UNIVERSIDAD ADOLFO IBÁÑEZ

PROYECTO DE TÍTULO

Desarrollo de un Plan Director de Ciberseguridad e Implementación de Quick Wins para una Start-Up

---

Autor:
Felipe Tomás Andrés Gutiérrez López

Profesor guía:
Mary Fernanda Milla

Proyecto realizado acorde a los requerimientos para el título de Ingeniería Civil Informática

24 de diciembre de 2023

UAI | FACULTAD DE INGENIERÍA Y CIENCIAS

UNIVERSIDAD ADOLFO IBÁÑEZ

Resumen

Facultad de Ingeniería y Ciencias

Ingeniería Civil Informática

Desarrollo de un Plan Director de Ciberseguridad e Implementación de Quick Wins para una Start-Up

por Felipe Tomás Andrés Gutiérrez López

Este informe de proyecto de pasantía analiza la brecha de ciberseguridad presente en Ceptinel, una startup chilena que ofrece soluciones Software as a Service (SaaS) a entidades financieras para mitigar el crimen financiero. Estos servicios están alojados en servidores de Microsoft Azure, un proveedor de servicios en la nube. Ceptinel busca mejorar su nivel de ciberseguridad para garantizar el cumplimiento de los estándares de la industria y las regulaciones establecidas por la Comisión para el Mercado Financiero (CMF). El objetivo principal es garantizar la disponibilidad, trazabilidad, integridad y confidencialidad de los datos de los clientes a través de un plan director de ciberseguridad.

Este informe enfatiza la importancia crítica de la ciberseguridad para Ceptinel, ya que un compromiso de datos podría resultar en pérdidas financieras significativas y comprometer la reputación de la empresa. Se propone la implementación de un plan director de ciberseguridad para lograr rápidamente resultados positivos en la protección de datos. Una evaluación exhaustiva de la infraestructura crítica de la empresa y la elección de soluciones tecnológicas adecuadas son partes fundamentales del proceso para satisfacer las necesidades específicas de la empresa.

Si bien no se lograron todos los objetivos específicos, este proyecto de pasantía logró con éxito el objetivo principal de mejorar el nivel de seguridad de los datos de los clientes de Ceptinel a un nivel satisfactorio. La implementación del plan director de ciberseguridad proporciona una base sólida para que Ceptinel cumpla con los estándares requeridos por la CMF y garantice la confianza de sus clientes.

UNIVERSIDAD ADOLFO IBÁÑEZ

Abstract

Faculty of Engineering and Science

Informatics Engineering

Development of a Cybersecurity Director Plan and Implementation of Quick Wins for a Start-Up

by Felipe Tomás Andrés Gutiérrez López

This internship project report analyzes the cybersecurity gap present in Ceptinel, a chilean startup that offers Software as a service (SaaS) solutions to financial entities for them to mitigate financial crime, these services are hosted on Microsoft Azure servers, a cloud provider. Ceptinel aims to enhance its cybersecurity level to ensure compliance with industry standards and the regulations set by the Comisión para el Mercado Financiero (CMF). The primary goal is to ensure the availability, traceability, integrity, and confidentiality of customer data through a cybersecurity director plan.

This report emphasizes the critical importance of cybersecurity for Ceptinel, as data compromise could result in significant financial losses, and compromise the company's reputation. The implementation of a cybersecurity director plan is proposed to swiftly achieve positive results in data protection. A comprehensive evaluation of the critical infrastructure of the company and the choice of suitable technology solutions are fundamental parts of the process to meet the company's specific needs.

Even though not every specific objective was successfully achieved, this internship project successfully attained the primary goal of improving the level of security of Ceptinel's customer data to a satisfactory level. The implementation of the cybersecurity director plan provides a solid foundation for Ceptinel to meet the CMF's required standards and ensure the trust of its clients.

Índice general

Resumen I

Abstract II

1. Introducción 1

2. Objetivos 5
2.1. Objetivo General 5
2.2. Objetivos Específicos 5

3. Medidas de Desempeño 6

4. Metodología 7

5. Estado del Arte 8
5.1. Solución de Plan de Acción de Ciberseguridad 8
5.1.1. Plan Director de Ciberseguridad 8
5.2. Soluciones de Seguridad de Aplicación 8
5.2.1. Azure WAF en Web Application Gateway 8
5.2.2. Amazon Web Services WAF (AWS WAF) 8
5.3. Soluciones de Seguridad de Redes 9
5.3.1. Ubuntu Uncomplicated Firewall 9
5.3.2. Azure Firewall 9
5.3.3. Amazon Web Services Network Firewall 9
5.4. Soluciones de Seguridad de Puntos Finales 9
5.4.1. Microsoft Intune 9
5.4.2. Cisco Meraki Systems Manager 10

6. Solución Propuesta 11
6.1. Solución 11
6.2. Plan de Implementación 12
6.3. Análisis de Riesgos de Implementación 13

7. Desarrollo del Proyecto 15
7.1. Implementación de Plan Director 15
7.2. Implementación de Firewalls en la Arquitectura Cloud de la Empresa . 15
7.3. Implementación de Microsoft Intune 17

8. Resultados y Análisis 18

9. Conclusiones y Discusión 20
Referencias 21

A. IBM Data Breach Report 2023 **22**

Capítulo 1

Introducción

Ceptinel es una Start-up chilena que inició sus operaciones en 2019, cuenta con una base de clientes compuesta principalmente por entidades financieras[1], como bancos, corredoras de bolsa y aseguradoras. La empresa ofrece servicios de anti-lavado de dinero, prevención de fraude y prevención de abuso de mercado. Estos servicios ayudan a las entidades financieras a proteger sus activos y a cumplir con regulaciones. También ofrece auditorías continuas, un canal de quejas externo o portal ético y monitoreo de procesos. La empresa ha logrado expandirse en varios países de Latinoamérica, incluyendo Perú, y Panamá, teniendo como objetivo de negocios llegar al resto de Latinoamércia comenzando por países como Colombia y México, para finalmente llegar a Estados Unidos. Desde una mirada técnica, la empresa ofrece a sus clientes dos opciones de alojamiento para sus servicios: la nube de Microsoft Azure[2] o las premisas de los clientes. Los servicios alojados en la nube son gestionados por Microsoft, mientras que los servicios alojados en las premisas de los clientes son gestionados por los propios clientes. Todas las soluciones constan de aplicaciones web, por lo tanto son accesibles por internet.

