UNIVERSIDAD ANDRES BELLO

Facultad de Ingeniería

Plataforma Chilena de Concientización de Seguridad de la Información – PCCSI

Tesis para la Obtención del Grado de Magíster en Gestión de las Tecnologías de la Información y Telecomunicaciones

Autores:
Christian Campodónico Ortiz, Antonio Ormazábal Sbarbaro

Profesor Tutor:
PhD. David Ruete Zúñiga

Santiago de Chile, 2021.

Universidad Andrés Bello

ÍNDICE DE CONTENIDOS

Universidad Andrés Bello

ÍNDICE DE TABLAS

Universidad Andrés Bello

ÍNDICE ILUSTRACIONES

1. INTRODUCCIÓN

1.1. Introducción

El 80% de los problemas de seguridad de las empresas son causados por los usuarios (Kaspersky Labs, 2019), ya sea por desconocimiento o en algunos casos por obtener un beneficio, todas las estadísticas indican que los usuarios en las empresas continúan siendo el eslabón más débil en la cadena de seguridad de la información. (Mitnick & Simón, 2005)

Educar a los usuarios para fortalecer sus conocimientos, y entregarles técnicas y tips de cómo actuar, cuando se encuentran ante un intento de phishing o un posible virus es vital para evitar ciberataques y pérdida de información.

Debido a la intensificación de la necesidad de mejorar la seguridad de la información, muchas organizaciones han establecido programas de concientización sobre la seguridad de la información, para asegurarse de que sus empleados estén informados y sean conscientes de los riesgos de seguridad, protegiéndose a sí mismos y a su rentabilidad. Para que un programa de concientización sobre seguridad añada valor a una organización, y al mismo tiempo contribuya al ámbito de la seguridad de la información, es necesario disponer de un conjunto de métodos para estudiar y medir su efecto. (Krugera & Kearney, 2006)

No se puede implementar un programa de seguridad de la información eficaz sin poner en marcha un programa de concientización y capacitación de los empleados para abordar la política, los procedimientos y las herramientas. El aprendizaje consiste en tres elementos clave:

1. Concientización, que se utiliza para estimular, motivar y recordar a la audiencia lo que se espera de ellos.

2. Entrenamiento, el proceso que enseña una habilidad o el uso de una herramienta requerida.

3. Educación, la capacitación especializada y profunda necesaria para apoyar las herramientas o como proceso de desarrollo profesional.

Existen en el mercado algunas plataformas de concientización que ayudan a este proceso, pero el problema principal es que los contenidos educativos no están hechos para la realidad chilena o el solo hecho de ver un video con voces mexicanas o españolas desalienta el proceso educativo.

Kevin Mitnick en su Libro "El arte de la Intrusión" (Mitnick & Simón, 2005) escribe una frase que es utilizada comúnmente entre los especialistas en seguridad *"al final, los ataques de Ingeniería Social ocurren cuando la gente es estúpida, o más comúnmente simplemente ignorante acerca de las prácticas comunes de seguridad"*. Por lo tanto, pensamos que la ignorancia se puede corregir mediante procesos educativos adecuados que ocurran como una constante en el tiempo, hasta que logren generar un hábito de seguridad.

1.2. Motivación

En la actualidad a nivel mundial existen varias plataformas orientadas a educar sobre temas de ciberseguridad, no obstante, como se indicaba en la introducción sus contenidos no están ajustados a la realidad nacional y sus costos por usuario pueden ser muy altos para la realidad de las empresas chilenas. El principal problema actualmente son las amenazas digitales, intentos de extorsión o de robo de información son cada vez más sofisticadas y su número cada vez más alto.

En el último informe de Ciberseguridad de IBM (IBM.com, 2020) encontramos los siguientes puntos:

Los investigadores del IBM X-Force Threat Intelligence, declaran que, durante el año 2019, hubo tres principales vectores de infección inicial en las empresas: Phishing (31%), Scan y Explotación de red (30%) y Credenciales Robadas (29%), siendo los ataques denominados Phishing y Spear Phishing la mayor fuente de amenazas a la información, seguido muy de cerca por los ataques de red. En estos tres casos el factor humano es predominante.

- El número de ataques a sistemas industriales ha crecido en más de 2.000%, siendo las redes del tipo scada o industriales un blanco apetecible por los delincuentes cibernéticos.
    - El año 2016 La empresa de suministro eléctrico de la región ucraniana de Ivano-Frankvisk dejó sin electricidad a miles de hogares en (alrededor de 1,5 millones de habitantes, que requieren electricidad para temperar sus casas) por culpa del troyano BlackEnergy que afectó el sistema de control e ingresó mediante un correo electrónico fraudulento. (The Register, 2016)
- Más de 8.500 millones de archivos resultaron infectados, lo que supone un crecimiento del 200% con respecto al año anterior.
    - En 2017 en el caso conocido como Panama Papers 2,6 terabytes de información fue enviada a periodistas de todo el mundo con información sobre el uso de paraísos fiscales por parte de políticos.

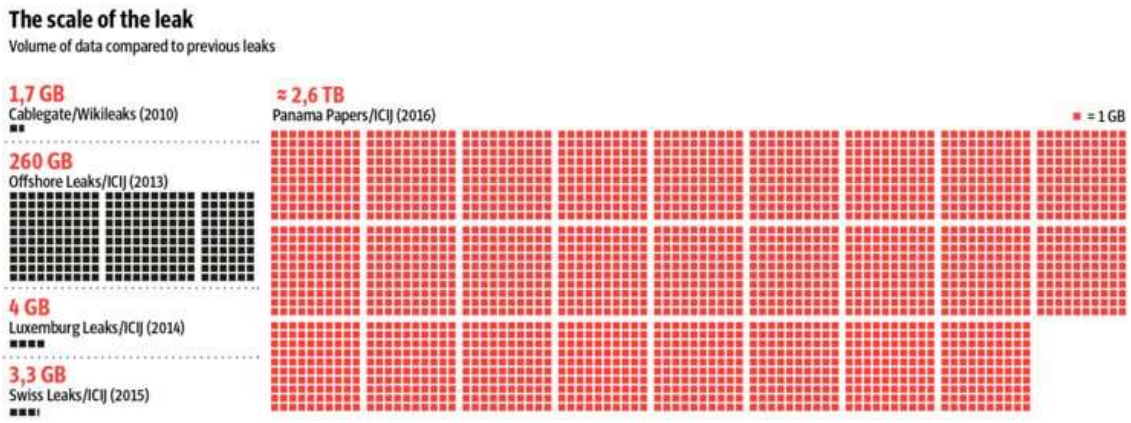


ILUSTRACIÓN 1 CANTIDAD DE INFORMACIÓN DIVULGADA EN INCIDENTES DE SEGURIDAD

La Ilustración 1, muestra la cantidad de información divulgada en distintos casos de robo de información conocidos

- La industria de los servicios financieros sigue siendo el blanco preferido para los cibercriminales.
    - En 2018, más de 10 millones de dólares fueron sustraídos mediante transferencias internacionales en el Banco de Chile.
- El ransomware se ha convertido en el tipo de ataque más «popular» en 2019

> "Las empresas acostumbran a tener alguna solución tecnológica de seguridad [pero] la ingeniería social elude a todas las tecnologías, incluyendo el firewall. La tecnología es fundamental, pero, debemos observar a las personas y los procesos. La ingeniería social es una forma de piratería informática que utiliza tácticas de influencia". (Mitnick & Simón, 2005)

En Chile Según los registros del SII en 2019 (www.sii.cl, 2019), el número de empresas activas es de un total de 1.271.895, que informan 9.526.391 trabajadores dependientes. De este universo de trabajadores hay un gran porcentaje que utiliza computador y requiere capacitación en temas de seguridad de la Información.

En la siguiente tabla se observa el número de empresas según número de trabajadores, que conforman el total del universo laboral chileno

TABLA 1 NÚMERO DE EMPRESAS SEGÚN NÚMERO DE TRABAJADORES EN CHILE

Tamaño	Número de trabajadores	Número de empresas	Porcentaje del total
Micro	0-9	239.920	79,2%
Pequeña	10-49	49.311	16,3%
Mediana	50-249	10.838	3,6%
Grande	250 y más	2.764	0,9%
Total		**302.833[2]**	**100%**

Fuente: Elaboración propia en base a la Tercera Encuesta Longitudinal de Empresas.
Nota: los trabajadores incluyen a los dueños y socios que trabajen en la empresa.

Para ahondar más en los números y basándonos en el boletín (Ministerio de Economía Fomento y Turismo, 2015) sobre los resultados de la tercera encuesta longitudinal de empresas del Ministerio de economía, elaborado en octubre de 2015 por la unidad de estudios, podemos asegurar los siguientes puntos:

Del Universo de trabajadores dependientes informados,

- 84,6% cuenta con al menos un dispositivo activo para fines laborales.
- 46 % de los trabajadores usa dispositivos para el trabajo.
- 74,9% usa Software de Oficina.
- 75,8% Utiliza Internet.
- 94,5% lo usa para Comunicación vía correo y mensajería.
- 82,7 % realiza tramites en el SII.

Estas cifras nos demuestran que el mercado es lo suficientemente amplio como para requerir un plan continuo de capacitación y concientización para todos los usuarios de las organizaciones, el cual esté diseñado y personalizado para cada empresa según el perfil de sus trabajadores y que sea una plataforma web que no requiera conocimientos previos y cuyos contenidos sean cercanos y atrayentes para el gran número de trabajadores

Actualmente las normativas legales y marcos de trabajo de seguridad como ISO27001 y NIST o la ley de protección de datos personales europea GDPR incorporan la concientización de usuarios como un proceso importante y hasta

obligatorio dentro los procesos corporativos. De esta manera la ISO 27001 (ISO/IEC 27001:2013(E), 2013), indica en los controles auditables del anexo A lo siguiente;

- 7.2.2 Concientización, educación y capacitación en SI: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.
- 7.2.3 Proceso disciplinario: Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.

Por su parte, la Ley General de Protección de datos europea (GDPR) indica que: Se debe crear una política de seguridad que garantice que los miembros de su equipo conozcan la seguridad de los datos. Debe incluir orientación sobre seguridad de correo electrónico, contraseñas, autenticación de dos factores, encriptación de dispositivos y VPN.

Otra normativa que exige la capacitación de usuarios es la PCI-DSS, para el manejo de pagos por medios electrónicos, que indica en su control 12.6, implementar un programa formal de concientización de seguridad para que todo el personal sea consciente de la importancia de la seguridad de los datos del titular de la tarjeta "así como para educar al personal" al contratarlo y al menos anualmente "

Pese a que los requerimientos normativos lo exigen y que existen plataformas de apoyo a la concientización, los resultados no siempre son los esperados y la participación de los usuarios es baja, principalmente por que los contenidos son poco atingentes a la realidad chilena.

A continuación, se muestra el resultado de una campaña de concientización vía newsletter realizado en una compañía chilena. (fuente reservada), en el cual se

aprecia que, de un universo de 500 usuarios, solo un 7% de estos comenzó la campaña y sólo un 4% la finalizó, por lo tanto, su efectividad fue muy baja. Consultada la fuente, indica que es principalmente debido a que los contenidos de la campaña no eran atractivos para el usuario.

El proceso de concientización de Seguridad de la Información en las empresas no es fácil de llevar a cabo, se requiere el compromiso del resto de la organización comenzando desde las áreas directivas hacia abajo y debe abordar a todas las áreas que manejen información de la empresa, ya sea digital o física

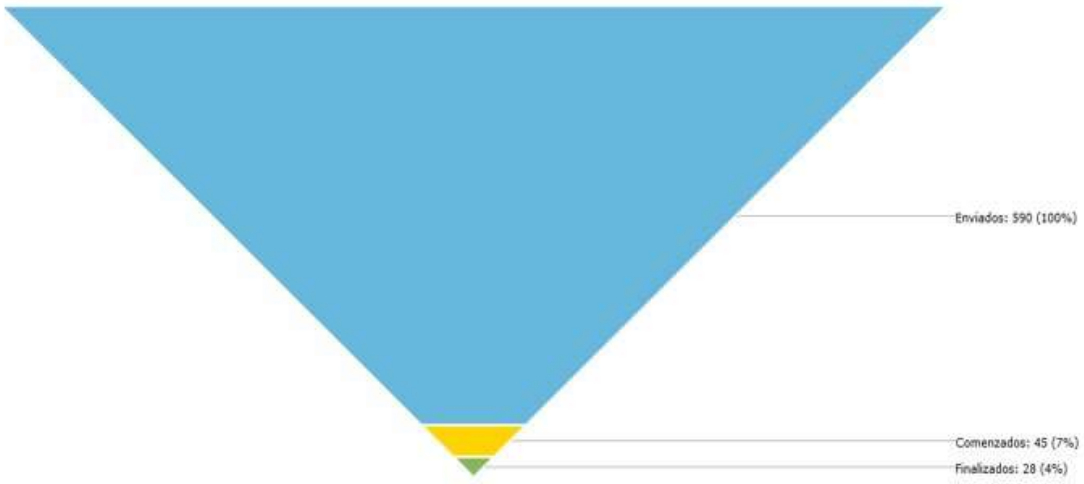


ILUSTRACIÓN 2 TASA DE EFECTIVIDAD DE UNA CAMPAÑA NORMAL DE CONCIENTIZACIÓN

1.3. Marco de Trabajo

El marco de trabajo a utilizar será diseñar una plataforma web, basada en los servicios de nuestra nube privada de alta disponibilidad, que permita generar el envío de correo electrónico, recopilar estadísticas de uso, subir y publicar videos educativos y realizar la autenticación correcta de usuarios con la velocidad y escalabilidad necesarias para cubrir el universo de usuarios a los que se pretende

llegar. Se utilizará una plataforma de pago por uso debido a que solo se requiere invertir en infraestructura de cómputo inicial y se implementaran servicios cognitivos que pueden ayudar a generar información de mejor calidad para el análisis de los usuarios.

