivel) y LLD (bajo nivel)
2		GP	Jefe área de TD	Políticas corporativas relacionadas al Anti DDoS	Alinea las necesidades de seguridad a la del negocio.	Se requiere la formalización y comunicación de la política.
3		E	Gerente de TI	Clasificación de eventos asociados a ataques DDoS.	Diferencias eventos de ataque, incidentes y falsos positivos.	Eventos requiere especificar por protocolo, tráfico y tipo.
4		I	Jefe área de TD	Plan de respuesta ante incidentes DDoS	Mejor respuesta frente eventos de ataque DDoS	Procedimiento técnico, de comunicación y roles asociados
5		A	Jefe área de TD	KPI mensual y anual de la solución AntiDDoS	Alinear los OKR del plan estratégicos con sus KPI	Ingresado al plan estratégico: OKR, KPI y actividades.
Épica 2 (E2): **Infraestructura altamente disponible.**						
	Servicio Hosting	GA	Gerente de TI	Diagrama de arquitectura de red en alta disponibilidad	Documentar, conocer y comprender la infraestructura de red	Se requiere HLD (alto nivel) y LLD (bajo nivel)
		GA	Gerente de TI	Diagrama de arquitectura del DR Cpanel	Documentar, conocer y comprender la solución DR para el servicio Hosting	Se requiere HLD (alto nivel) y LLD (bajo nivel)

		GP	Jefe área de TD	Políticas corporativas del mantenimiento de red.	Alinea el trabajo diario del área de TI/Operaciones, al negocio de hosting.	Se requiere la formalización y comunicación de la política.
		GP	Jefe área de TD	Políticas corporativas sobre el DR cPanel	Alinea el trabajo diario del área de TI/Operaciones, al negocio de hosting.	Se requiere la formalización y comunicación de la política.
		E	Gerente de TI	Clasificación de eventos asociados la disponibilidad.	Diferencias eventos de caída de red, incidentes y falsos positivos.	Requiere especificar la clasificación de una caída por red.
		I	Jefe área de TD	Plan de respuesta ante caídas no esperadas (incluye DR)	Mejor respuesta frente a eventos de caídas de red no esperadas.	Procedimiento técnico, de comunicación y roles asociados
	Servicio de Venta en línea	GA	Gerente de TI	Diagrama de arquitectura de sistema en alta disponibilidad	Documentar, conocer y comprender los sistemas operacionales.	Se requiere HLD (alto nivel) y LLD (bajo nivel)
		GP	Jefe área de TD	Políticas corporativas del mantenimiento del sistema.	Alinea las necesidades de seguridad y el desarrollo de sistemas, a la del negocio.	Se requiere la formalización y comunicación de la política.
		I	Jefe área de TD	Plan de respuesta ante caídas no esperadas del sistema	Mejor respuesta frente a eventos de caídas no esperadas de los sistemas	Procedimiento técnico, de comunicación y roles asociados

Notas: Los procedimientos de seguridad disponen de las siguientes áreas tácticas: Gestión de Aplicaciones (GA); Gobierno y Políticas (GP); Priorización de Eventos (E); Gestión de Incidentes (I); Informes y analítica (A).