Hoy en día la empresa, un proveedor externo de servicios de prevención de fraude para entidades financieras, busca elevar sus estándares de ciberseguridad para cumplir con las exigencias de sus clientes. De no cumplir estas exigencias, esto podría llevar a la pérdida de clientes, o en el peor de los casos, a una brecha de datos o reducción de la disponibilidad de sus servicios. Según la Comisión para el Mercado Financiero (CMF), las entidades financieras deben exigir estándares de ciberseguridad a sus proveedores.

> *"La entidad, como parte de la gestión de sus servicios críticos externalizados, ha implantado un proceso de verificación periodica de la aplicación y cumplimiento de sus políticas de seguridad de la información y ciberseguridad, de manera de garantizar la adecuada protección de los activos de información que son utilizados o administrados por proveedores externos. Asimismo, monitorea permanentemente la infraestructura conectada con proveedores externos, y analiza e implementa medidas para detectar y mitigar potenciales amenazas a la ciberseguridad de la entidad"*(CMF, 2020b)

Dentro de estas exigencias, las principales a destacar se encuentran estipuladas en el capítulo 20-07 de la recopilación actualizada de normas de la CMF:

> *"La entidad debe cerciorarse que el proveedor de servicio mantiene un programa de seguridad de la información que le permita asegurar la confidencialidad, integridad, trazabilidad*

[1] Instituciones que ofrecen una gama de servicios financieros, como cuentas bancarias, préstamos, seguros, y productos de inversión.

[2] Microsoft Azure es una plataforma de computación en la nube.

> *y disponibilidad de sus activos de información y la de sus clientes. Estas condiciones deben ser consistentes con las políticas y estándares adoptados por la entidad y quedar incorporadas en el contrato de prestación de servicios."*(CMF, 2020a)

> *"La entidad debe asegurarse que el proveedor disponga de medidas efectivas de control y protección sobre ataques externos que persigan la indisponibilidad de los servicios contratados, como, por ejemplo, los de denegación de servicios. Adicionalmente, para los servicios criticos externalizados, la entidad deberá controlar la realización periodica por parte del proveedor de evaluaciones de vulnerabilidad de su infraestructura técnológica y testeos de penetración"*(CMF, 2020a)

Determinando que los clientes de Ceptinel deben exigir a la empresa contar con una infraestructura de seguridad que permita proteger principalmente la disponibilidad de sus servicios, asi como la confidencialidad, integriadad y trazabilidad de los datos proporcionados por las entidades financieras a las que sirve Ceptinel.

En caso de una brecha de datos, según el Data Breach Report de IBM, las pérdidas ante una brecha rondan los 3,69 millones de dólares estadounidenses(IBM, 2023a). El calculo de esta cifra se ve desglosado en el apéndice A.

Ceptinel ha realizado pruebas de penetración y análisis de vulnerbailidades para evaluar su nivel de riesgo en ciberseguridad. Como resultado, se han identificado ocho riesgos de criticidad alta (Naranjo) y dos riesgos de criticidad muy alta (Rojo).

Probabilidad Impacto	Raro	Poco Probable	Posible	Muy Probable	Casi Seguro
Despreciable					
Menor					
Moderado	Trojan Horses	Sniffing Attacks	DNS Spoofing	Phishing Password Attacks	
Mayor	Malware Attacks Birthday Attacks		Brute Force attacks Drive-by Attacks	Session Hijacking MITM Attacks	SSH port exploit
Catastrófico			Ransomware Dos/DDoS	Escalado Horizontal	

FIGURA 1.1: Matriz de riesgos informáticos Ceptinel. Elaboración propia.

Además, según el último reporte de análisis de vulnerabilidades de aplicación efectuado por un cliente, Ceptinel presenta las siguientes vulnerabilidades categorizadas por su severidad, este cliente destaca que estas vulnerabilidades deben ser mitigadas lo antes posible.

Factor	Problemas de severidad baja	Problemas de severidad media	Problemas de severidad alta
Application Security	3	3	1
DNS Health	1	0	0
Network Security	2	5	2
Patching Cadence	2	2	2

FIGURA 1.2: Resumen de Analisis de vulnerabilidades. Elaborado por cliente.

En un proceso de hacking ético interno se levantaron 10 vulnerabilidades dentro de todos los servicios cloud en Ceptinel. En específico, la evaluación de seguridad muestra vulnerabilidades de dependencias del lenguaje de programación JavaScript, por la no implementación de HSTS (HTTP Strict Transport Security), por conexión no encriptada y por certificados SSL[3]/TLS[4] autofirmados, no confiables o expirados.

Respecto al estado de la arquitectura de redes de Ceptinel, como se mencionó previamente, esta arquitectura está alojada en Microsoft Azure y se compone de recursos como máquinas virtuales, tarjetas de red, grupos de seguridad e IPs privadas y públicas (estáticas y dinámicas). Cabe destacar que, contrario a lo explicitado en el diagrama, los servidores sí presentan un Firewall, este es el Ubuntu Uncomplicated Firewall integrado en el sistema operativo Linux Ubuntu de los servidores.