El alcance estará limitado a la presentación del problema y en el diseño conceptual de un método de trabajo que incluya: Diseño de solución tecnológica, plan de costos, y diseño de plan de trabajo para la generación de contenidos locales, los cuales se basará en el uso de temáticas de contingencia nacional y en lo posible con personajes de conocimiento público.

2. IDENTIFICACIÓN DEL PROBLEMA

A continuación, y luego de una lluvia de ideas podremos analizar las causas principales seleccionadas que tienen relación con la problemática planteada en este documento. Como resultado podremos evidenciar que en base a diversas causas obtendremos como origen el efecto central, para esto se utilizará un diagrama de Ishikawa que permitirá visualizar las causas como espinas hasta llegar a la cabeza como problema central, al cual se espera dar una solución.

2.1. Diagrama de Causa y Efecto

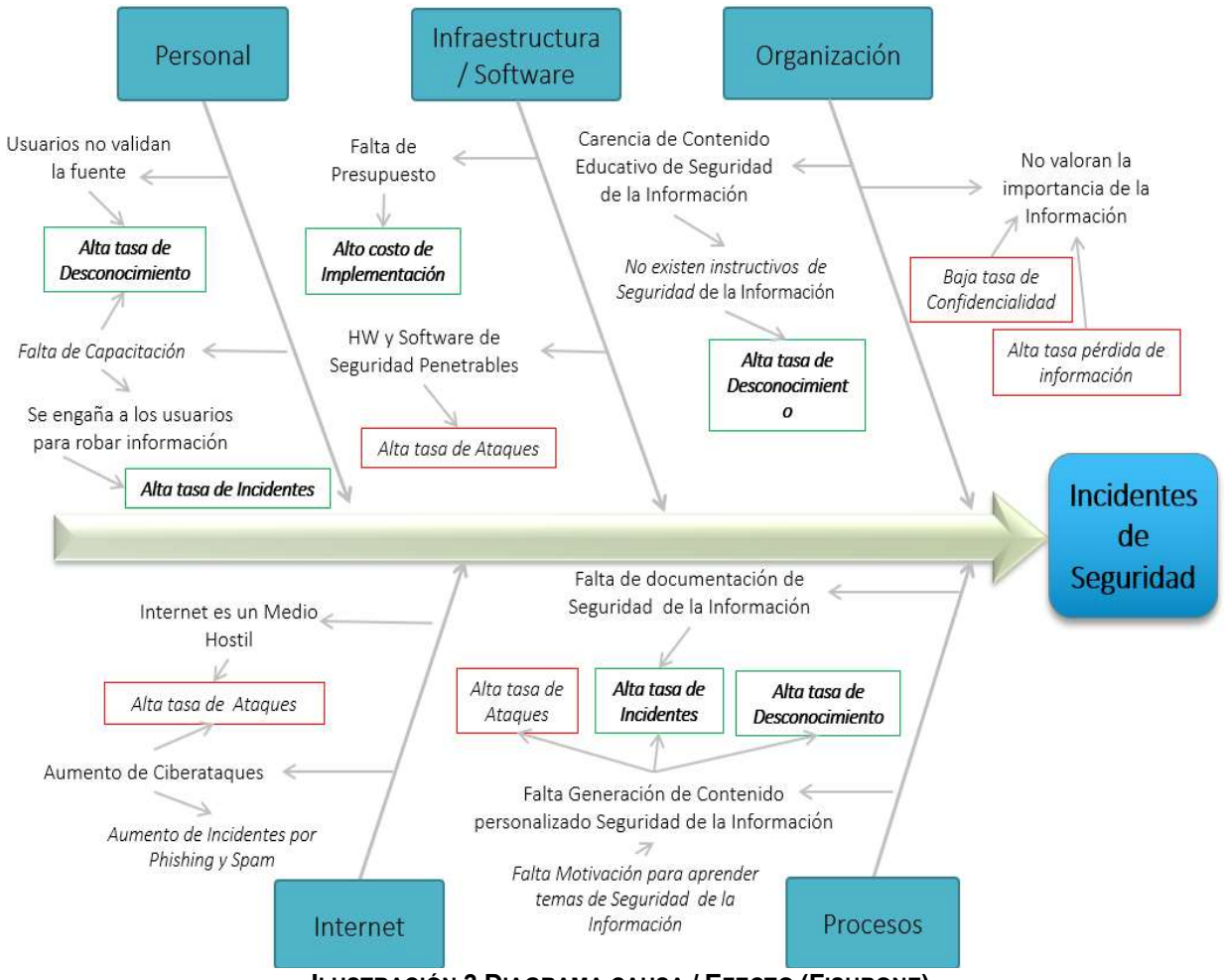


ILUSTRACIÓN 3 DIAGRAMA CAUSA / EFECTO (FISHBONE)

2.2. Identificación de las Causas

A continuación, se detallan las causas que conforman las espinas mayores denominadas causas principales, y algunas causas menores que generan estas espinas mayores.

TABLA 2 DEFINICIÓN DE CAUSA EN DIAGRAMA CAUSA - EFECTO

N°	Tabla de Causas del Diagrama de Ishikawa	ID
1	**La Organización**	**C-1**
1.1	No valorar la importancia de la Información	1.1
1.1.1	Baja Tasa de Confidencialidad	1.1.1
1.1.2	Alta tasa de perdida de información	1.1.2
1.2	Carencia de Contenido Educativo de Seguridad de la Información	1.2
1.2.1	No existen instructivos de Seguridad de la Información	1.2.1
1.2.2	Alta tasa de desconocimiento	1.2.2
2	**Los Procesos**	**C-2**
2.1	Falta de documentación de Seguridad de la Información	2.1
2.1.1	Alta tasa de Incidentes	2.1.1
2.2	Falta Generación de Contenido personalizado Seguridad de la Información	2.2
2.2.1	Alta tasa de Ataques	2.2.1
2.2.2	Alta tasa de Incidentes	2.2.2
2.2.3	Alta tasa de Desconocimiento	2.2.3
2.2.4	Falta Motivación para aprender temas de Seguridad de la Información	2.2.4
3	**La Infraestructura y Software**	**C-3**
3.1	Falta de Presupuesto	3.1
3.1.1	Alto costo de Implementación	3.1.1
3.2	HW y SW de Seguridad Penetrables	3.2
3.2.1	Alta tasa de Ataques	3.2.1
4	**Internet**	**C-4**
4.1	Es un medio Hostil	4.1
4.1.1	Alta tasa de Ataques	4.1.1
4.2	Aumento de Ciber ataques	4.2
4.2.1	Aumento de Incidentes por Phishing y Spam	4.2.1
5	**Personal**	**C-5**
5.1	Usuarios no validan la fuente	5.1
5.1.1	Alta tasa de Desconocimiento	5.1.1
5.2	Falta de capacitación	5.2
5.2.1	Se engaña a los usuarios para robar información	5.2.1
5.2.2	Alta tasa de Incidentes	5.2.2

2.3. La Organización (C-1)

La información es uno de los activos más valiosos que puede tener una organización (Najar Pacheco & Suárez Suárez, 2015). El valor real de esa información depende de cómo es gestionada, del tiempo que se emplea para procesarla y traducirla en el lanzamiento de productos o servicios y de en qué medida se utiliza eficientemente y es cualitativamente mejor que la de las empresas competidoras.

Cuando la organización no valora la importancia de su información está condenada a su fracaso, dado que expone uno de sus bienes más preciados y la confidencialidad de su información o se genera una pérdida de datos producto de actos maliciosos, lo que sin duda afectará su productividad, imagen, bienes y hasta posiblemente los llevarán a la quiebra o simplemente beneficiarán a su competencia.

Muchas veces las organizaciones están muy preocupadas de su propio negocio y la alta gerencia no pone foco en temas con relación a la seguridad de la información, por lo tanto no generan contenido interno en temas de seguridad, descuidando o exponiendo su información, lo cual se traduce en una evidente carencia de contenido educativo de seguridad TI, debido principalmente a que no existen instructivos en esta área o no hay personal dedicado a preocuparse de estos temas que son críticos para todas las organizaciones y existe una alta tasa de desconocimiento entre los usuarios.

2.4. Los Procesos (C-2)

Cuando las organizaciones no están en conocimiento de los potenciales riesgos que existen, al no atender de buena forma los problemas de la seguridad de la información, dado que generalmente escasean los procesos para prevenir o remediar de buena forma las contingencias y no se realiza entrega de estos

temas a los usuarios. Y si la documentación es entregada, no es en forma sistémica o con un plan global o el contenido entregado no es personalizado y no está en línea con la realidad nacional ni de la empresa, lo cual los hace poco cercanos y pierden eficacia. Si a lo anterior sumamos que los usuarios están preocupados solo en cumplir con sus labores diarias por las cuales son medidos y remunerados, no existe una motivación para aprender temas de seguridad de la Información y simplemente no revisan la documentación entregada o la completan solo por cumplir, pero no les queda el aprendizaje que se requiere para prepararse en caso de algún ciberataque, concluyendo que la alta tasa de desconocimiento de los usuarios desmotivados por aprender acerca de seguridad de la información, genera mayor tasa de ataques aumentando los incidentes de seguridad.

2.5. La Infraestructura y Software (C-3)

Cuando hablamos de infraestructura y software nos encontramos con diversas realidades en cada organización, lo que está relacionado generalmente al número de usuarios y presupuestos que disponen para resguardar sus sistemas e información, muchas veces hay que lidiar con la falta de presupuesto por los altos costos de implementación o a veces aunque posiblemente se cuenta con el presupuesto necesario para realizar mejoras, podríamos decir que todo el hardware y software de seguridad son penetrables en algún porcentaje, dado que solo basta configurar incorrectamente un componente para provocar una grieta en la pared (Mitnick & Simón, 2005). También sabemos que los ataques han aumentado exponencialmente, durante el primer trimestre de 2020, Fortinet documentó un aumento del 17% en los virus en enero, un incremento del 52% en febrero y un alarmante aumento del 131% en marzo en comparación con los mismos meses en 2019. (Fortinet, Q1-2020). Si además no hay un buen mantenimiento a las plataformas de seguridad estas grietas en la pared se transformaran en orificios por donde aumentara la tasa de ataques.

2.6. Internet (C-4)

Los resultados de Fortinet Threat Intelligence Insider Latin America para el primer trimestre de 2020 (Fortinet, Q1-2020) revelan un aumento en los intentos de atraer víctimas desprevenidas a sitios maliciosos, por ende, no es duda que internet es un medio hostil que va en aumento y no se detendrá. Además, también en el mismo informe y como se indicó en el punto anterior los ciber ataques aumentaron considerablemente en comparación con el año 2019, reportando un promedio de aproximadamente 600 nuevas campañas de phishing por día en marzo de 2020, confirmado el aumento de Spam y Phishing (Fortinet, Q1-2020).

2.7. El Personal (C-5)

El bien más preciado de toda organización son las personas (Mitnick & Simón, 2005), pero lamentablemente también son el eslabón más débil de la cadena de Seguridad (Mitnick & Simón, 2005), dado que generalmente son engañados para robar su información y la de su organización porque no tienen conciencia de los peligros que conlleva acceder a sitios desconocidos o el ejecutar archivos sospechosos sin validar su fuente u origen, confirmando que existe una alta tasa de desconocimiento en los empleados lo que en el corto plazo provocara una alta tasa de incidentes de seguridad.

La norma ISO 27001 en sus controles A.7.2.2 y A.7.2.3 (ISO/IEC 27001:2013(E), 2013) establece que las personas relacionadas con el sistema de gestión de seguridad de la información deben estar capacitadas y concientizadas. E incluso debiese generarse un sistema de amonestación

2.8. Identificación del Efecto – Incidencias de Seguridad

Todas las causas expuestas anteriormente generan un efecto final en el aumento de incidencias de seguridad que dañan a la organización, por ende, debemos trabajar en mitigarlas en los aspectos que sean posible.