E. Cuadro de tecnologías e historias de usuario del caso de aplicación.

N	Activo Crítico	Cat	Como… (Rol)	Necesito la tecnología… (Objetivo)	Para… (Motivación)	Criterios de aceptación
Épica 1 (E1): **Protección contra ataques DDoS**						
1	Servicio Hosting y Servicio Venta en línea	CoN	Gerente de TI	Firewall Anti DDoS Híbrido	Protegernos ante ataques DDoS Volumétricos	Ataques inundación APP, UDP, TCP syn, países, reputación, derivación
2		CoX	Gerente de TI	SIEM con integración a Anti DDoS	Detectar patrones y mejorar la respuesta ante ataques.	Integrar la solución con equipos Firewall de perímetro o Switch core.
3		MoN	Gerente de TI	Panel de Gestión de la plataforma, monitoreo y soporte.	Dar respuesta y atención ante incidentes de tipo DDoS y estar alineado a los OKR.	Servicio o Capacitación en gestión de la plataforma. Reportes que soporte los indicadores KPI.
Épica 2 (E2): **Infraestructura altamente disponible.**						
4	Servicio Hosting	CoN	Gerente de TI	Red de Switches H.A.	Lograr el indicador de disponibilidad prometida.	Pruebas ATP Pruebas exitosas de HA
5		CoN	Gerente de TI	Replica de datos o DR para WHM/cPanel	Cumplir con el procedimiento técnico de Recuperación ante Desastres (DR) para Hosting.	Prueba de Contingencia de cPanel Simulacro de Contingencia de cPanel
6	Venta en línea	CoN	Gerente de TI	Servidores Web y Base de datos en HA	Mejorar la disponibilidad del servicio web y sistemas internos.	Prueba de HA de Sistemas

Nota. Las tecnologías están categorizadas por el Contenido (CoN), por el Contexto (CoX) y de tipo Monitoreo (MoN)

F. Tabla de Controles CIS y grupos de implementación

Control crítico #1: Inventario y control de activos hardware				Grupos de implementación		
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**	**IG 1**	**IG 2**	**IG 3**
1.1	Equipos	Identificar	Utilizar una herramienta de descubrimiento activo		X	X
1.2	Equipos	Identificar	Utilizar una herramienta de descubrimiento pasivo de activos			X
1.3	Equipos	Identificar	Utilizar DHCP Logging para actualizar el inventario de activos		X	X
1.4	Equipos	Identificar	Mantener un inventario de activos detallado	X	X	X
1.5	Equipos	Identificar	Mantener la información del inventario de activos		X	X
1.6	Equipos	Responder	Gestionar los activos no autorizados	X	X	X
1.7	Equipos	Proteger	Implementar control de acceso a nivel de puerto		X	X
1.8	Equipos	Proteger	Utilizar certificados clientes para autenticar activos hardware			X
Control crítico #2: Inventario y control de activos software						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
2.1	Aplicaciones	Identificar	Mantener un inventario de software autorizado	X	X	X
2.2	Aplicaciones	Identificar	Asegurar que el software tenga soporte del fabricante	X	X	X
2.3	Aplicaciones	Identificar	Utilizar herramientas de inventario de software		X	X
2.4	Aplicaciones	Identificar	Rastrear información del inventario de software		X	X
2.5	Aplicaciones	Identificar	Integrar los inventarios de activos de hardware y software			X
2.6	Aplicaciones	Responder	Gestionar el software no aprobado	X	X	X
2.7	Aplicaciones	Proteger	Utilizar lista blanca de aplicaciones			X
2.8	Aplicaciones	Proteger	Implementar lista blanca de librerías			X
2.9	Aplicaciones	Proteger	Implementar lista blanca de scripts			X
2.10	Aplicaciones	Proteger	Separar física o lógicamente las aplicaciones de alto riesgo			X
Control crítico #3: Gestión continua de vulnerabilidades						
Sub-	**Tipo de**	**Función de**	**Control**			