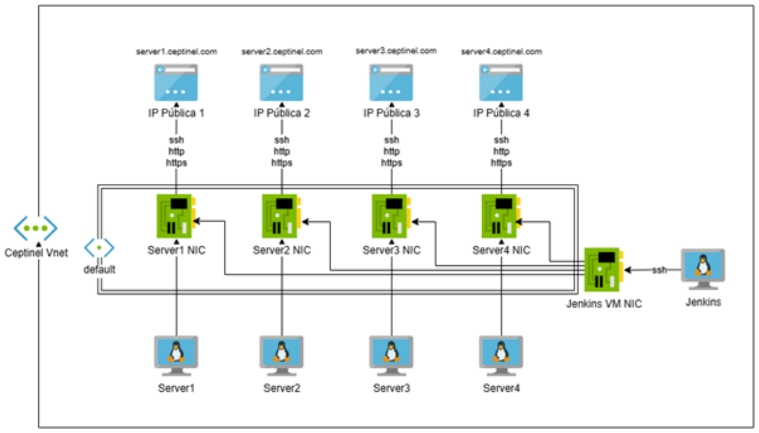

FIGURA 1.3: Arquitectura de redes de Ceptinel general. Elaboración propia.

En particular, para cada cliente, sus recursos se muestran en la Figura 1.4, se descata que los puertos HTTP[5], HTTPS[6] y SSH están abiertos, expuestos a internet y no se encuentran filtrados.

[3]Secure Socket Layer, es un protocolo de cifrado para comunicaciones en internet.
[4]Transport Layer Security, es un protocolo de cifrado para redes de computadores.
[5]Hypertext Transfer Protocol, se utiliza para comunicación no cifrada con aplicaciones web.
[6]Hypertext Transfer Protol Secure, se utiliza para comunicación cifrada con aplicaciones web.

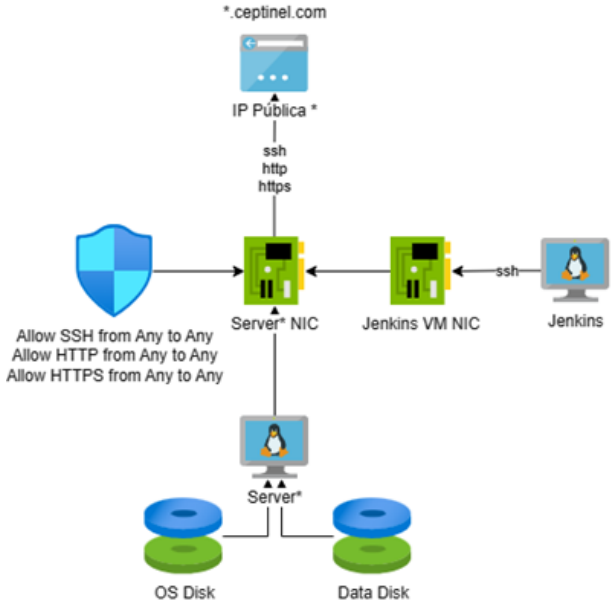

FIGURA 1.4: Arquitectura de redes de Ceptinel por cliente. Elaboración propia.

Finalmente, en evaluaciones de riesgo y campañas de concientización de ciberseguridad, se encontraron diversas vulnerabildades catalogables como de error humano, entre las cuales existen tres vulnerabilidades de alto riesgo (Naranjo) y una de riesgo muy alto (Rojo).

Probabilidad Impacto	Raro	Posible	Muy Probable	Casi Seguro
Despreciable	Despliegues inestables o no aprobados	No bloqueo de escritorios		
Moderado	Uso de sitios web riesgosos en la red de trabajo	Eliminación de información por error	Uso de software no autorizado Phishing	Empleados comparten credenciales de acceso a distintos servidores
Mayor		Divulgación de contraseñas por usuarios	Compartir información privilegiada por accidente	Uso de librerías no validadas

FIGURA 1.5: Matriz de riesgo de error humano Ceptinel

Capítulo 2

Objetivos

2.1. Objetivo General

Desarrollar e implementar un plan de acción integral de ciberseguridad que mejore significativamente la postura de seguridad de Ceptinel en 3 meses, logrando el cumplimiento total de los requisitos del cliente, aumentando la confianza con este y mitigando las vulnerabilidades encontradas en las áreas de aplicación, red, error humano y puntos finales.

2.2. Objetivos Específicos

1. Reducir el número de vulnerabilidades presentes en el procedimiento de hacking ético interno en 100 % en 3 meses de trabajo.
2. Remediar todas las vulnerabilidades descubiertas en el análisis de aplicación efectuado por el cliente en 3 meses de trabajo. Este analisis se encuentra en la Figura 1.2
3. En un plazo de 3 meses, desarrollar una estrategia de ciberseguridad que incluya concientización de empleados en temas de ciberseguridad y otras medidas que permitan mitigar el 30 % de los riesgos cuya causa principal sea el error humano presentes en la Figura 1.5.

Capítulo 3

Medidas de Desempeño

El desempeño del objetivo general será medido a través del conjunto de medidas de desempeño a utilizar en los objetivos específicos.
La eliminación total de vulnerabilidades y riesgos encontrados por el cliente se vería evidenciada en una reevaluación de vulnerabilidades de aplicación por parte del cliente. Esta misma medida de desempeño será utilizada para el objetivo de remediar las vulnerabilidades encontradas en el proceso de hacking ético interno.

$$\frac{CVi\ -CVf}{CVi} * 100 = \%\ de\ Vulnerabilidades\ mitigadas \tag{3.1}$$

Donde,
CVi= Conteo de Vulnerabilidades Inicial
CVf = Conteo de Vulnerabilidades Final

La implementación exitosa de una estrategia de seguridad se vería reflejada en la reducción del puntaje en la matriz de riesgo de errores humanos, este puntaje es asignado en base al riesgo expresado con colores en la matriz, en una escala de 1 a 4, siendo 4 los mas riesgosos. Se busca reducir el impacto de la situación de riesgo o la probabilidad de que ocurra una situación de riesgo.

$$\frac{Puntaje\ total\ en\ matriz\ de\ riesgo\ de\ error\ humano}{Puntaje\ total\ en\ matriz\ de\ riesgo\ pre\ solución} * 100 = \%\ de\ Mitigación \tag{3.2}$$