Nuestro propósito es enfocarnos en las causas revisadas anteriormente, generando una plataforma chilena de seguridad con contenido personalizado para educar a los usuarios fortaleciendo sus conocimientos, y entregarles técnicas y tips de cómo actuar cuando se encuentran ante un intento de phishing o un posible virus. Es vital educarlos para evitar ciberataques y pérdida de información. A diferencia de las plataformas disponibles para la capacitación de usuarios en conceptos de seguridad de la información, nuestra propuesta principal es que los contenidos sean cercanos, conocidos y locales de manera de impactar adecuadamente al usuario final y lograr que ocurra el aprendizaje.

Nuestra propuesta es armar una plataforma 100% chilena con contenidos 100% chilenos, adaptados a nuestra realidad y capaz de utilizar los últimos eventos nacionales conocidos para formar conciencia en los usuarios. Una plataforma que entregue contenidos y sea capaz de simular ataques de phishing, ransomware entre otros.

La plataforma será denominada Plataforma Chilena de Concientización de Seguridad de la información (en adelante PCCSI) y debe estar enfocada en resolver las problemáticas de contenidos, facilidad del aprendizaje, costos asociados a la realidad chilena y debe ejecutarse sobre una plataforma tecnológica resiliente que permita escalar rápidamente en cantidad de usuarios y cuyos costos estén asociados al consumo mensual de recursos tecnológicos

2.8.1. Los Problemas

A continuación, se presentan los problemas que abordaremos para dar solución con nuestra plataforma, la cual será explicada de mejor forma en los próximos capítulos.

TABLA 3 IDENTIFICACIÓN DE PROBLEMAS

N°	Problemas	ID
1	Alta tasa de Desconocimiento	P01
2	Alta tasa de Incidentes	P02
3	Alto costo de Implementación	P03

3. OBJETIVOS E HIPÓTESIS

Con los temas analizados en el punto anterior en cuanto a las causas y efecto, hemos definido los objetivos de nuestro proyecto, una hipótesis y el alcance con sus limitaciones.

3.1. Objetivo General

Nuestro objetivo general consiste en diseñar e implementar servicios a través de una Plataforma Chilena de Concientización de Seguridad de la Información – PCCSI para reducir las incidencias de seguridad de las organizaciones.

Será una solución 100% chilena, con contenidos 100% chilenos, basados en marcos referenciales internacionales adaptados a nuestra realidad y capaz de utilizar los últimos eventos nacionales conocidos para formar conciencia en los usuarios de las organizaciones.

3.2. Objetivos Específicos

Para lograr el objetivo principal planteado, se han definido los siguientes objetivos específicos que tienen como foco dar solución a las causas y sub-causas de los problemas mencionados en el diagrama causa Efecto:

- Disminuir la Alta tasa de Desconocimiento de información.
- Disminuir la Alta tasa de Incidentes.
- Disminuir los Altos costos de Implementación.

3.3. Métricas de los Objetivos Específicos

A continuación, se presentan las métricas consideradas para evaluar el éxito de los objetivos específicos planteados en la sección anterior,3.2 para ello se considera la nomenclatura de la siguiente tabla.

TABLA 4 IDENTIFICADOR DE OBJETIVOS ESPECÍFICOS

Objetivo Específico	Identificador
OE01	Disminuir la Alta tasa de Desconocimiento de información
OE02	Disminuir la Alta tasa de Incidentes
OE03	Disminuir los Altos costos de Implementación

Se realiza la definición de acuerdo con el valor actual de la métrica (VAM) y criterio de éxito esperado (CEM) de cada una de ellas, el resumen de estas se observa en siguiente tabla.

TABLA 5 MÉTRICA DE OBJETIVOS ESPECÍFICOS

Objetivo Específico	Métrica / Unidad	VAM	CEM
OE01	CFA: Correos Falsos Abiertos	74%	40%
	TCE: Total Correos Enviados		
	TC: Tasa Conocimiento		
	TC = (CFA / TCE) * 100		
OE02	NIS: Número de Incidentes de Seguridad	29%	20%
	TCE: Total Correos Enviados		
	TI = Tasa de Incidentes		
	TI = (NIS / TCE) * 100		
OE03	CIE: Costo / Usuario Plataforma Existente	30	>30
	USD Anual * Usuario		

- OE01: TC: corresponde al porcentaje de correos falsos abiertos durante las pruebas a realizar.

- OE02: TI: Corresponde al porcentaje de Incidentes de Seguridad creados a partir de los usuarios que ingresarán información personal durante las pruebas a realizar.
- OE03: CIE: Costo Anual por usuario en dólares americanos en la plataforma a desarrollar.

3.3.1. Trazabilidad

A continuación, se presenta una matriz de trazabilidad donde aprecian los problemas que resuelve el éxito de cada uno de los objetivos específicos planteados en las Secciones Anteriores.

TABLA 6 MATRIZ DE TRAZABILIDAD

N°	Objetivos Específicos	Problemas		
		P01	P02	P03
1	OE01	X	X	
2	OE02		X	
3	OE03			X

3.4. Hipótesis

Diariamente se registra que el número de incidentes de ciberseguridad o seguridad de la información va en constante aumento y los daños producto de estos ataques son más cuantiosos en relación con la información divulgada o secuestrada, lo que repercute en un impacto financiero para la empresa afectada. Dentro de estos incidentes de seguridad el 80% es provocado por usuarios sin los conocimientos adecuados para detectar los engaños y prevenirlos. Un proceso de educación adecuado requiere que sus contenidos sean presentados

de una manera cercana y adecuada al alumno/usuario de manera de ser correctamente comprendidos y se genere el conocimiento.

El mercado nacional requiere de plataformas tecnológicas que le permitan educar en conceptos de ciberseguridad y finalmente bajar los incidentes de seguridad que cada día van creciendo producto del desconocimiento de los usuarios y la ineficacia de complejos sistemas de seguridad los cuales son altamente costosos.

En base a lo anterior esta Tesis abordara el desarrollo de una plataforma Chilena de Concientización de Seguridad de la Información, basada en contenido local y que tiene por objetivo bajar el desconocimiento de los usuarios en temas de seguridad de la información y en consecuencia bajar la cantidad de Incidentes de Seguridad a un costo menor que las plataformas existentes.

4. ALCANCE DEL PROYECTO

A continuación, se presenta el alcance del proyecto, indicando cuales aspectos de la problemática presentada en sección problemas serán abordados o bien se buscará una solución. Además de presentar las limitaciones y supuestos que enmarcan el desarrollo de este.

4.1. Alcances

Diseñar una Plataforma Chilena de Concientización de Seguridad de la información (www.pccsi.cl) con Definición de Requerimientos técnicos y Diseño de plataforma TI híbrida según buenas prácticas de infraestructura tecnológica.

OE01 Disminuir la Alta tasa de Desconocimiento de información.

Diseñar los siguientes módulos en la plataforma:

- Programación (Agenda de actividades durante el año).
- Módulos de capacitación.
- Evaluaciones.
- Informes.

OE02 Disminuir la Alta tasa de Incidentes.

Diseñar los siguientes módulos en la plataforma:

- Programación (Agenda de actividades durante el año).
- Plantillas de contenidos.
- Campañas temáticas educativas.
- Informes de desempeño.

OE03 Disminuir los Altos costos de Implementación.

- Definir tecnología resiliente que permita una modalidad de pago por uso de manera a mantener costos bajos y por consecuencia lograr un precio más bajo a los usuarios.

4.2. Limitaciones al Alcance

El desarrollo de la presente tesis se acota a lo planteado en las definiciones del punto anterior. No se realizará la implementación completa de la solución ni se ejecutará su plan comercial. Los costos presupuestados serán estimados utilizando las calculadoras de estimación de costos de las plataformas de los fabricantes, cloud y onpremise a utilizar y el desarrollo técnico se planteará a modo de maqueta.

4.3. Supuestos del Alcance

El desarrollo de la plataforma propuesta supone contar con los recursos monetarios y de mano de obra de personal especialista necesarios.

Se supone contar con los requerimientos legales de constitución de empresa y definiciones de participación de accionistas clara.

5. MARCO TEÓRICO

5.1. Ingeniería Social

Cuando nos referimos a Seguridad de la Información, esta debe ser entendida como protección de los contenidos informativos tanto físicos como a nivel digital, es decir ya sea un documento impreso o un correo electrónico lo importante es su contenido más que su contenedor. De esta manera, un Incidente de Seguridad de la Información se define como una serie de eventos inesperados o no deseados que tienen la probabilidad significativa de comprometer las operaciones del negocio y de amenazar la Seguridad de la Información. (Asociación Española de Normalización, 2016). El compromiso puede ocurrir por factores tecnológicos o humanos, y pueden deberse a errores o en el peor de los casos a acciones malintencionadas de terceros.

El acto de irrumpir un sistema informático y realizar acciones malintencionadas sobre estos sistemas tecnológicos se denomina Cracking (Jazdzewski & Jazdzewski, 1995). Sin embargo, como la misma definición de The Jargon File lo indica : "Contrariamente al mito generalizado, esto no suele implicar un salto misterioso de brillantez hacker, sino más bien la persistencia y la repetición obstinada de un puñado de trucos bastante conocidos que explotan las debilidades comunes en la seguridad de los sistemas de destino" En el 80% de las veces (Kaspersky Labs, 2019) estas debilidades comunes existen porque los usuarios son engañados y realizan acciones que permiten que se efectúe el ataque, como por ejemplo abrir un correo inadecuado o descargar un archivo malicioso. Según uno de los hackers más famosos, Kevin Mitnick, "Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores." (Mitnick & Simón, 2005). Según Mitnick, los ataques de ingeniería social muchas veces son llevados a cabo solo con ayuda de un teléfono y están basados en cuatro principios básicos y comunes a todas las personas:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir No.
- A todos nos gusta que nos alaben.

Bajo estos principios los primeros engaños a los usuarios eran mediante llamadas telefónica realizando suplantaciones de identidad. Con el aumento del uso del correo electrónico en las empresas las técnicas de engaño evolucionaron hacia mensajes de identidades falsas que permiten realizar acciones más sofisticadas como inducir a que el usuario entregue datos personales, instale alguna aplicación o realice alguna acción que permita abrir la puerta para que el cracker acceda. Uno de los engaños más conocidos se utiliza para pedir dinero mediante engaños y se refiere al llamado “Príncipe Nigeriano”: Esta estafa consiste en ilusionar a la víctima con una fortuna inexistente y persuadirla para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna. Las sumas solicitadas son bastante elevadas, pero insignificantes comparadas con la fortuna que las víctimas esperan recibir. La estafa nigeriana puede entenderse como una versión contemporánea del cuento del tío. (Wikipedia.org, s.f.). Actualmente este tipo de engaño se realiza vía correo electrónico y han surgido múltiples variantes que defraudan a personas de todo el mundo, es el llamado pishing que explicaremos más adelante.

Normalmente para acceder a un sistema externo y obtener información se debe realizar 7 distintas actividades o etapas: Reconocimiento, Preparación, Distribución, Explotación, Instalación, Comando y Control y Acciones sobre los objetivos (Instituto Nacional de Ciberseguridad de España (INCIBE), 2020). Cualquiera de estas etapas requiere mucha preparación y estudio, por lo que puede tomar semanas o meses realizar un ataque exitoso. La ingeniería social es la manera más rápida para acceder a un sistema externo, ya que es más fácil engañar a las personas que a los sistemas.

5.2. Phishing y Spear Phishing

Como se explicó en el capítulo anterior el phishing es una técnica de ingeniería social que utiliza el engaño mediante correo electrónico o sitios web falsos que intentan obtener dinero o datos personales de la víctima. Por su parte, el Spear Phishing es un tipo de engaño dirigido a una empresa o persona en particular, en el que el atacante conoce a la víctima o su información básica y utiliza herramientas especialmente preparadas para atacar a esta víctima, por lo tanto, es más elaborado y difícil de detectar.

El phishing es el tipo de ataque que más ha crecido en el último tiempo. Solo en el 2018 las detecciones de phishing por correo electrónico aumentaron un 250%, según los informes mensuales que realiza Microsoft (Microsoft, s.f.), esta tendencia continuó en alza durante 2019, de hecho, Durante el mes de enero de 2019, el equipo de Seguridad de Microsoft detectó un promedio de 225.000 intentos diarios de phishing y en febrero de 2019 se incrementaron hasta los 300.000. El 14 de febrero se alcanzó un pico máximo de 480.000, casi medio millón de ataques durante el Día de San Valentín pasado, fecha en la que muchas personas están en su smartphone y redes sociales.