control	activo	Seguridad				
3.1	Aplicaciones	Detectar	Ejecutar herramientas de escaneo de vulnerabilidades automatizadas		X	X
3.2	Aplicaciones	Detectar	Realizar análisis de vulnerabilidades autenticados		X	X
3.3	Aplicaciones	Proteger	Proteger las cuentas dedicadas a auditorías		X	X
3.4	Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches del sistema operativo	X	X	X
3.5	Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches de software	X	X	X
3.6	Aplicaciones	Responder	Comparar escaneos de vulnerabilidades consecutivos		X	X
3.7	Aplicaciones	Responder	Utilizar un proceso de calificación de riesgo		X	X
Control crítico #4: Uso controlado de privilegios administrativos						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
4.1	Usuarios	Detectar	Mantener un inventario de cuentas administrativas		X	X
4.2	Usuarios	Proteger	Cambiar contraseñas por defecto	X	X	X
4.3	Usuarios	Proteger	Asegurar el uso de cuentas administrativas dedicadas	X	X	X
4.4	Usuarios	Proteger	Usar contraseñas únicas		X	X
4.5	Usuarios	Proteger	Usar autenticación multifactor para todo acceso administrativo		X	X
4.6	Usuarios	Proteger	Usar máquinas dedicadas para toda tarea administrativa			X
4.7	Usuarios	Proteger	Limitar el acceso a herramientas de scripts		X	X
4.8	Usuarios	Detectar	Registrar y alertar cambios de miembros en grupos administrativos		X	X
4.9	Usuarios	Detectar	Registrar y alertar los inicios de sesión fallidos a cuentas administrativas		X	X
Control crítico #5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
5.1	Aplicaciones	Proteger	Establecer configuraciones seguras	X	X	X
5.2	Aplicaciones	Proteger	Mantener imágenes seguras		X	X
5.3	Aplicaciones	Proteger	Almacenar las imágenes maestras de forma segura		X	X
5.4	Aplicaciones	Proteger	Implementar herramientas de gestión de configuración de sistema		X	X

5.5	Aplicaciones	Detectar	Implementar sistemas de monitoreo automatizado de configuración		X	X
Control crítico #6: Mantenimiento, monitoreo y análisis de logs de auditoría						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
6.1	Red	Detectar	Utilizar tres fuentes de tiempo sincronizadas		X	X
6.2	Red	Detectar	Activar registros de auditoría	X	X	X
6.3	Red	Detectar	Habilitar registros detallados		X	X
6.4	Red	Detectar	Asegurar almacenamiento adecuado para registros		X	X
6.5	Red	Detectar	Gestión centralizada de registros		X	X
6.6	Red	Detectar	Desplegar herramientas SIEM o de Análisis de registros		X	X
6.7	Red	Detectar	Revisar regularmente los registros		X	X
6.8	Red	Detectar	Ajustar regularmente el SIEM			X
Control crítico #7: Protección de correo electrónico y navegador web						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
7.1	Aplicaciones	Proteger	Asegurar el uso de navegadores y clientes de correo electrónico que cuenten con soporte		X	X
7.2	Aplicaciones	Proteger	Deshabilitar plugins innecesarios de navegadores o clientes de correo electrónico		X	X
7.3	Aplicaciones	Proteger	Limitar el uso de lenguajes de scripting en navegadores web y clientes de correo electrónico		X	X
7.4	Red	Proteger	Mantener y aplicar filtros de URL basados en red		X	X
7.5	Red	Proteger	Suscribirse a servicios de categorización de URL		X	X
7.6	Red	Detectar	Registrar todas las peticiones de URLs		X	X
7.7	Red	Proteger	Utilizar servicios de filtrado DNS	X	X	X
7.8	Red	Proteger	Implementar DMARC y habilitar verificación del lado del receptor		X	X
7.9	Red	Proteger	Bloquear tipos de archivos innecesarios		X	X
7.10	Red	Proteger	Utilizar técnicas de sandbox para todos los adjuntos de correo electrónico			X
Control crítico #8: Defensa contra malware						
Sub-	**Tipo de**	**Función de**	**Control**			