Capítulo 4

Metodología

Las metodologías utilizadas en este proyecto dependerán del área de ciberseguridad en la que se trabaje. Para el área de seguridad de aplicación, la metodología a utilizar es DevSecOps, que incorpora el pilar de seguridad en el proceso actual de desarrollo e integración continua DevOps y en las decisiones de arquitectura, con el fin de solucionar vulnerabilidades y amenazas presentes previo a su descubrimiento en los despliegues a producción. Para el área de seguridad de redes, se utilizará la metodología de evaluación de riesgos. Para esta metodología se utiliza la matriz de riesgo de diagnóstico, los controles existentes en la estructura cloud y otras herramientas de diagnóstico para desarrollar una estrategia de mitigación que lleva un proceso de monitoreo de solución, revisión, comunicación y documentación. Finalmente, para el área de error humano y protección de puntos finales, se utilizará una metodología de modelamiento de amenazas, en particular como un modelo centrado en las amenazas, en donde el enfoque principal son las posibles amenazas de error humano con mayor posibilidad de ocurrencia, se definen activos y límites de confianza, y en base a este modelo se define una estrategia de mitigación, de forma iterativa.

Capítulo 5

Estado del Arte

5.1. Solución de Plan de Acción de Ciberseguridad

5.1.1. Plan Director de Ciberseguridad

El plan director de ciberseguridad tiene un enfoque basado en el establecimiento de una estrategia de ciberseguridad clara y detallada, que incluye la implementación de un marco de seguridad, quick wins[1] para aplicaciones web y endpoints, y capacitación de empleados en seguridad. Esta solución es efectiva para organizaciones que desean tener un control total sobre su seguridad de la información, sin embargo, puede ser costosa de implementar en términos de tiempo y recursos.

5.2. Soluciones de Seguridad de Aplicación

Como soluciones de seguridad de aplicaciones web, los firewalls de aplicación (WAF) fueron investigados. Los firewalls de aplicaciones web ayudan a proteger las aplicaciones web de ataques maliciosos y tráfico de Internet no deseado, incluidos bots, inyecciones y denegación de servicio en la capa de aplicación. (Oracle, 2023)

5.2.1. Azure WAF en Web Application Gateway

El Azure Web Application Gateway es un balanceador de tráfico que permite administrar el tráfico web de aplicaciones en la nube. Esta solución se utiliza comúnmente en aplicaciones web individuales y puede estar configurada en su modo WAF, que examina todo el tráfico web HTTP y HTTPS para proteger la aplicación contra amenazas, vulnerabilidades y *exploits* conocidos. Esta opción se encuentra en un rango de precio medio, estimando costos de $280 dólares estadounidenses mensuales según el Azure Pricing Calculator, en base a las horas en que se encuentra activo y el nivel de tráfico en el Application Gateway.

5.2.2. Amazon Web Services WAF (AWS WAF)

AWS WAF es un firewall de aplicaciones web que permite proteger las aplicaciones web contra ataques comunes, como la inyección de código SQL, el scripting entre sitios (XSS) y los ataques de fuerza bruta. AWS WAF se puede utilizar para proteger aplicaciones web alojadas en Amazon Elastic Compute Cloud, Amazon Elastic Container Service y Amazon CloudFront. Este servicio tiene un costo de $0.005 dólares estadounidenses por cada solicitud HTTP o HTTPS.

[1] Los quick wins son medidas de bajo costo relativo en términos de tiempo y dinero, con un impacto positivo inmediato.

5.3. Soluciones de Seguridad de Redes

Como soluciones de seguridad de red, se investigaron los firewall de red. Estos son dispositivos que se colocan entre una red interna y una red externa para controlar el tráfico de red y bloquear el tráfico no autorizado. Los firewalls de red pueden ayudar a proteger las organizaciones de ataques externos, como la intrusión, el robo de datos y la propagación de malware.

5.3.1. Ubuntu Uncomplicated Firewall

Este es el firewall predeterminado del sistema operativo Ubuntu utilizado en los servidores de Ceptinel. Este firewall por defecto está desactivado y su característica principal es filtrar tráfico en base a puertos o nombre de servicio. Este servicio es gratuito.

5.3.2. Azure Firewall

Azure Firewall es un servicio de seguridad de firewall de red inteligente que se aloja en la nube y ofrece protección para servicios cloud en Azure. Se trata de un firewall de próxima generación que permite bloquear tráfico de red con reglas en base a puertos, URL y aplicaciones. Además, esta solución provee de tecnología Threat Intelligence. Esta opción depende del tipo de firewall que se ordene (Basic, Standard, Premium) siendo el estimado en Basic de $288 dólares estadounidenses mensuales, Standard de $900 dólares estadounidenses mensuales y Premium de $1200 dólares estadounidenses mensuales de acuerdo con Azure Pricing Calculator.

5.3.3. Amazon Web Services Network Firewall

AWS Network Firewall es un servicio de firewall de red administrado que proporciona protección para las cargas de trabajo en AWS. Se trata de un firewall de próxima generación que permite bloquear tráfico de red con reglas en base a puertos, direcciones IP y aplicaciones. AWS Network Firewall también proporciona tecnología Threat Intelligence para ayudar a identificar y bloquear ataques conocidos. Este firewall tiene un costo de $0,395 dólares estadounidenses por hora de uso.

5.4. Soluciones de Seguridad de Puntos Finales

Como soluciones de seguridad de puntos finales, se investigaron los administradores de dispositivos móviles, estas son soluciones que permiten a organizaciones administrar y proteger dispositivos móviles de sus empleados sea cual sea su sistema operativo.

5.4.1. Microsoft Intune

Microsoft Intune es una solución de administración de endpoints que permite a un administrador tener control sobre el dispositivo. Ofrece servicios para la gestión de acceso de usuarios, definición de políticas y reglas de acceso a aplicaciones y/o páginas web, eliminación de información en caso de pérdida o robo de dispositivo e integración de servicios de defensa Microsoft Defender contra amenazas en todos los dispositivos registrados en el directorio activo. Según Microsoft, el costo del plan

Microsoft Security + Mobility E3 que contiene Microsoft Intune es de $36 dólares estadounidenses por usuario al mes.