Hoy en día, con la ampliación de los servicios de ciberseguridad de la compañía analiza más de 6,5 billones de incidencias de seguridad al día. (Microsoft, s.f.)

Existen diferentes tipos de phishing y se pueden clasificar de la siguiente manera:

a) Deceptive Phishing.

Se trata de tipo más común de engaño, en el cual, los ciberdelincuentes se hacen pasar por una empresa de confianza (robo de identidad) y le envían al usuario un mensaje de correo electrónico falso con los colores, tipografía y logotipos de la empresa. Los cibercriminales actúan como representantes solicitando algún tipo de información personal como los datos de la tarjeta de crédito, etc.

También puede ser que el texto del correo contenga un enlace malicioso que envía al usuario a una página web fraudulenta donde se le solicita los datos de inicio de sesión.

ILUSTRACIÓN 4 MUESTRA DE CORREO FRAUDULENTO

Según el CSIRT del gobierno de Chile, solo en una semana, se detectaron cuatro sitios fraudulentos en el país (Equipo de Respuesta ante Incidentes de Seguridad informática, s.f.). A estos debiesen sumarse los no detectados o reportados, por lo tanto, los intentos de engaño son más comunes de lo esperado.

b) Malware-Based Phishing.

Este tipo de engaño implica la ejecución de un software malicioso en los computadores de los usuarios. El malware se puede introducir como archivo adjunto en un correo o como archivo descargable en un sitio web. Su objetivo es comprometer el dispositivo de la víctima y obtener información o recompensa por liberar los archivos comprometidos (Ransomware).

c) Search Engine Phishing.

Se produce cuando los cibercriminales crean o pagan entradas falsas para que los buscadores como Google redireccionen al usuario a páginas web

fraudulentas. Logran que se indexen legítimamente en los motores de búsqueda y los usuarios las encuentran en una búsqueda normal.

d) Content-Injection Phishing.

Este tipo de ataque los cibercriminales reemplazan parte del contenido de un sitio web legítimo con contenido falso diseñado para engañar o desviar al usuario a entregar su información confidencial. Este tipo de ataque es más sofisticado porque requiere vulnerar el servidor web del sitio víctima.

Uno de los casos más conocido de este tipo de phishing, fue la sufrida por el banco Español Sabadell, en el que durante un corto periodo de tiempo aparecieron un par de anuncios de pago en las dos primeras posiciones de los resultados de búsqueda de Google. Ingresando en cualquiera de ellos, el usuario llegaba a una página web fraudulenta que solo se diferenciaba de la oficial por su URL.

e) Man-in-the-Middle Phishing.

Es el tipo de ataque phishing más difícil de detectar y de realizar, ya que el cibercriminal debe estar en la misma red que la víctima y se sitúa entre el computador del usuario y el servidor, grabando y manipulando así, la información que se transmite entre ellos.

f) DNS-Based Phishing.

En esta modalidad también conocida como Pharming. Los delincuentes manipulan los sistemas de DNS, resolución de nombres o archivos hosts de una de un sistema para que las solicitudes de consulta de URL devuelvan una dirección falsa y las comunicaciones sean dirigidas a un sitio web falso.

La consecuencia es que los usuarios desconocen que la página web donde están ingresando información confidencial está controlada por estos cibercriminales.

5.3. Ransomware

El ransomware es un programa de software malicioso que infecta los computadores y exigen el pago de dinero (recompensa – ransom) para restablecer el funcionamiento del sistema. Por lo general cifrando sus datos o amenazando con difundirlos. Este tipo de malware es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña. (Kaspersky Labs, 2019).

Es una de las ciberamenazas más peligrosas a nivel mundial, ya que un ataque exitoso de este tipo podría tener múltiples impactos sobre una organización, desde el daño reputacional y la exposición de información estratégica confidencial, hasta la interrupción completa del negocio. Incluso, si vamos más allá de lo tecnológico, en septiembre de 2020, se dio a conocer la primera muerte de una persona por consecuencia de un ataque de ransomware a un hospital en Alemania, que no pudo ser atendida por fallos en los sistemas.

ILUSTRACIÓN 5 PANTALLA DE RECOMPENSA DE UN RANSOMWARE

Si bien los primeros casos se denunciaron en Rusia en 2005, desde entonces, las estafas se han propagado a todo el mundo y nuevas variantes siguen

sumando víctimas. En septiembre de 2013, apareció CryptoLocker, que dirigió sus ataques a todas las versiones del sistema operativo Windows. Este ransomware logró infectar cientos de miles de computadoras personales y sistemas empresariales. Las víctimas, de manera inconsciente, abrieron correos electrónicos procedentes supuestamente de servicios de soporte al cliente de FedEx, UPS, DHL y otras empresas. Después de activarse, mostraba un cronómetro en la pantalla que exigía un pago de 300 dólares en un plazo de 72 horas.

El método más común utilizado por los cibercriminales al momento de infectar un equipo es a través de ataques de Phishing. En esta acción utilizan información cada vez más dirigida, personalizada y específica para generar confianza y engañar a las potenciales víctimas. El objetivo es hacer que abran archivos adjuntos o hagan clic en enlaces para descargar archivos PDF, Word u otros documentos maliciosos. Otra técnica muy utilizada por los atacantes consiste en aprovecharse de una configuración predeterminada de Windows que oculta la extensión de los archivos conocidos, por ejemplo, un adjunto que parece llamarse "factura.pdf", corresponde realmente a “factura.pdf.exe”.Otra técnica empleada es adjuntar archivos comprimidos con password, con esto evaden el análisis de seguridad automatizado de algunas plataformas de correo electrónico. (Bacian, 2020).

En su informe para el CSIRT del gobierno de chile, el investigador Germán Fernández, Líder Red Team y Threat Intelligence de la empresa CronUp, explica que el ransomware es una amenaza que está generando billones de dólares de ganancias para quienes perpetran estos ataques, a costa de miles de víctimas que pierden dinero, ven paralizadas sus operaciones y recientemente, incluso ha costado la vida de una persona. (Bacian, 2020)

El modelo de negocio RaaS (Ransomware As a Service) ha permitido a los operadores de ransomware separar las funciones, principalmente entre el equipo desarrollador y los grupos llamados “afiliados” quienes se encargan de ganar el acceso inicial, para comprometer la red corporativa objetivo. Se estima que tanto

los ataques independientes como el modelo de negocio RaaS, enfocado en objetivos de alto valor (BGH o Big Game Hunting), generarán para el año 2021 una ganancia superior a los $20 billones de dólares para el cibercrimen.

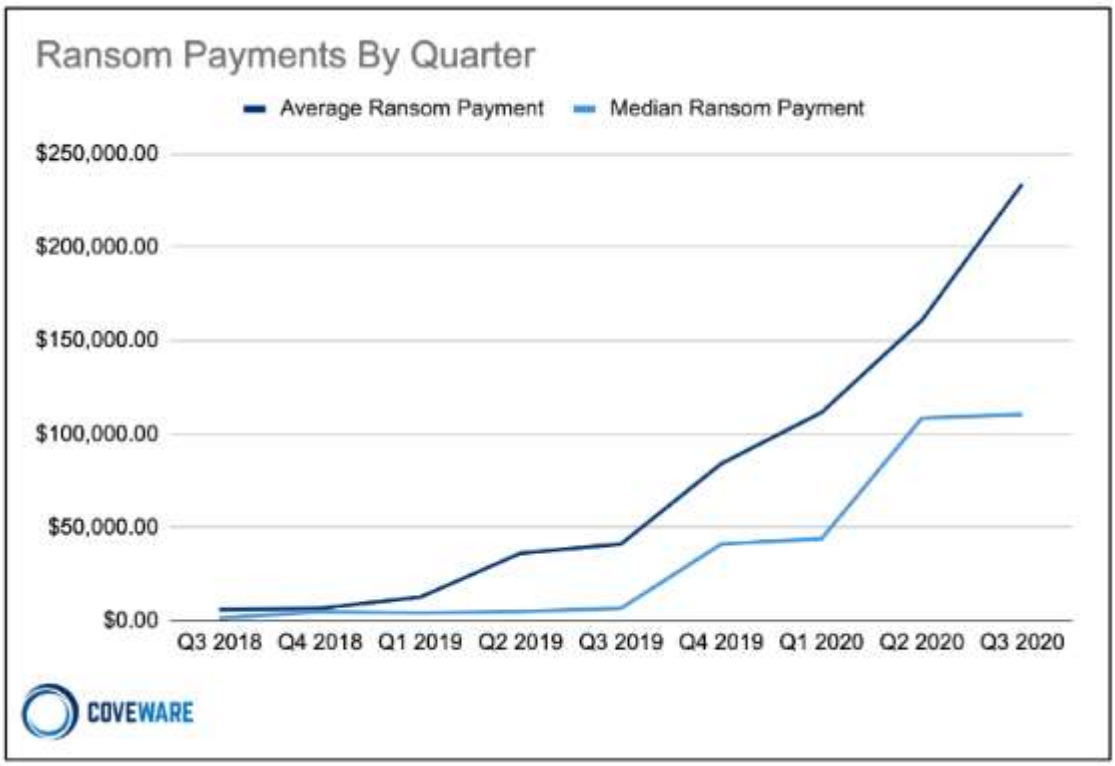


ILUSTRACIÓN 6 TENDENCIA Y EVOLUCIÓN DEL MONTO PEDIDO PARA EL RESCATE

5.4. Requerimientos Normativos y Legales

En seguridad de la información existe una serie de normas o frameworks de trabajo validados por la industria y creados principalmente para organizar y categorizar las actividades relativas a la gestión y buenas prácticas en la implementación de sistemas de seguridad. Si bien el estándar normativo más difundido es el creado por la Organización Internacional de Estandarización (ISO), que entre sus artefactos presenta la serie ISO/IEC 27000, familia de documentos orientados que contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener

Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). (Asociación Española de Normalización, 2016)

Particularmente, la norma ISO 27001 en sus controles A.7.2.2 y A.7.2.3 (ISO/IEC 27001:2013(E), 2013) establece que las personas relacionadas con el sistema de gestión de seguridad de la información deben estar capacitadas y concientizadas. En otras palabras, en dichos controles, la norma establece que:

La organización debe:

a) Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información.

b) Asegurarse de que dichas personas sean competentes, basándose en la educación, formación o experiencia adecuadas.

c) Cuando se aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones.

d) Conservar la información documentada apropiada, como evidencia de la competencia.

Esto valida la necesidad existente en las organizaciones para sus usuarios y trabajadores sean capacitados en el manejo adecuado de la información, procurando velar por su confidencialidad, integridad y disponibilidad.

Por su parte, el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (Payment Card Industry Data Security Standard) o PCI DSS fue desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía que ayuda a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago débito y crédito. (Wikipedia, 2019). Esta normativa que es obligatoria en algunos países indica en su control 12: *Una política de seguridad sólida establece el grado de seguridad para toda la organización y asesora al*

personal sobre qué hacer y qué se espera de ellos. Todo el personal debe conocer la sensibilidad de los datos y sus responsabilidades de protección. Por lo tanto, todos los empleados deben estar informados sobre sus deberes de protección y seguridad de datos. (PCI DSS GUIDE, s.f.)

En este caso la necesidad de mantener al personal concientizado de hace una obligación legal.

Otro reglamento importante que exige capacitación en procesos de seguridad, es la Regulación General de Protección de datos personales europea, GDPR, que norma el manejo en organizaciones que almacenen, retengan o transfieran de información personal y sensible de ciudadanos europeos comunitarios, en su artículo 47, párrafo n, indica que debe existir formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales. (privacy-regulation.eu, s.f.)

HIPAA es el acrónimo de Health Insurance Portability and Accountability Act (Ley de Portabilidad y Responsabilidad del Seguro Médico de Estados Unidos) y norma el uso de información sensible de pacientes en recintos de salud. En ella, las Reglas de privacidad y seguridad de HIPAA, incluidas las mejoras de la Ley HITECH de 2009 y la Regla general de 2013, y la Ley CAN-SPAM de 2003, recomienda para todos los empleados de la Organización del Centro de Llamadas que tienen acceso a información de salud protegida (PHI) y que necesitan capacitación de sensibilización sobre las normas de privacidad y seguridad de HIPAA. Nuevamente los procesos de concientización se hacen exigibles.

Por su parte el NIST (National Institute of Standards and Technology), presenta uno de los marcos de trabajo más importantes y conocidos en cuanto a procesos de seguridad y si bien no es una regulación legal, la publicación especial 800-50 recomienda concienciación y capacitación en seguridad que cubran los siguientes temas:

- Suplantación de identidad.
- Seguridad por contraseña.