control	activo	Seguridad				
8.1	Equipos	Proteger	Utilizar software de gestión centralizada contra malware		X	X
8.2	Equipos	Proteger	Asegurar que el software y las firmas contra malware estén actualizadas		X	X
8.3	Equipos	Proteger	Habilitar características anti-explotación de sistemas operativos / implementar tecnologías anti-explotación		X	X
8.4	Equipos	Detectar	Configurar escaneo anti-malware de dispositivos removibles	X	X	X
8.5	Equipos	Proteger	Configurar equipos para no autoejecutar contenido	X	X	X
8.6	Equipos	Detectar	Centralizar los registros anti-malware		X	X
8.7	Red	Detectar	Habilitar registros de consultas DNS		X	X
8.8	Equipos	Detectar	Habilitar registros de auditoría de línea de comandos		X	X
Control crítico #9: Limitación y control de puertos de red, protocolos y servicios						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
9.1	Equipos	Identificar	Asociar puertos, servicios y protocolos activos al inventario de activos		X	X
9.2	Equipos	Proteger	Asegurar que solo puertos, protocolos y servicios aprobados se están ejecutando		X	X
9.3	Equipos	Detectar	Realizar regularmente escaneos automatizados de puertos		X	X
9.4	Equipos	Proteger	Aplicar firewalls basados en host o filtrado de puertos	X	X	X
9.5	Equipos	Proteger	Implementar firewalls de aplicación			X
Control crítico #10: Capacidad de recuperación de datos						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
10.1	Datos	Proteger	Asegurar los respaldos regulares automatizados	X	X	X
10.2	Datos	Proteger	Realizar respaldos de sistemas completos	X	X	X
10.3	Datos	Proteger	Probar los datos en los medios de respaldo		X	X
10.4	Datos	Proteger	Asegurar la protección de las copias de respaldo	X	X	X
10.5	Datos	Proteger	Asegurar que las copias de respaldo tengan al menos un destino discontinuo	X	X	X
Control crítico #11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores						
Sub-	**Tipo de**	**Función de**	**Control**			

control	activo	Seguridad				
11.1	Red	Identificar	Mantener configuraciones de seguridad estándar en equipos de red		X	X
11.2	Red	Identificar	Documentar las configuraciones de reglas de tráfico		X	X
11.3	Red	Detectar	Utilizar herramientas automatizadas para verificar configuraciones de equipos y detectar cambios		X	X
11.4	Red	Proteger	Instalar la última versión estable de cualquier actualización de seguridad en todos los equipos de red	X	X	X
11.5	Red	Proteger	Gestionar equipos de red utilizando autenticación multi-factor y sesiones cifradas		X	X
11.6	Red	Proteger	Utilizar máquinas dedicadas para todas las tareas administrativas en la red		X	X
11.7	Red	Proteger	Administrar la infraestructura de red mediante una red dedicada		X	X
Control crítico #12: Defensa de borde						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
12.1	Red	Identificar	Mantener un inventario de los bordes de la red	X	X	X
12.2	Red	Detectar	Escanear de conexiones no autorizadas en los bordes confiables de la red		X	X
12.3	Red	Proteger	Denegar comunicaciones con direcciones IPs maliciosas conocidas		X	X
12.4	Red	Proteger	Denegar comunicaciones sobre puertos no autorizados	X	X	X
12.5	Red	Detectar	Configurar sistemas de monitoreo para registro paquetes de red		X	X
12.6	Red	Detectar	Desplegar sensores IDS basados en red		X	X
12.7	Red	Proteger	Desplegar IPS basado en red			X
12.8	Red	Detectar	Desplegar colectores NetFlow en equipos de borde de la red		X	X
12.9	Red	Detectar	Desplegar servidor proxy de filtrado de capa de aplicación			X
12.10	Red	Detectar	Descifrar el tráfico de red en el proxy			X
12.11	Usuarios	Proteger	Requerir autenticación multi-factor en todos los inicios de sesión remotos		X	X
12.12	Equipos	Proteger	Gestionar todos los dispositivos remotos que se conectan a la red interna			X
Control crítico #13: Protección de datos						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			