5.4.2. Cisco Meraki Systems Manager

Cisco Meraki Systems Manager es otra solución de administración de endpoints que proporciona una plataforma unificada para administrar todos los dispositivos conectados a la red. Ofrece servicios para la gestión de acceso de usuarios, la definición de políticas y reglas de acceso a aplicaciones y páginas web, la eliminación de información en caso de pérdida o robo de dispositivo, y la integración de servicios de seguridad de Cisco. Este servicio tiene un valor de $14,99 dólares estadounidenses por dispositivo al mes.

Capítulo 6

Solución Propuesta

6.1. Solución

La solución escogida es un plan director de ciberseguridad, que se apoye con el marco de ciberseguridad de los Center of Internet Security Critical Security Controls en su octava versión (CIS Controls V8), una lista de medidas de seguridad críticas desarrolladas por el Center of Internet Security para ayudar a organizaciones a protegerse contra las amenazas cibernéticas. CIS desarrolló un herramienta de autoevaluación para los controles, llamada CIS Controls Self Assessment Tool (CIS CSAT), que será utilizada par facilitar el diagnostico, priorización e implementación de los controles.

Este plan director busca abordar el área de seguridad de aplicación y seguridad de redes utilizando ambos firewalls de Azure (de aplicación y de redes) en conjunto, buscando reformar la arquitectura de redes actual de Ceptinel. Estos recursos han sido elegidos debido a que los servidores de Ceptinel se encuentran en la nube de Azure, entonces, por temas de compatibilidad y simpleza de implementación, las soluciones de seguridad de redes y de aplicación debiesen pertenecer a Azure.

Además, este plan contempla la implementación de Microsoft Intune con el fin de proteger los puntos finales otorgados por la empresa. Esto se debe principalmente a que esta solución ofrece un mayor control a nivel administrativo en términos de políticas y aplicaciones, y debido a que se utilizan múltiples dispositivos por usuario.

6.2. Plan de Implementación

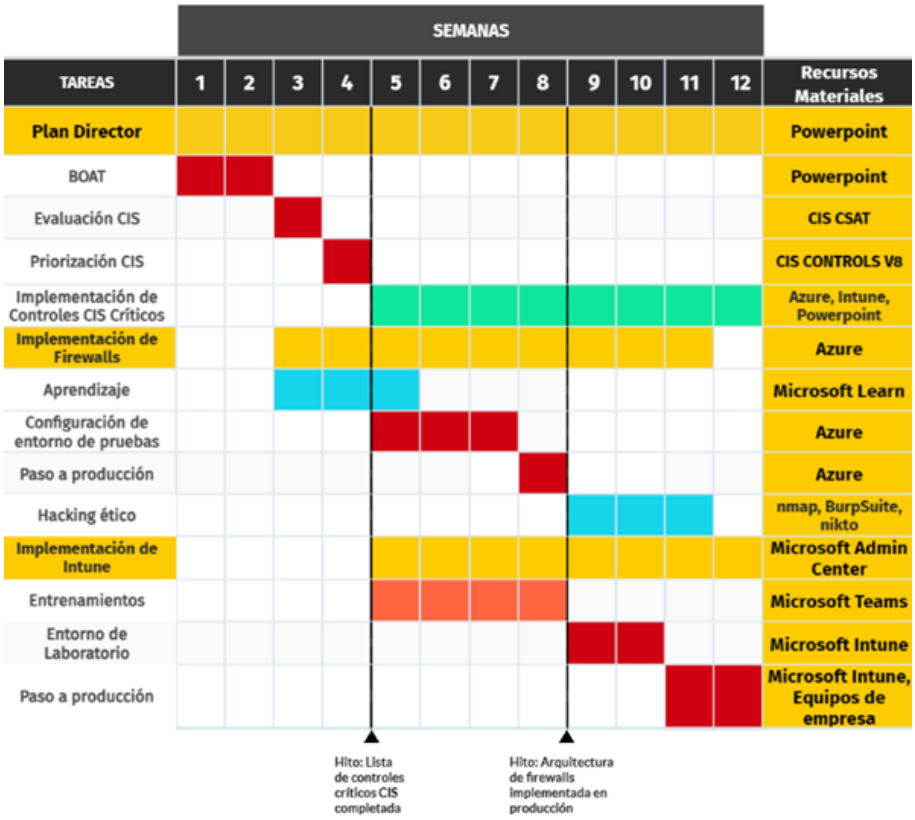

FIGURA 6.1: Plan de implementación del proyecto. Elaboración propia.

6.3. Análisis de Riesgos de Implementación

Probabilidad Impacto	Raro	Poco Probable	Posible	Muy Probable	Casi Seguro
Despreciable					
Menor			Mal recibimiento de las medidas de seguridad por parte de empleados		
Moderado		Insuficientes recursos o pericia para una ejecución efectiva	Vulnerabilidades de terceros	Disrupción de sistemas de trabajo funcionales durante implementación	
Mayor		Implementación inadecuada de plan director	Falta de monitoreo y mantención de las soluciones		
Catastrófico		Brecha de datos durante la implementación			

FIGURA 6.2: Matriz de riesgos informáticos Ceptinel. Elaboración propia.