- Navegación web segura.
- Ingeniería social.
- Malware.
- Seguridad móvil.
- Seguridad física.
- Media removible

Por lo tanto, toda institución que siga los lineamientos formales de NIST deberá contar con un proceso de capacitación que informe y de herramientas a los usuarios para manejar la información digital de manera adecuada.

5.5. Plataformas de Concientización de Seguridad Automatizadas

Si bien los procesos de crear conciencia sobre la seguridad de la información se pueden realizar mediante el uso de técnicas tradicionales de enseñanza, el uso de herramientas automatizadas permite crear experiencias educativas organizadas y perfiladas para los distintos roles de una empresa y abarcar empresas distribuidas en distintas regiones o países. Existen diversas plataformas administradas que logran este objetivo, los contenidos educativos ofrecidos por ellos no siempre parecen cercanos a la realidad social y cultural del trabajador promedio en chile.

Las plataformas automatizadas de concientización de seguridad existentes en el mercado, suelen incluir módulos para la ejecución de pruebas de phishing a distintos grupos dentro de la empresa, y suelen incluir herramientas de evaluación y control de conocimientos, sin embargo, la gran falencia de estas plataformas automatizadas suelen ser los contenidos.

Las ventajas comunes de usar estas plataformas automatizadas están principalmente en:

- Son soluciones llave en mano, simple y rápida de implementar.
- Los contenidos suelen ser editables por el administrador.
- El diseño de los módulos es estético y pedagógico enfocado en el cambio de comportamiento del usuario.

- Suelen incluir módulos de Identificación de usuarios de riesgo y refuerzo en su capacitación.
- Permiten realizar simulación de Phishing y Ransomware para medir la línea base y evolución de hábitos de seguridad.
- Realizan Tracking automático de registros para auditoría y cumplimiento.

Si bien, estas características comunes son bastante efectivas en lograr una interacción de seguridad con los usuarios, el proceso puede verse mejorado al utilizar contenidos más cercanos a la realidad del usuario final.

Estas plataformas pueden implementarse tanto en modelos de infraestructura Onpremise o cloud, y sus precios fluctúan entre los 10 dólares y los 30 dólares por usuario al año, según la cantidad de usuarios a contratar y el tipo de membresía.

				Most Popular	
MSRP Pricing By Seat - 1 Year	**Silver**	**Gold**	**Platinum**	**Diamond**	**PhishER**
25-50	$18.00	$21.75	$25.50	$30.50	-
51-100	$16.00	$19.25	$22.50	$27.50	-
101-500	$13.00	$15.50	$18.00	$23.00	$10.00
501-1000	$12.00	$14.25	$16.50	$21.50	$7.00
1001-2000	$11.00	$13.00	$15.00	$20.00	$6.00
2001-3000	$10.00	$11.75	$13.50	$18.50	$5.00
3001-5000	$9.00	$10.50	$12.00	$17.00	$4.50
5001+	Get A Quote	Get A Quote	Get A Quote	Get A Quote	Get A Quote

ILUSTRACIÓN 7 TABLA DE PRECIOS DE KNOWBE4

A continuación, veremos las definiciones esenciales de las arquitecturas tanto onpremise como cloud.

5.6. Arquitecturas de Infraestructura Onpremises

5.6.1. Evolución del TI en los últimos 10 Años

Como podemos apreciar en la Ilustración N°8, la evolución de la infraestructura TI en los últimos años se ha ido simplificando, inicialmente se requerían múltiples capas que se conformaban por servidores independientes que se conectaban a su almacenamiento por redes SAN, luego se debía considerar todo el hardware y software adicional para lograr realizar el backup de estos sistemas y archivos con diversos equipos que optimizaban la WAN o permitían una administración centralizada.

Con las nuevas herramientas de virtualización y las plataformas Hiperconvergentes podemos pasar de utilizar 1 rack completo de 42 unidades de rack (UR) a solo 4 UR, lo cual nos significa evidentemente ahorros en cuanto a espacio, energía y por sobre todo en su administración.

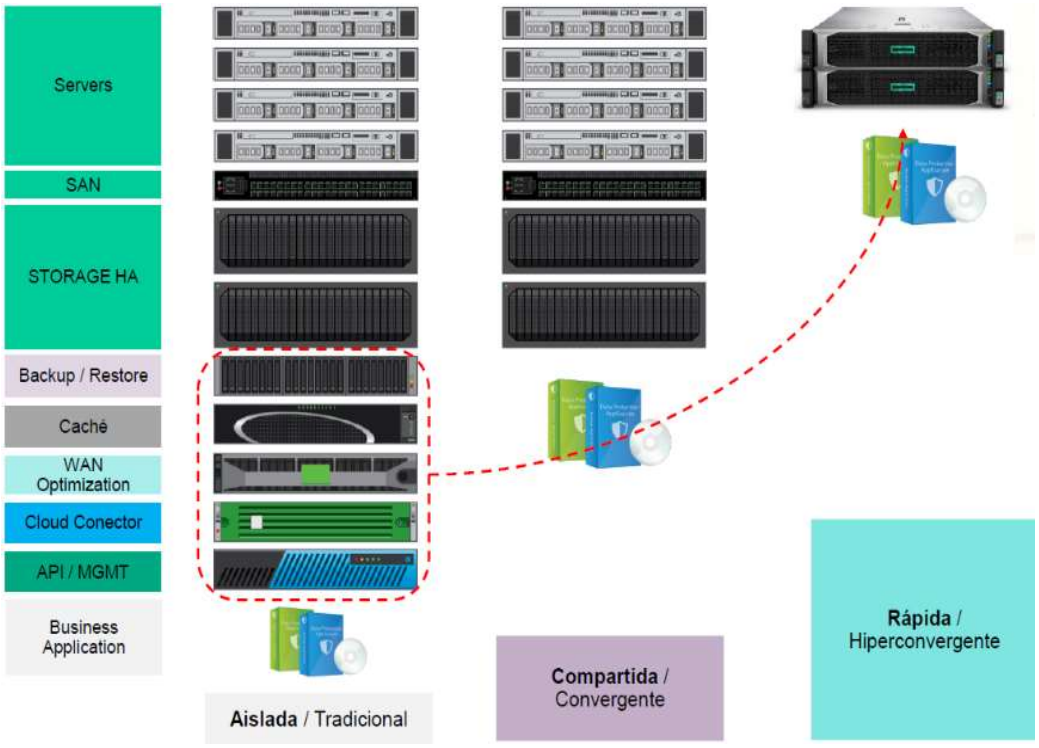


ILUSTRACIÓN 8 EVOLUCIÓN DE LA ARQUITECTURA DE SERVIDORES

5.6.2. Servidores Físicos

Los servidores físicos hoy en día siguen siendo una opción para empresas de todos los tamaños, pero generalmente son más utilizadas por pymes o medianas empresas por falta de presupuesto o para instalar sus sistemas menos críticos dado que no poseen alta disponibilidad (HA) por sí solos, no obstante al agregar más servidores u otros componentes de almacenamiento adicional como Storages con doble controladora, podemos armar infraestructura para trabajo de alta disponibilidad o sistemas de Virtualizacion en HA como veremos más adelante.

ILUSTRACIÓN 9 SERVIDORES FÍSICOS INDEPENDIENTES

5.6.3. Sistemas HA Tradicionales

Los sistemas HA tradicionales son hoy en día una de las plataformas más utilizadas a nivel mundial, dado que son el paso previo hacia las nuevas tecnologías Convergentes e Hyperconvergentes o para migrar en forma parcial o total sus cargas a las Nubes Publicas.

Estos sistemas generalmente se componen de diversas capas de hardware en forma independiente como se detalla a continuación:

- Servidores Físicos que manejan generalmente el Proceso *(CPU y RAM).*
- Conexiones vía SAN directa al Storage o Switches SAN FC *(Redes de Almacenamiento de Alta Velocidad).*

- Storages con controladoras redundantes, que van desde propósito general con mix de discos SAS y SATA a Misión Critica All-Flash.

Al unificar estas 3 líneas de Hardware y aplicar software de Virtualizacion de cualquier fabricante, como por ejemplo VMWARE, HIPER-V, RHEV u otro similar, contaremos con sistemas de alta disponibilidad básicos desde 2 nodos a sistemas de Metro-clúster, con tantos recursos como lo posea el Hardware configurado.

Las desventajas de este tipo de plataformas son las siguientes:

- Se requiere una gran inversión inicial.
- Generalmente se sobredimensionan las plataformas y se paga por recursos que no son utilizados.
- La administración no está centralizada por ende se debe administrar cada línea con diversos especialistas.

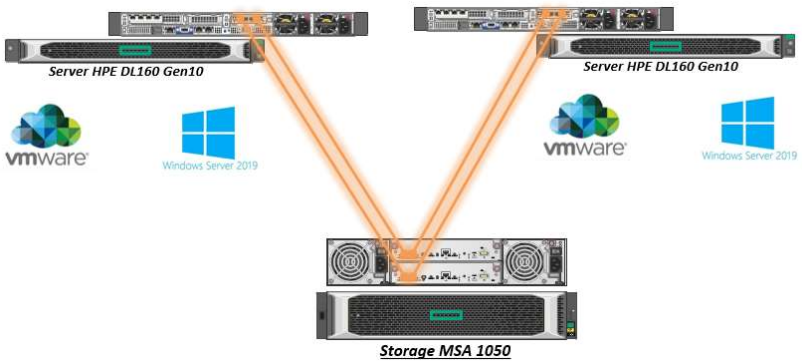


ILUSTRACIÓN 10 ESQUEMA DE UN CLUSTER VIRTUAL HA BÁSICO – DE 2 CAPAS

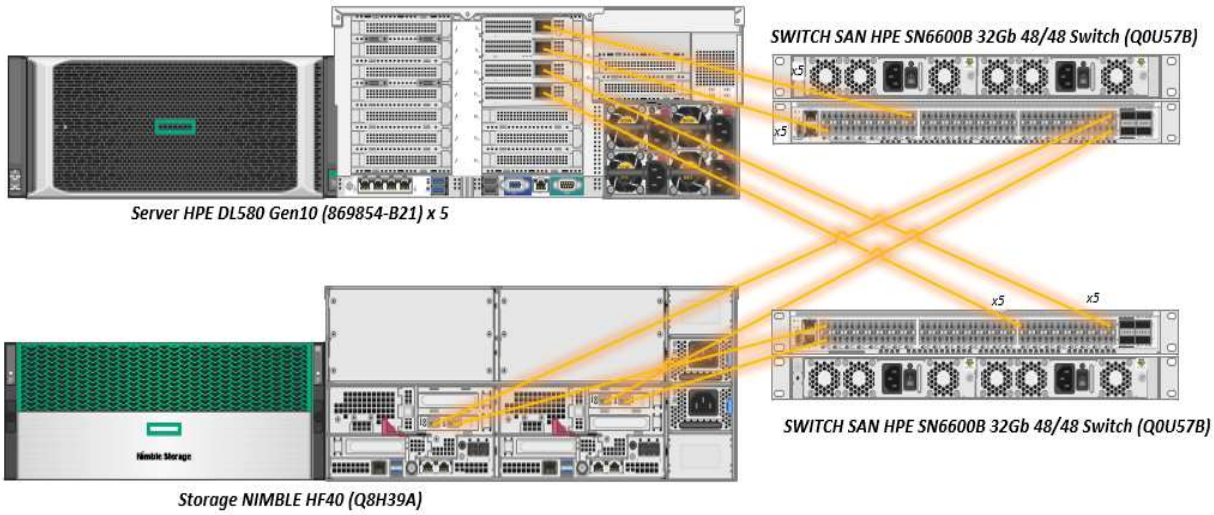


ILUSTRACIÓN 11 ESQUEMA DE UN CLUSTER VIRTUAL HA AVANZADO - DE 3 CAPAS

5.6.4. Hiperconvergencia

La Hiperconvergencia es una infraestructura definida por software unificado para el cómputo y el almacenamiento, separa las operaciones independientes de la infraestructura de almacenamiento y cómputo y las converge a nivel de hipervisor, simplificando la operación y obteniendo una experiencia única de administración, además de eliminar las conexiones nativas de sistemas de almacenamiento como red SAN, conexiones FC, etc.

Hemos elegido mencionar la Hiperconvergencia de VMware vSAN (vSAN, 2021) porque es una de las más utilizadas a nivel mundial dado que es simple de administrar y manejar si ya se trabaja en un ambiente virtual con VMware, además si se mescla con otras aplicaciones como VMware Cloud Foundation (VMCloudFdtn, 2021) facilita la implementación y ejecución de una nube hibrida.

Adicionalmente queremos hablar de la Hiperconvergencia HPE Simplivity porque agrega además una eficiencia del almacenamiento única en el mercado, logrando entregar el almacenamiento propio de la virtualización y agregando respaldos de seguridad en el mismo espacio, optimizando el recurso de almacenamiento al punto de garantizar al menos 10 veces lo que hace el resto del mercado, además

agrega una protección mayor, suficiente para asegurar un 99,9999% de disponibilidad de un recurso virtualizado, finalmente unifica la administración integrándose a la interfaz de administración virtualizada más usada en las empresas. (HCI Simplivity, HPE, s.f.)