13.1	Datos	Identificar	Mantener un inventario de información sensible	X	X	X
13.2	Datos	Proteger	Remover datos o sistemas sensibles que no son accedidos regularmente por la organización	X	X	X
13.3	Datos	Detectar	Monitorear y bloquear el tráfico de red no autorizado			X
13.4	Datos	Proteger	Permitir solamente el acceso a proveedores de servicios de nube o correo autorizados		X	X
13.5	Datos	Detectar	Monitorear y detectar cualquier uso no autorizado de cifrado			X
13.6	Datos	Proteger	Cifrar el disco duro de todos los dispositivos móviles	X	X	X
13.7	Datos	Proteger	Gestionar dispositivos USB		X	X
13.8	Datos	Proteger	Gestionar las configuraciones de lectura/escritura de sistemas para medios removibles externos			X
13.9	Datos	Proteger	Cifrar los datos en dispositivos de almacenamiento USB			X
Control crítico #14: Control de acceso basado en la necesidad de conocer						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
14.1	Red	Proteger	Segmentar la red basado en sensibilidad		X	X
14.2	Red	Proteger	Habilitar filtrado de firewall entre VLANs		X	X
14.3	Red	Proteger	Deshabilitar comunicaciones entre estaciones de trabajo		X	X
14.4	Datos	Proteger	Cifrar toda la información sensible en tránsito		X	X
14.5	Datos	Detectar	Utilizar una herramienta de descubrimiento activo para identificar datos sensibles			X
14.6	Datos	Proteger	Proteger la información mediante lista de control de acceso	X	X	X
14.7	Datos	Proteger	Aplicar control de acceso a datos mediante herramientas automatizadas			X
14.8	Datos	Proteger	Cifrar información sensible en reposo			X
14.9	Datos	Detectar	Imponer el registro detallado para acceso o cambios en datos sensibles			X
Control crítico #15: Control de acceso inalámbrico						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
15.1	Red	Identificar	Mantener un inventario de puntos de acceso inalámbrico autorizados		X	X
15.2	Red	Detectar	Detectar puntos de acceso inalámbricos conectados a la red cableada		X	X

15.3	Red	Detectar	Usar un sistema de detección de intrusión inalámbrica		X	X
15.4	Equipos	Proteger	Deshabilitar el acceso inalámbrico en dispositivos si no se requiere			X
15.5	Equipos	Proteger	Limitar el acceso inalámbrico en dispositivos cliente			X
15.6	Equipos	Proteger	Inhabilitar las capacidades de red inalámbrica punto a punto en clientes inalámbricos		X	X
15.7	Red	Proteger	Usar estándar de cifrado avanzado (AES) para cifrar datos inalámbricos	X	X	X
15.8	Red	Proteger	Usar protocolos de autenticación inalámbrica que requieran autenticación mutua multi-factor			X
15.9	Equipos	Proteger	Deshabilitar el acceso periférico inalámbrico de dispositivos		X	X
15.10	Red	Proteger	Crear una red inalámbrica separada para dispositivos personales y no confiables	X	X	X
Control crítico #16: Monitoreo y control de cuentas						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
16.1	Usuarios	Identificar	Mantener un inventario de sistemas de autenticación		X	X
16.2	Usuarios	Proteger	Configurar un punto de autenticación centralizado		X	X
16.3	Usuarios	Proteger	Requerir Autenticación Multi-factor		X	X
16.4	Usuarios	Proteger	Cifrar o hashear todas las credenciales de autenticación		X	X
16.5	Usuarios	Proteger	Cifrar la transmisión de nombres de usuario y credenciales de autenticación		X	X
16.6	Usuarios	Identificar	Mantener un inventario de cuentas		X	X
16.7	Usuarios	Proteger	Establecer un proceso para revocar el acceso		X	X
16.8	Usuarios	Responder	Deshabilitar cualquier cuenta no asociada	X	X	X
16.9	Usuarios	Responder	Desactivar cuentas inactivas	X	X	X
16.10	Usuarios	Proteger	Asegurar que todas las cuentas tengan fecha de caducidad		X	X
16.11	Usuarios	Proteger	Bloquear sesiones de estaciones de trabajo tras inactividad	X	X	X
16.12	Usuarios	Detectar	Monitorear los intentos de acceso a cuentas desactivadas		X	X
16.13	Usuarios	Detectar	Alertar sobre desviación de comportamiento de inicio de sesión de cuentas			X
Control crítico #17: Implementar un programa de concienciación y entrenamiento de seguridad						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			