De los riesgos presentados en la matriz de riesgos, se han priorizado los siguientes para su mitigación durante la implementación del plan director de ciberseguridad:

1. Brecha de datos durante la implementación: Para mitigar este riesgo, se ha diseñado un proceso de instalación de firewalls que garantiza que los servidores no tengan acceso a Internet hasta que el firewall esté activo. Además, se ha implementado el cifrado de datos durante el proceso de instalación, generando copias cifradas de los discos de datos y replicándose en un ambiente isolado sin conexión al entorno anterior.
2. Falta de monitoreo y mantención de las soluciones: Para abordar este riesgo, se ha implementado un dashboard de monitoreo de recursos de nube Azure. Asimismo, se ha establecido un programa de revisión y mantenimiento periódico de las soluciones implementadas. Durante la implementación, se realiza una semana de revisión en modo pasivo del WAF y otra semana en modo activo.
3. Implementación inadecuada de plan director: Con el objetivo de asegurar una implementación adecuada del plan director de ciberseguridad, se han definido procesos y directrices claras en el mismo. Esto incluye un cronograma detallado, asignación de roles y responsabilidades, así como un proceso de revisión y seguimiento continuo para evaluar el progreso y realizar ajustes si es necesario. Además, se ha asignado personal especializado y se ha establecido un

programa de formación interna para garantizar la pericia necesaria en la ejecución del plan.

4. Potencial disrupción en sistemas de trabajo funcionando durante la implementación: Para minimizar el impacto en los sistemas en funcionamiento durante la implementación, se han realizado pruebas exhaustivas de compatibilidad antes de implementar las medidas de seguridad. Asimismo, se ha establecido una comunicación efectiva con los clientes y otros equipos involucrados para coordinar la implementación de manera que se eviten las posibles disrupciones.
5. Vulnerabilidades de terceros: Se han establecido acuerdos claros con los proveedores de servicios tercerizados para garantizar el cumplimiento de los estándares de seguridad requeridos. Se realizan evaluaciones regulares de seguridad de los servicios tercerizados y se mantiene un inventario actualizado de parches y actualizaciones para mitigar posibles vulnerabilidades.
6. Insuficientes recursos o pericia para una ejecución efectiva del plan director: Se ha asegurado que los recursos necesarios estén disponibles para llevar a cabo el plan director de ciberseguridad de manera efectiva. Se realiza una evaluación mensual de las necesidades de recursos y habilidades para asegurar una ejecución exitosa.
7. Mal recibimiento de las medidas de seguridad por parte de los empleados: Se ha implementado un enfoque integral para fomentar una cultura de seguridad en toda la organización. Se han fortalecido los programas de concientización y capacitación en seguridad, destacando la importancia de las medidas implementadas y cómo cada empleado puede contribuir a la protección de la información y los activos de la empresa. Además, se han establecido políticas claras y procedimientos para reportar incidentes de seguridad, de manera que se promueva una actitud receptiva y proactiva hacia la mejora de la ciberseguridad en la empresa.

Cada uno de estos riesgos identificados ha sido abordado mediante el uso de políticas, procedimientos y mejores prácticas de seguridad. Las medidas de mitigación han sido diseñadas y adaptadas a las necesidades específicas de la empresa, con el objetivo de garantizar una implementación exitosa del plan director de ciberseguridad y de los quick wins asociados.

Capítulo 7

Desarrollo del Proyecto

7.1. Implementación de Plan Director

El Plan director de ciberseguridad de Ceptinel comenzó con una evaluación a nivel de negocio utilizando el framework BOAT. Esto permitió obtener una comprensión integral de los objetivos del negocio y la importancia de sus activos críticos, sentando las bases para la implementación de estrategias de mitigación de riesgos.

Posteriormente, se llevó a cabo un diagnóstico utilizando la herramienta CSAT (Controls Self Assessment Tool) de CIS para evaluar el nivel de cumplimiento de los CIS Controls V8 en la empresa. Con base en esta evaluación, se creó una lista de controles prioritarios a implementar. La priorización de los controles se basó en la facilidad de implementación, dando énfasis a aquellos que pueden ser implementados rápidamente, conocidos como Quick Wins. Entre estos Quick Wins se incluyen la implementación de firewalls en la arquitectura cloud de Ceptinel y la implementación de Microsoft Intune en los dispositivos de la empresa.

7.2. Implementación de Firewalls en la Arquitectura Cloud de la Empresa

La implementación de los Firewall se realizó siguiendo la metodología Risk Assessment, que se enfoca en la identificación y mitigación de amenazas y vulnerabilidades. A continuación, se describen los principales pasos llevados a cabo durante el proceso:

Se identificaron máquinas virtuales de Azure como servidores para la aplicación web Ceptinel. Estos servidores cuentan con bases de datos internas y dirección IP pública estática.

Se realizó una evaluación exhaustiva de las amenazas y vulnerabilidades asociadas. Se identificaron problemas de seguridad reportados en procesos de hacking ético, clasificados con alta severidad en Application Security y Network Security.

Se evaluó la probabilidad e impacto de las vulnerabilidades identificadas, teniendo en cuenta los resultados de la matriz de riesgo previamente establecida, así como las vulnerabilidades encontradas en las auditorías de hacking ético mencionadas anteriormente.

Se analizaron los controles de seguridad existentes. El aplicativo Ceptinel cuenta con protección básica contra ataques de inyección de código SQL y las máquinas virtuales disponen de una protección básica contra ataques de denegación de servicios

al ser un recurso de Microsoft Azure. Además estos servidores cuentan con el uso activo de Ubuntu Uncomplicated Firewall.

Se llevó a cabo una determinación de los riesgos basada en una matriz previamente establecida, considerando la probabilidad e impacto de las amenazas identificadas.

Se implementó una estrategia de mitigación de vulnerabilidades mediante la incorporación de un WAF. Se diseñó una arquitectura de redes que permitió separar el tráfico protegido por el WAF (HTTP y HTTPS) y el tráfico de SSH (por requisito de la empresa, este puerto debe estar expuesto a internet, pero no necesariamente expuesto al cliente, por lo que se decidió separar todo este tráfico y que utilice otra dirección IP), todos protegidos por el firewall de red de Azure. Además, se incorporó un espacio de análisis de *logs*, así logrando almacenar toda la información relevante que estos firewalls puedan almacenar.