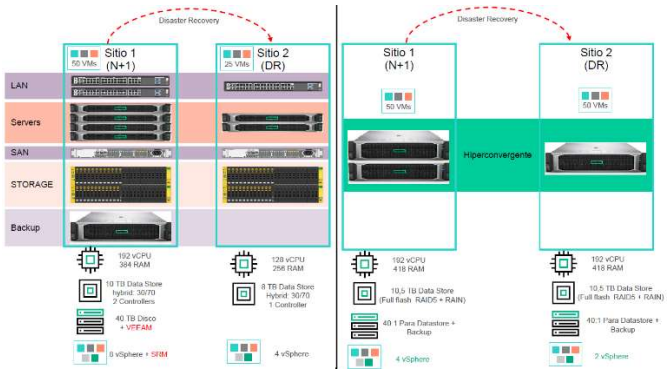


ILUSTRACIÓN 12 DIAGRAMA DE UNA SOLUCIÓN HA TRADICIONAL VS HCI

5.6.5. Modelo Pago por Uso

Nos enfocaremos en la marca HPE, dado que ofrece un modelo de consumo real estableciendo un rango de compromiso mínimo en cuanto al consumo de Infraestructura TI, pero este sistema no tiene relación con estructuras de ingeniería financiera, basados en el arrendamiento o la suscripción vía Leasing. Las ofertas de HPE Greenlake (HPE GreenLake, 2021) se basan en una TI cuyo uso y costos se miden con una visibilidad y granularidad del 100 % emulando completamente la operación de la Nube.

Esta funcionalidad de medición integrada se ha diseñado específicamente para satisfacer el requisito de garantizar que el costo coincida con el consumo para la infraestructura de TI que se está utilizando realmente o si se requiere aumentar sus recursos en forma dinámica por un periodo puntual o prolongado.

HPE GreenLake representa la oferta líder de TI como servicio de HPE y brinda la experiencia en la nube a aplicaciones y datos en cualquier lugar (todo tipo de nubes, centros de datos y extremos) con un modelo de operaciones unificado.

ILUSTRACIÓN 13 PROPUESTA DE VALOR DE HPE

Propuesta de valor de HPE para realizar la transición hacia modelos basados en el consumo:

HPE GreenLake proporciona servicios de nube e infraestructura para cargas de trabajo locales, totalmente gestionados en un modelo de pago por consumo.

Sobre la base de HPE GreenLake Central, un nuevo portal de autoservicio intuitivo y consola de operaciones, las empresas pueden implementar servicios rápidamente, obtener conocimiento sobre costos y cumplimiento, además de simplificar la gestión en todo su entorno híbrido. (Daniel Newman, 2020).

5.7. Arquitecturas de Infraestructura Cloud

5.7.1. Nube Pública

La nube pública es un servicio informático ofrecido por un proveedor externo mediante internet que está disponible para quien quiera usarlo o comprarlo, según los planes disponibles. Así, los clientes solo tienen que pagar por el uso que hacen de ciclos de CPU, el almacenamiento o el ancho de banda consumido.

Al contrario que en las nubes privadas, las nubes públicas permiten ahorrar a las organizaciones grandes gastos derivados de comprar, administrar y mantener hardware e infraestructura de aplicaciones locales. De esta forma, el responsable del trabajo de administración y mantenimiento del sistema es el proveedor del servicio.

Además, una nube pública se puede implementar con mayor velocidad que las infraestructuras locales y con plataformas que proporcionan una escalabilidad casi infinita. Por ende, los empleados de una empresa pueden acceder a la nube pública a través de la misma aplicación o mediante el navegador, desde cualquier lugar con acceso a internet.

Las más conocidos son los siguientes:

- ✓ Microsoft Azure
- ✓ Amazon Web Services
- ✓ Google Cloud

También hay otras nubes reconocidas como:

- ✓ Oracle
- ✓ IBM Softlayer
- ✓ Vmware
- ✓ Veeam
- ✓ Wasabi

5.7.2. Nube Publica Azure

Azure es la plataforma de cómputo, redes, almacenamiento, administración y análisis en la nube de Microsoft, y está compuesta por un conjunto servicios en la nube en constante expansión que permiten a las organizaciones afrontar sus desafíos empresariales actuales y futuras (Microsoft, 2019).

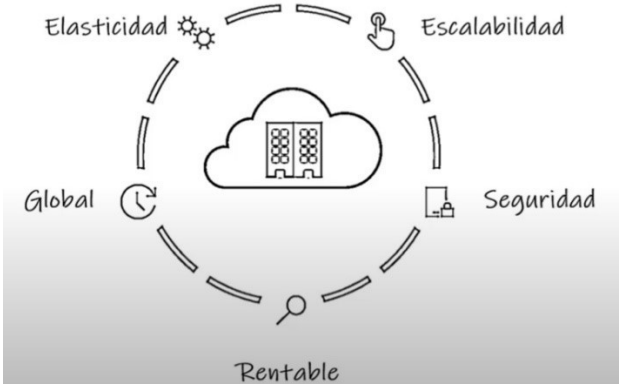


ILUSTRACIÓN 14 BENEFICIOS DEL COMPUTO EN LA NUBE.

A continuación, explicaremos las plataformas de Computo que pueden ser adquiridas de Azure.

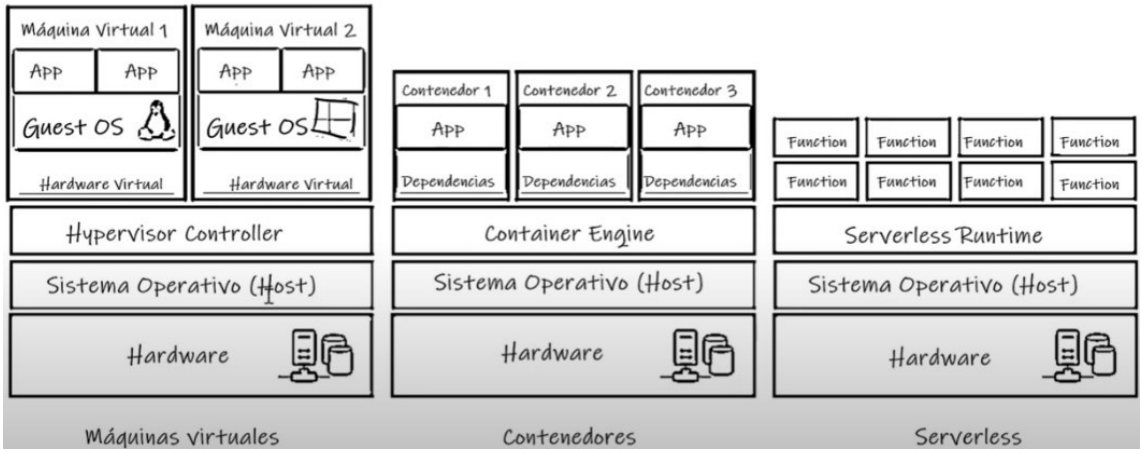


ILUSTRACIÓN 15 PLATAFORMA DE CÓMPUTO DISPONIBLES EN AZURE

5.7.3. Virtual Machines

Cuando hablamos de máquinas virtuales nos referimos a la emulación de un equipo físico que es manejado en forma virtual, puede tener Sistema operativo Windows o Linux, con diversas capacidades de hardware y soporte todo según lo desee.

En Vmware se instala un Hypervisor llamado vSphere en un hardware físico que se apodera de los recursos (CPU, RAM, DISCO y RED) y luego se crean las máquinas virtuales (VM´s).

En el caso de Azure, el hardware que ejecuta la máquina virtual está ubicado en el servidor físico de alguno de sus centros de datos que nosotros elijamos (Microsoft Azure - VMS, 2020).

ILUSTRACIÓN 16 COMPONENTES DE LAS MÁQUINAS VIRTUALES

5.7.4. Container

Los contenedores son una forma de Virtualización, que a diferencia de las máquinas virtuales no requieren un sistema operativo invitado, dado que virtualizan el sistema operativo subyacente y hace que la aplicación en

contenedor perciba que tiene el sistema operativo (incluidas la CPU, la memoria, el almacenamiento de archivos y las conexiones de red) todo para ella sola. Dado que se abstraen las diferencias en el sistema operativo y la infraestructura subyacente, siempre que la imagen base sea coherente, el contenedor se puede implementar y ejecutar en cualquier lugar.

Esto permite que los contenedores sean mucho más eficientes y ligeros. Las aplicaciones en contenedor se pueden iniciar en segundos y pueden caber muchas más instancias de la aplicación en la máquina en comparación con un escenario de máquina virtual (Microsoft Azure - Container, 2020)

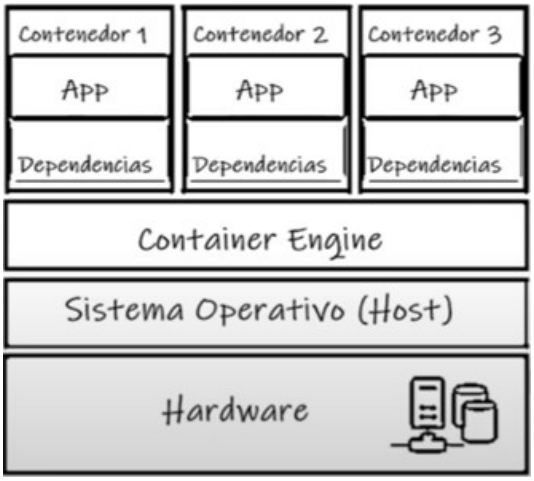


ILUSTRACIÓN 17 COMPONENTES DEL CONTAINER

5.7.5. Serverless

Con sistemas basados en Serverless se deja de usar un servidor físico o uno en la nube, claramente individualizados por contenedores temporales y sin estado donde se ejecutan los códigos de las aplicaciones. Estos contenedores se crean en el momento que ejecutas la aplicación y luego desaparecen, por lo que el servidor pasa a ser una parte menos visible del sistema.

Esta tecnología se asocia con FaaS que significa Function as a Service, que fue creada en 2014 y que luego se ha ido desarrollando mediante proyectos tan importantes como Microsoft Azure Functions, IBM/Apache OpenWhisk, Google Cloud Functions o AWS Lambda.

Azure Functions Está desarrollado por Microsoft y permite utilizar aplicaciones como Bash, Powershell, Java, Python, C#, F#, PHP o Batch. (Microsoft Azure - Serverless, 2020)

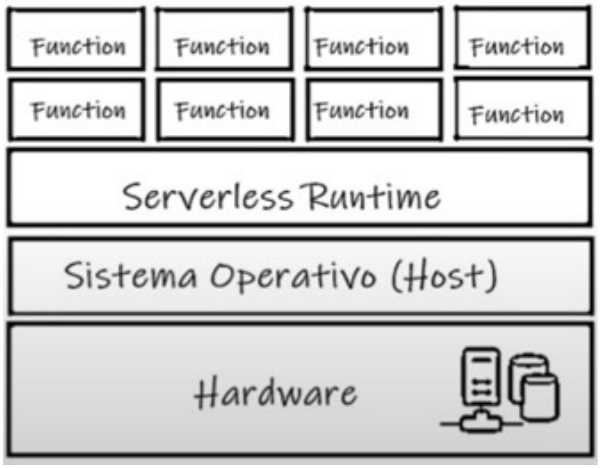


ILUSTRACIÓN 18 COMPONENTES DEL SERVERLESS

6. ESTUDIO DE MERCADO

Nuestro estudio de mercado tiene por objetivo analizar dos áreas fundamentales que tienen relación con proveedores que prestan servicios de Concientización de Seguridad TI y con clientes que tienen o no estos servicios actualmente o que están interesados en adquirirlos, para lo anterior confeccionamos 2 encuestas simples que nos permitirán revisar resultados y sacar conclusiones, pero primero daremos una revisión a la situación actual en términos de servicios de concientización de seguridad TI en el mercado nacional e internacional.

6.1. Plataformas Existentes en el Mercado

Según la Consultora internacional Forrester en su informe: The Forrester Wave™ Security Awareness And Training Solutions, Q1 2020-1 (Budge & O'Malley, 2020), existen en el Mercado 12 compañías que cuentan con plataformas automatizadas para la capacitación en seguridad de la información, tal como se aprecia en el diagrama a continuación.

ILUSTRACIÓN 19 FORRESTER WAVE 2020

Si bien estas plataformas knowbe4 y Proofpoint son las más utilizadas en el mercado internacional existe una muy utilizada en el mercado nacional, SMARTFENSE, que no aparece en los cuadrantes internacionales de Forrester o Gartner.