17.1	N/A	N/A	Realizar un análisis de brecha de habilidades		X	X
17.2	N/A	N/A	Realizar capacitación para llenar la brecha de habilidades		X	X
17.3	N/A	N/A	Implementar un programa de concienciación de seguridad	X	X	X
17.4	N/A	N/A	Actualice el contenido de concienciación con frecuencia		X	X
17.5	N/A	N/A	Entrenar a la fuerza laboral en la autenticación segura	X	X	X
17.6	N/A	N/A	Capacitar a la fuerza laboral en la identificación de ataques de ingeniería social	X	X	X
17.7	N/A	N/A	Capacitar a la fuerza laboral en manejo de datos sensibles	X	X	X
17.8	N/A	N/A	Capacitar a la fuerza laboral sobre las causas de la exposición involuntaria a los datos	X	X	X
17.9	N/A	N/A	Capacite a la fuerza laboral sobre cómo identificar y reportar incidentes	X	X	X
Control crítico #18: Seguridad del software de aplicación						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
18.1	N/A	N/A	Establecer prácticas seguras de codificación		X	X
18.2	N/A	N/A	Asegurar que la verificación explícita de errores se realice para todo el software desarrollado internamente		X	X
18.3	N/A	N/A	Verificar que el software adquirido aún tiene soporte		X	X
18.4	N/A	N/A	Usar sólo componentes de terceros actualizados y de confianza			X
18.5	N/A	N/A	Usar únicamente algoritmos de cifrado revisados y estandarizados		X	X
18.6	N/A	N/A	Asegurar que el personal de desarrollo de software esté capacitado en programación segura		X	X
18.7	N/A	N/A	Aplicar herramientas de análisis de código estático y dinámico		X	X
18.8	N/A	N/A	Establecer un proceso para aceptar y tratar los reportes de vulnerabilidades del software		X	X
18.9	N/A	N/A	Sistemas separados de producción y no producción		X	X
18.10	N/A	N/A	Implementar Firewall de aplicación Web (WAFs)		X	X
18.11	N/A	N/A	Usar plantillas de configuración de hardening estándar para bases de datos		X	X
Control crítico #19: Respuesta y manejo de incidentes						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			

19.1	N/A	N/A	Documentar los procedimientos de respuesta de incidentes	X	X	X
19.2	N/A	N/A	Asignar cargos y responsabilidades para la respuesta a incidentes		X	X
19.3	N/A	N/A	Designar personal de gestión para apoyar el manejo de incidentes	X	X	X
19.4	N/A	N/A	Idear estándares para toda la organización para reporte de incidentes		X	X
19.5	N/A	N/A	Mantener información de contacto para reportar incidentes de seguridad	X	X	X
19.6	N/A	N/A	Publicar información relacionada con la notificación de anomalías e incidentes informáticos	X	X	X
19.7	N/A	N/A	Llevar a cabo sesiones periódicas de escenarios de incidentes para el personal		X	X
19.8	N/A	N/A	Crear un esquema de priorización y puntuación de incidentes			X
Control crítico #20: Pruebas de penetración y ejercicios de equipo rojo						
Sub-control	**Tipo de activo**	**Función de Seguridad**	**Control**			
20.1	N/A	N/A	Establecer un programa de prueba de penetración		X	X
20.2	N/A	N/A	Llevar a cabo pruebas periódicas de penetración externa e interna		X	X
20.3	N/A	N/A	Realizar Ejercicios Periódicos del Equipo Rojo			X
20.4	N/A	N/A	Incluir pruebas de presencia de información y artefactos no protegidos de sistema		X	X
20.5	N/A	N/A	Crear banco de pruebas para elementos que normalmente no se prueban en producción		X	X
20.6	N/A	N/A	Usar herramientas de prueba de penetración y exploración de vulnerabilidades en conjunto		X	X
20.7	N/A	N/A	Asegurar que los resultados de la prueba de penetración estén documentados usando estándares abiertos y legibles por máquina			X
20.8	N/A	N/A	Controlar y supervisar las cuentas asociadas con las pruebas de penetración		X	X

Nota. Tabla adaptada del documento *Controles Críticos de Ciberseguridad* del CERT-PY, Centro de Respuestas a Incidentes Cibernéticos de Paraguay, Ministerio de Tecnologías de la Información y Comunicación del Gobierno de Paraguay. https://cert.gov.py/controles-criticos-seguridad