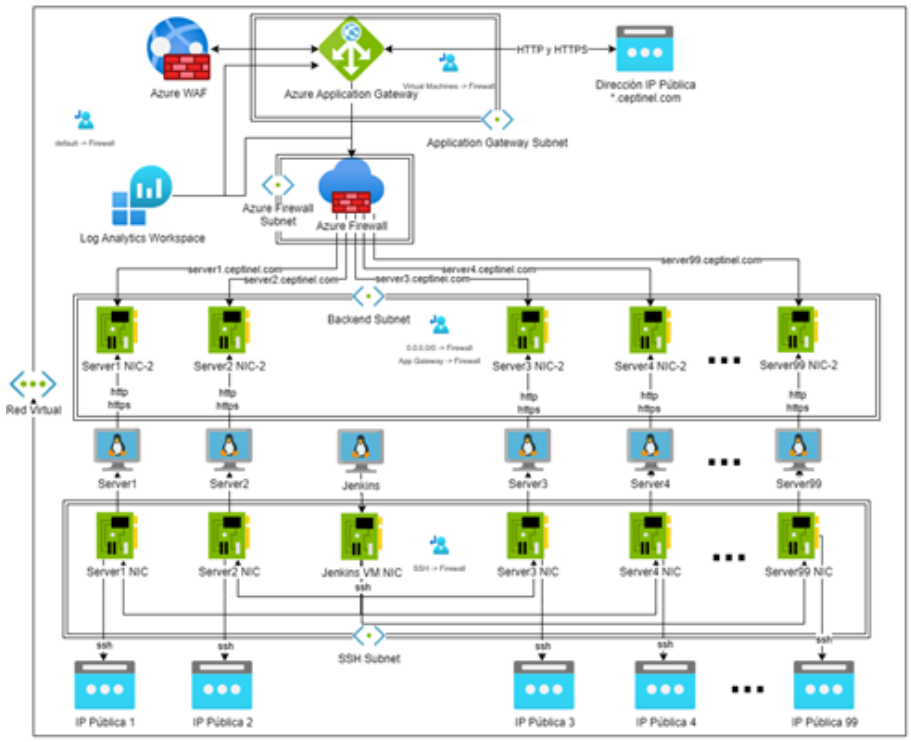

FIGURA 7.1: Nueva arquitectura de redes Ceptinel. Elaboración propia.

Se realizó un monitoreo y revisión continuos de los firewalls, incluyendo pruebas de penetración, escaneos de red y observación de su funcionamiento en modo pasivo y activo.

Se documentó detalladamente el proceso de instalación, configuración, y pruebas realizadas a la arquitectura implementada. También, se comunicaron las acciones realizadas al cliente, desde el apagado de los servidores hasta la activación del WAF en modo activo.

7.3. Implementación de Microsoft Intune

Para la implementación de Microsoft Intune, se siguió un enfoque basado en la metodología de modelado de amenazas utilizando *Process for Attack Simulation & Threat Analysis* (PASTA), cerciorando que el enfoque sea centrado en las amenazas de error humano. El proceso incluyó varias sesiones de entrenamiento en colaboración con el equipo de Microsoft México. Durante estas sesiones, se estableció un entorno de laboratorio que permitió la conexión de dos equipos (endpoints) diferentes. Se definieron y exploraron varias políticas de seguridad y se analizaron diversas opciones disponibles en la herramienta Intune.

El objetivo principal era utilizar Intune como solución para mitigar vulnerabilidades y amenazas relacionadas con errores humanos. Mediante la aplicación de la metodología de modelamiento de amenazas PASTA, se buscaba identificar los posibles escenarios de ataque y las amenazas que podrían surgir debido a errores o malas prácticas por parte de los usuarios para así evitarlos utilizando políticas de Microsoft Intune.

Sin embargo, debido a complicaciones de calendarización y limitaciones de tiempo dentro del marco temporal del proyecto, no fue posible completar el paso a producción de la herramienta Intune. Aunque no se logró implementar completamente en este proyecto, las sesiones de entrenamiento y las pruebas en el entorno de laboratorio proporcionaron conocimientos valiosos sobre las capacidades y opciones de seguridad que ofrece Intune para mitigar amenazas y vulnerabilidades.

Capítulo 8

Resultados y Análisis

Durante la implementación del plan director de ciberseguridad y los quick wins asociados, se lograron los siguientes avances en la protección de los activos de la empresa y la mitigación de riesgos:

1. Implementación parcial de Microsoft Intune: A pesar de que no se pudo completar la implementación de Microsoft Intune dentro del marco temporal establecido en el proyecto, se logró avanzar en su configuración y preparación. La falta de consideración de incidentes en el plan de implementación fue un factor que afectó su total despliegue. Sin embargo, se espera que en el futuro se concluya la implementación de Intune para brindar una administración más segura de los dispositivos de la empresa.
2. Impacto positivo del WAF: Si bien algunos empleados tuvieron una recepción negativa a la nueva arquitectura WAF, debido a mayores tiempos de respuestas o algunos problemas durante su configuración, en términos de seguridad, su implementación fue positiva y efectiva. Tanto el último proceso de análisis de vulnerabilidades por parte del cliente como el ultimo proceso de hacking ético interno confirmaron que el WAF logró mitigar exitosamente todas las vulnerabilidades asociadas al área de seguridad de aplicación, con la excepción de la no implementación de HSTS (HTTP Strict Transport Security) en el servidor, esto fue levantado en el proceso de hacking ético interno, y el uso de una versión desactualizada de la librería de JavaScript Angular.js en la aplicación web, levantado en el análisis de vulnerabilidades del cliente, ambas excepciones fueron remediadas al día siguiente de ser informadas, logrando marcar un 100 % de mitigación de vulnerabilidades tanto para el análisis de vulnerabilidades de cliente, como para el hacking ético interno.
3. Impacto del Plan director de ciberseguridad: La evaluación de CIS Controls V8 ha permitido establecer un plan de controles a implementar para elevar el nivel de ciberseguridad de la empresa después del proyecto. A través de los quick wins implementados, se logró implementar el 60 % de los controles que no se encontraban completados al inicio del proyecto, mientras que el restante 40 % fue abordado mediante propuestas de mitigación dentro del plan director de ciberseguridad. Si bien el enfoque se ha centrado principalmente en la rapidez de implementación, es relevante destacar que, posterior a las implementaciones, una evaluación final de controles identificó la completitud de un total de 41 controles de los 56 evaluados, lo que representa un 73 % de completitud de controles del marco.
4. Oportunidades de mejora identificadas: Durante la implementación, se identificaron áreas de mejora tanto en la empresa como en el proyecto. Estas incluyen

la atención a los procesos de respaldo y recuperación, optimización de las reglas y excepciones del firewall de aplicación, así como la revisión y clarificación de las políticas y procedimientos de ciberseguridad.