ILUSTRACIÓN 20 CUADRANTE MÁGICO DE GARTNER 2019

A continuación, se describen tres de las plataformas más utilizadas en el mercado nacional:

Knowbe4: Es una empresa ubicada en Florida, EUA, y fue fundada en 2010, es considerada líder en el segmento de concientización. KnowBe4, Inc. diseña y desarrolla un software de infraestructura cloud, proporcionando una plataforma para capacitación en conciencia de seguridad, empresas, programas de concienciación de clientes y otros módulos relacionados, así como también ofrece seguridad, pruebas de falsificación de dominio, contraseña débil y herramientas de capacitación. KnowBe4 sirve a clientes en todo el mundo. Su

plataforma soporta sobre 20 distintos lenguajes y contiene la biblioteca en español más grande que el resto de las plataformas, sin embargo, tras consultar a un partner local nos indica que no poseen contenidos específicos para Chile.

Proofpoint: fue fundada en 2002 por Eric Hahn, ex director de tecnología de Netscape, desde ese entonces ha crecido a más de 2500 empleados que prestan servicios a más de 4000 empresas en todo el mundo. La compañía se hizo pública en abril de 2012, cotiza en el NASDAQ y reportó ingresos de $ 717 millones en 2018. Ofrece distintos servicios de seguridad y protección datos y entre ellos destacan Proofpoint Security Awareness Training, el cual ofrece módulos de entrenamiento y pruebas de phishing simulado en 35 lenguajes. Nuevamente no se evidenciaron contenidos específicos para Chile.

Smartfense: Es una empresa española, especialista en concientización de seguridad. Si bien no aparece en los cuadrantes de Forrester y Gartner, es la plataforma con mayor despliegue en Chile. Posee distintos módulos interactivos de aprendizaje e integra además componentes de simulación de Phishing y Ransomware para medir la efectividad de las acciones realizadas y conocer la evolución del comportamiento de los usuarios de manera objetiva.

6.2. Situación Actual de la Concientización como Servicio en Chile

Al realizar el análisis de las empresas de seguridad de la información en el mercado nacional, podemos concluir que hay una gran cantidad que se dedica a temas de ciberseguridad ofreciendo distintos tipos de productos y servicios como, por ejemplo:

1. Venta de antivirus y hardware de seguridad multimarca.
2. Administración de plataformas Endpoint.
3. Ventas y servicios de implementación de Firewall, WAF, IPS, IDS, DLP, AntiSpam, Web Filter, Etc.
4. Ethical Hacking.

5. Análisis de Vulnerabilidades.
6. Otros.

Pero pocas empresas ofrecen dentro de su catálogo de productos o servicios, temas de concientización gestionados por ellos mimos y generalmente se basan en alianzas con plataformas internacionales como Knowbe4 (kepler, s.f.) o Smartfense (Stega, s.f.) Que si bien son reconocidas en el ámbito internacional no contienen contenidos nacionales.

Para complementar lo anterior confeccionamos 2 encuestas orientadas a clientes finales y a empresas proveedoras de servicios de seguridad, de manera de conocer más en detalle el estado del arte real de la inversión en concientización y los métodos utilizados para realizarla:

A continuación, revisaremos las encuestas preparadas para proveedores y posteriormente a clientes.

6.3. Encuesta a Proveedores de Seguridad de la información

Como lo indicamos anteriormente esta encuesta fue enviada a contactos que actualmente trabajan en empresas que prestan servicios y comercializan productos relacionados con la seguridad de la información.

La encuesta a proveedores consta de 9 preguntas en total, pero en la pregunta N°3 consultamos si dan servicios de concientización para que continúen con preguntas focalizadas, las cuáles publicamos en el siguiente Link:

https://tinyurl.com/pccsi-proveedores

1. Por favor ingrese el nombre de su empresa.
2. Por favor ingrese su nombre y cargo si lo desea.
3. ¿Su empresa entrega el Servicio de Concientización de Seguridad (CSI) o similares a clientes?

4. ¿Cuál es el número estimado de Clientes que atienden con servicios de Seguridad de la Información?
5. ¿Cuál es el número estimado de Clientes que atienden con Servicios de Concientización de Seguridad (CSI)?
6. ¿De qué manera se entrega el Servicio de Concientización de Seguridad (CSI)?
7. ¿Cada cuánto tiempo son actualizados los contenidos entregados por el servicio de CSI?
8. ¿Sus clientes con el Servicio CSI han logrado bajar la cantidad o gravedad de los incidentes de seguridad internos?
9. ¿Autorizo a Compartir la información entregada para otros fines académicos?

6.3.1. Resultados de la Encuesta a Proveedores

Al comenzar a contactar a empresas de ciberseguridad nos encontramos con que muy pocas daban servicios de concientización y finalmente cerramos la muestra con 10 encuestas contestadas.

A continuación, se entrega el detalle de los resultados de las encuestas.

https://tinyurl.com/pccsi-proveedores-resultados

De las 10 encuestas que se respondieron, 7 indican que prestan servicios de concientización de seguridad que será en los que pondremos foco.

ILUSTRACIÓN 21 ENCUESTA A PROVEEDORES

Estos 7 contactos que trabajan en empresas de Ciberseguridad que respondieron la encuesta suman en total 1285 clientes aproximadamente a los cuales les prestan servicios de seguridad de la información, la empresa que menos clientes atiende tiene 5 y la que empresa con más clientes tiene 540, en promedio tenemos 185 clientes por empresa encuestada.

4. ¿Cuál es el numero estimado de Clientes que atienden con servicios de Seguridad de la Información?

7 Respuestas

Id. ↑	Nombre	Respuestas
1	anonymous	5
2	anonymous	300
3	anonymous	35
4	anonymous	15
5	anonymous	300
6	anonymous	540
7	anonymous	100

ILUSTRACIÓN 22 ENCUESTA PROVEEDORES – N° DE CLIENTES

Cuando consultamos a cuantos de sus clientes prestan servicios de concientización nos encontramos que es un porcentaje muy bajo versus la totalidad de clientes que poseen, lo cual no nos sorprende, porque la mayoría de los servicios que prestan tienen foco en otro tipo de soluciones de seguridad como los mencionados en la situación actual.

ILUSTRACIÓN 23 ENCUESTA PROVEEDORES – N° DE CLIENTES CONCIENTIZACIÓN

Las respuestas de la pregunta N°7 nos indica que la mayoría utiliza una plataforma externa con licenciamiento (5 de 7) y el contenido es actualizado semanal y mensualmente.

6. ¿De qué manera se entrega el Servicio de Concientización de Seguridad (CSI) ?

7 Respuestas

Id. ↑	Nombre	Respuestas
1	anonymous	Se utiliza una plataforma externa con licenciamiento
2	anonymous	Se utiliza una plataforma externa con licenciamiento
3	anonymous	A través de un proceso propio creado internamente
4	anonymous	Se utiliza una plataforma externa con licenciamiento
5	anonymous	Se utiliza una plataforma externa con licenciamiento
6	anonymous	Se utiliza una plataforma externa con licenciamiento
7	anonymous	Se subcontrata y lo realiza un tercero

ILUSTRACIÓN 24 RESULTADOS ENCUESTA PROVEEDORES

ILUSTRACIÓN 25 ACTUALIZACIÓN DE CONTENIDOS – RESPUESTAS

6.3.2. Conclusiones de la Encuesta a Proveedores

Como conclusión podemos deducir que las empresas que se dedican a comercializar productos y servicios de ciberseguridad no están poniendo foco en la concientización de los usuarios y más bien se dedican vender lo más solicitado.

6.4. Encuesta a Clientes Finales

Nuestro segundo objetivo fue realizar una encuesta para llegar a clientes finales que actualmente tengan servicios o no de concientización de seguridad, además de tener una referencia de cómo es su percepción en cuanto a los temas de seguridad de su empresa y si consideran importante que los usuarios estén capacitados.

La encuesta a clientes consta de 8 preguntas y fue contestada por usuarios de diversos sectores y áreas, las cuáles publicamos en el siguiente Link:

https://tinyurl.com/clientes-pccsi

1. Por favor ingrese su nombre, cargo y empresa si lo desea.

2. Indique el número estimado de trabajadores que utilizan dispositivos computacionales en su empresa.
3. ¿Qué tan Importante es la Seguridad de la Información para su empresa?
4. ¿Cómo calificaría el nivel de la Seguridad de la Información en su empresa?
5. ¿Considera que usted y los usuarios de su empresa están preparados para evitar un ataque Informático?
6. ¿Qué tan importante considera Usted que los usuarios estén Capacitados en temas de la Seguridad de la Información?
7. ¿Cuánto estaría dispuesto a invertir en forma anual para capacitar a un usuario en temas básicos de la Seguridad de la Información?
8. ¿Su empresa cuenta con un presupuesto anual estimado para cubrir temas relacionados con la Seguridad de la Información?

6.4.1. Resultados de la Encuesta a Clientes

Generamos un envío masivo de correos con el link de la encuesta a clientes chilenos de diversos sectores, además de la propagación por redes sociales y tuvimos una cantidad considerable de respuestas, realizando el cierre en 48 encuestas contestadas.

A continuación, se entrega el detalle de los resultados de las encuestas.

https://tinyurl.com/pccsi-clientes-resultados

la muestra nos permite analizar respuestas de distintas realidades dado que dentro de los encuestados hay empresas que van desde microempresas con 2 usuarios a grandes empresas con 20000 usuarios.

2. Indique el número estimado de trabajadores que utilizan dispositivos computacionales en su empresa

48 Respuestas

Id. ↑	Nombre	Respuestas
1	anonymous	2100
2	anonymous	20000
3	anonymous	60
4	anonymous	Gestión de riesgos de la información
5	anonymous	600
6	anonymous	100
7	anonymous	20
8	anonymous	300
9	anonymous	90
10	anonymous	380
11	anonymous	500
12	anonymous	5000
13	anonymous	250
14	anonymous	500
15	anonymous	90
16	anonymous	23
17	anonymous	7000
18	anonymous	Toda la consultora (30 personas aprox)
19	anonymous	50
20	anonymous	6

ILUSTRACIÓN 26 TABLA DE ENCUESTAS A CLIENTES

El 78 % de los encuestados considera que la Seguridad de la Información es importante para su empresa, obteniendo 4.33 de 5 posibles puntos.

ILUSTRACIÓN 27 DISTRIBUCIÓN DE VOTACIÓN

Los encuestados consideran que sus empresas cuentan con un nivel medio con una puntuación de 3.51 de 5, con relación a la seguridad de la información.

ILUSTRACIÓN 28 IMPORTANCIA DE LA SEGURIDAD EN LA EMPRESA

En este punto podemos destacar que los encuestados consideran mayoritariamente que los usuarios de su organización no están preparados para un ataque informático obteniendo una puntuación de 2.47 de 5 puntos posibles.

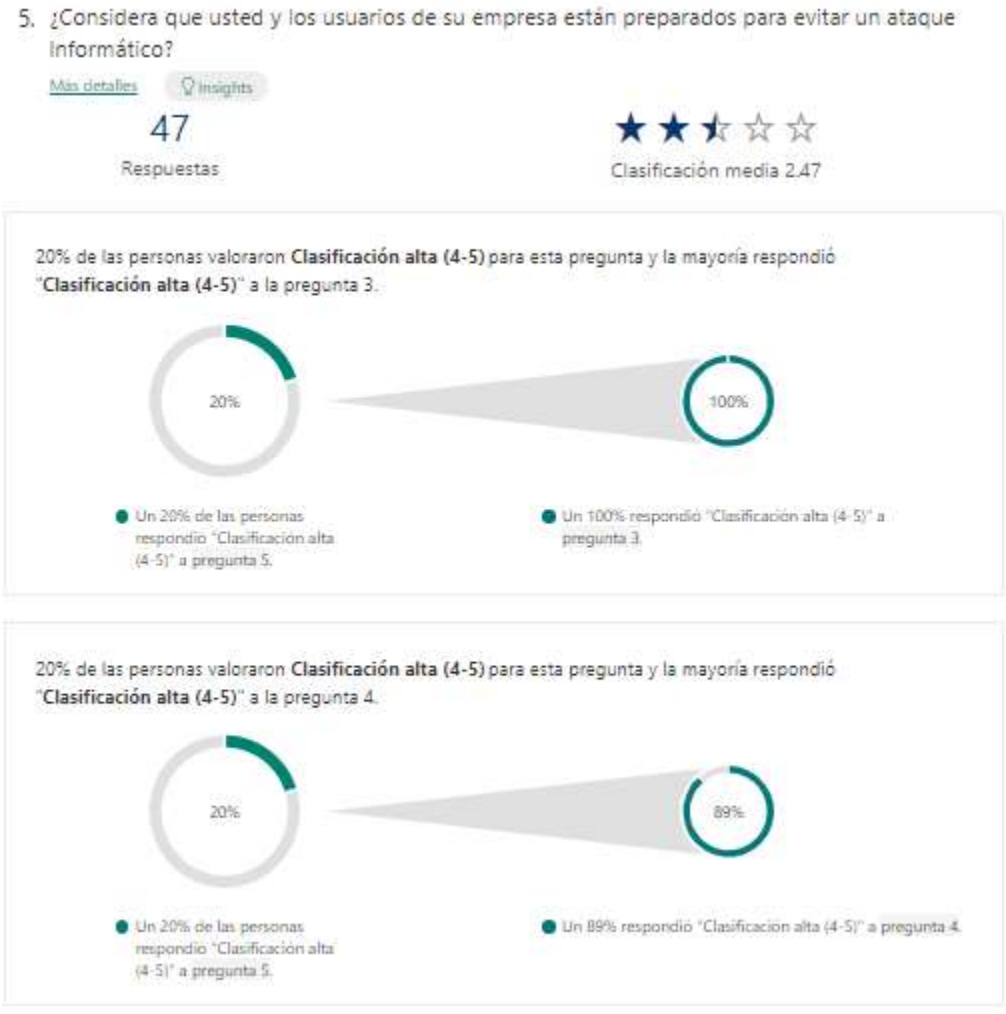


ILUSTRACIÓN 29 ESTIMACIÓN DE PREPARACIÓN DE LOS USUARIOS

La pregunta N°6 nos entrega un dato clave, donde 77% de los encuestados considera que es importante que los usuarios esten capacitados en temas de la seguridad de la informacion obteniendo una puntuación de 3.98 de 5 puntos posibles, lo cual se acerca a la puntuacion de la pregunta N°3.