Capítulo 9

Conclusiones y Discusión

En conclusión, el proyecto de implementación de medidas de ciberseguridad ha sido exitoso en fortalecer la postura de seguridad de la Ceptinel y mitigar los riesgos asociados a posibles amenazas y vulnerabilidades. La implementación de quick wins ha permitido proteger de manera efectiva los activos de información de la empresa, garantizando la disponibilidad, confidencialidad e integridad de los servicios de Ceptinel.

A pesar de los desafíos encontrados durante la implementación, los resultados han sido ampliamente reconocidos y valorados por los clientes y los cargos superiores de la empresa. Sin embargo, es importante señalar que la recepción de las medidas de seguridad por parte de los empleados ha sido mixta, con una respuesta inicial negativa por parte de los empleados debido a los cambios y restricciones impuestos. Esto ha resaltado la necesidad de una mayor concientización y capacitación sobre ciberseguridad para fomentar una cultura de seguridad sólida y promover una comprensión más amplia de la importancia de las medidas implementadas.

Aunque se han logrado avances notables en la implementación de controles de seguridad prioritarios, es importante reconocer que no todos los objetivos del proyecto se han cumplido por completo. El objetivo de desarrollar una estrategia de ciberseguridad que incluya la concientización de los empleados y la mitigación del 30 % de los riesgos causados principalmente por el error humano no se ha logrado debido a la no implementación de Microsoft Intune. Sin embargo, los quick wins implementados han permitido una mejor protección de los activos y una reducción total de las vulnerabilidades identificadas en los servidores web.

Referencias

AWS. (2023). *Network firewall, cloud firewall - aws network firewall.* https://aws.amazon.com/network-firewall/.

CMF. (2020a). Externalización de servicios. En *Recopilación actualizada de normas: Normas de carácter general* (p. 1-56).

CMF. (2020b). Gestión de seguridad de la información y ciberseguridad. En *Recopilación actualizada de normas: Normas de carácter general* (p. 3).

for Internet Security, C. (2023). *Cis critical security controls version 8.* https://www.cisecurity.org/controls/v8.

IBM. (2022). *Security threat intelligence index.* https://www.ibm.com/security/data-breach/threat-intelligence.

IBM. (2023a). *Cost of a data breach report.* https://www.ibm.com/reports/data-breach.

IBM. (2023b). *What is mobile device management (mdm)?* https://www.ibm.com/topics/mobile-device-management.

Meraki, C. (2023). *Mobile device management (mdm) — systems manager.* https://meraki.cisco.com/products/systems-manager/.

Microsoft. (2023a). *What is azure web application firewall on azure application gateway?* https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview.

Microsoft. (2023b). *What is microsoft intune?* https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune.

Microsoft. (s.f.a). *Azure application gateway features.* https://learn.microsoft.com/en-us/azure/application-gateway/features.

Microsoft. (s.f.b). *Microsoft 365 enterprise e3.* https://www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab.

Microsoft. (s.f.c). *What is azure firewall?* https://learn.microsoft.com/en-us/azure/firewall/overview.

Microsoft. (s.f.d). *Zero-trust network for web applications with azure firewall and application gateway.* https://learn.microsoft.com/en-us/azure/architecture/example-scenario/gateway/application-gateway-before-azure-firewall.

Oracle. (2023). *What is a waf (web application firewall)?* https://www.oracle.com/dk/security/cloud-security/what-is-waf/.

OWASP. (2012). *Pasta process for attack simulation and threat analysis.* Descargado de `https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf`

Ubuntu. (2023). *Ubuntu security - firewall.* https://ubuntu.com/server/docs/security-firewall.

Apéndice A

IBM Data Breach Report 2023

El costo de una brecha de datos se calcula utilizando costos basados en actividades, identificando y asignando costos de acuerdo al uso actual. Cuatro procesos relacionados con actividades forjan un rango de gastos asociados con una brecha de datos en una organización: Detección y escalamiento, notificación, Repuesta post-brecha y pérdidas de negocio

Detección y Escalamiento

Actividades que permiten a la compañía detectar una brecha, incluyendo:

- Actividades forenses y de investigación
- Evaluación y servicios de auditorías
- Manejo de crisis
- Comunicación con ejecutivos y junta directiva

Notificación

Actividades que permiten a la compañía notificar a interesados, reguladores de protección de datos y otros externos, incluyendo:

- Emails, cartas, llamadas salientes o notificaciones generales a interesados
- Determinación de requerimientos regulatorios
- Comuncación con reguladores
- Contacto con expertos externos

Respuesta Post-Brecha

Actividades que ayudan a las víctimas de una brecha a comunicarse con a compañía y realizar activivades de reparación a las vítcimas y reguladores, incluyendo:

- Mesas de ayuda y comunicación entrante
- Servicios de monitoreo de creidos y servicios de protección de identidad
- Emisión de nuevas cuentas o tarjetas de crédito
- Gastos legales
- Descuento en productos
- Multas regulatorias

Pérdidas de Negocio

Actividades que intentan minimizar la pérdida de clientes, disrupción de los servicios y pérdidas en ganancias, incluyendo:

- Disrupción de los servicios de la empresa y pérdidas de ingresos por baja de los servicios
- Costo de perder clientes y dificultad para obtener clientes nuevos
- Daño reputacional y decrecimiento de la buena voluntad