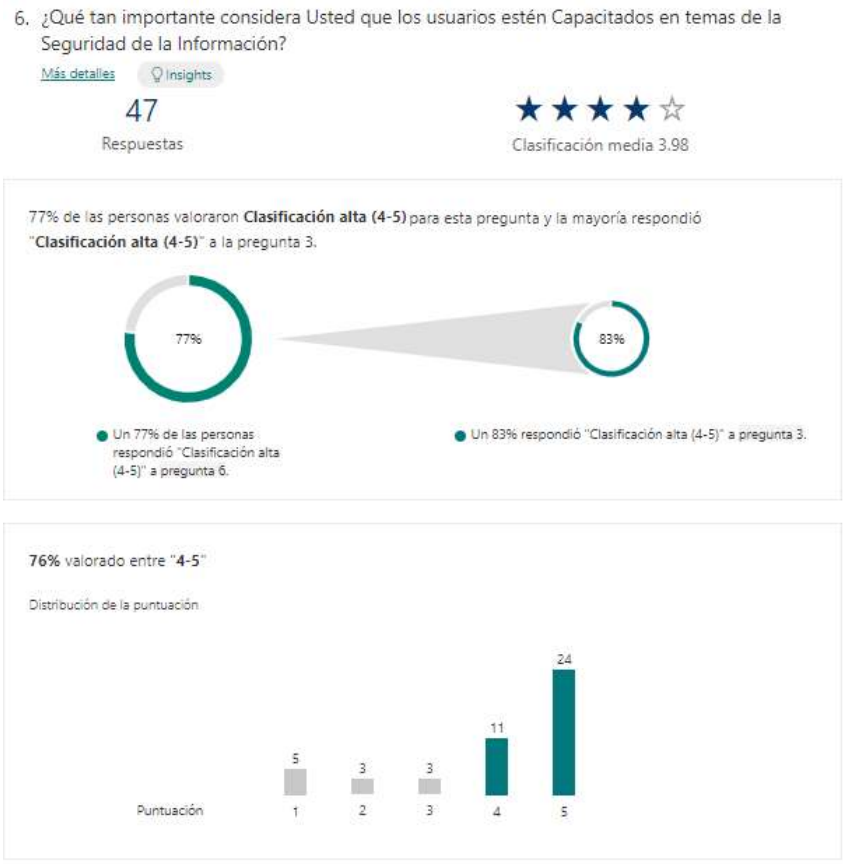


ILUSTRACIÓN 30 IMPORTANCIA DE LA PREPARACIÓN DE USUARIOS

Las preguntas N°7 y N°8 tienen como objetivo conocer temas económicos, pero principalmente nos sirve para ver la valorización que cada encuestado les da a los temas de seguridad TI.

La gran mayoría de los encuestados es decir el 75% de la muestra estaría dispuesto a invertir entre USD$ 10 a USD$ 25 (44%) y USD$26 a USD$50 (31%)

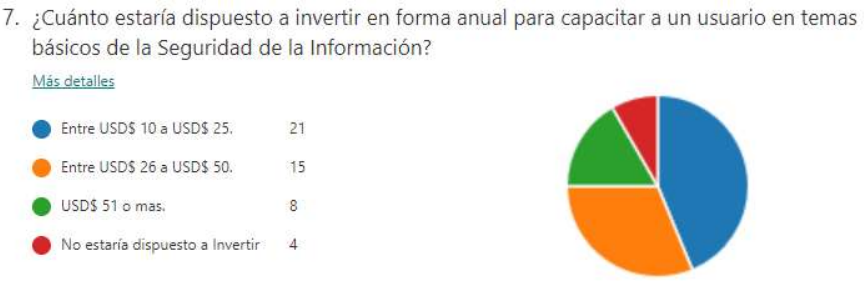


ILUSTRACIÓN 31 INTENCIÓN DE INVERSIÓN

Si bien el 75% de los encuestados estaría dispuesto a invertir para capacitar a los usuarios, cuando contestan la pregunta N°8 que tiene relación de si conoce el presupuesto anual estimado que invierte su empresa, nos encontramos con que 37 de los 48 encuestados contestan que solo se invierte cuando hay contingencias (38%) y por otro lado que se desconoce la Información (40%).

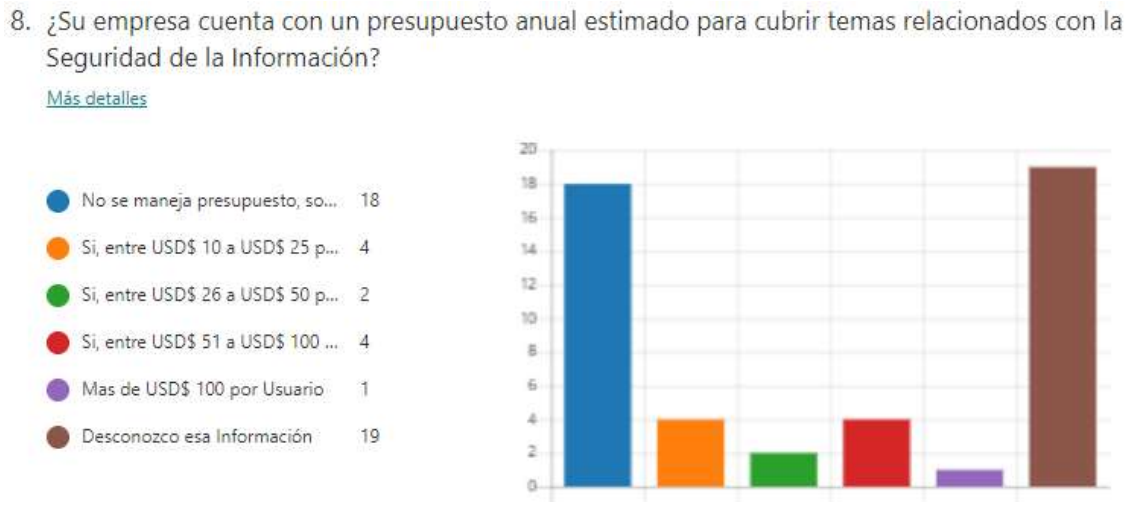


ILUSTRACIÓN 32 ¿EXISTE PRESUPUESTO ASIGNADO?

6.4.2. Conclusiones de la Encuesta a Clientes

La muestra de esta encuesta tuvo una mayor receptividad en los usuarios logrando un número considerable de respuestas que nos permite concluir que el 78% de los encuestados que son de diversos sectores y empresas considera importante los temas de seguridad y que el 77% considera que capacitar a los usuarios también es importante.

Por otro lado, visualizamos que existe un desconocimiento general acerca de cuanto y cuando se invierte en temas de seguridad.

6.5. Conclusiones del Estudio de Mercado

Después de 3 meses con las encuestas publicadas, nuestro estudio de mercado nos deja en claro que; si bien el tema de la seguridad de la información en Chile es considerado muy importante, pocas empresas se dedican a dar servicios de concientización a los usuarios y están más bien enfocadas a las soluciones estándar en temas de seguridad de TI como lo explicamos en la situación actual de las plataformas de concientización.

Analizando las respuestas de los clientes, la gran mayoría de los encuestados consideran que la seguridad de la información y capacitar a los usuarios es clave para bajar las incidencias de seguridad, pero hay un desconocimiento general en cuanto a los valores de este tipo de soluciones o el presupuesto que destinan sus empresas para cubrir esta brecha de seguridad de la información que sin duda como se repite en esta tesis cada día se confirma más que el usuario es el eslabón más débil (Mitnick & Simón, 2005).

Creemos que posiblemente una de las razones del por qué el mercado no entrega una cobertura mayor a este tipo de servicios de concientización, es por la falta interés de la mayoría de los usuarios finales por lo poco amistoso de los contenidos de las plataformas estándar y por qué muchas de estas empresas que tienen generalmente buenos profesionales en ciberseguridad pueden ser muy capaces de solucionar grandes problemas de seguridad o encontrar vulnerabilidades graves, pero no cuentan con las habilidades blandas necesarias para capacitar a los usuarios o simplemente no les gusta tocar temas simples y prefieren el código en vez de capacitar a usuarios con temas básicos.

7. MARCO METODOLÓGICO

Como metodología de trabajo, se utilizará la Metodología de Investigación Cuantitativa (Hernández R., 2010), la figura del modelo del marco metodológico. Debido a las facilidades que presenta, se ha elegido esta metodología, ya que su sistema de recolección de datos es más fiable y representa de manera más exacta los resultados para el desarrollo de este tipo de proyecto:

- Exige orden de cumplimiento para cada etapa del proyecto, es decir, antes de iniciar una nueva etapa, debe estar finalizada la etapa que le precede, lo que asegura que no queden etapas con tareas pendientes. Esto permite asegurar que los entregables de cada etapa se cumplan en plazos comprometidos.
- Los requisitos de entrada al diseño del modelo están claros por estar contenidas en normas ISO.
- Perfectamente orientado a la creación de una estructura documental.
- Los elementos para analizar a ser integrados se pueden tratar por separado y luego ser integrados de acuerdo a una estructura especialmente elaborada, para que cada una de las partes queden perfectamente combinadas.

ILUSTRACIÓN 33 FIGURA MARCO METODOLÓGICO

7.1. Metodología de Investigación Cuantitativa

El enfoque cuantitativo es secuencial y probatorio. Cada etapa debe terminar para comenzar otra y no se pueden saltar pasos del modelo.

Se comienza por la elaboración de una idea que debe definir su alcance. Una vez realizada esta tarea, se derivan los objetivos y preguntas de investigación, si ese fuese el caso, se revisa la literatura asociada al tema y se construye el marco teórico. Se establece el aporte de valor del trabajo y se determinan las variables relevantes que servirán para validar las metas propuestas. Se desarrolla un plan, para probar las variables (diseño), se miden las variables en un escenario controlado, se analizan los resultados obtenidos de la medición de variables y se establecen las conclusiones respecto a las metas planteadas. Este proceso se observa en la figura del modelo del marco metodológico.

La primera fase es el inicio de la investigación o proyecto, donde se presenta la idea que será estudiada. La idea representa el primer acercamiento a la realidad que se quiere estudiar, sin importar qué tipo de paradigma fundamente el estudio ni el enfoque que se adopte. En esta fase no se puede descartar la idea por buena o mala, pues hace falta más análisis e información para decidir.

En la segunda fase, se plantea el problema de investigación, se establecen los objetivos de investigación, las preguntas de investigación (si fuese necesario), se justifica la investigación y se evalúan las deficiencias en el conocimiento del problema. De nada sirve contar con un buen método, si no se tiene claro qué problema se quiere resolver.

El tiempo de pasar de la fase 1 a la fase 2 es relativa y depende de cuán familiarizado con el tema esté el investigador. En esta etapa, se necesita el problema específico en términos concretos y explícitos, de manera que sea susceptible de investigarse con procedimientos científicos (Selltiz, 1980). Ahora bien, como dice (Ackoff, 1967), un problema bien planteado está parcialmente resuelto.

En la siguiente fase, se revisa la literatura asociada al tema y se construye el marco teórico. Según (Hernández R., 2010) el desarrollo de esta fase da como resultado, por un lado, un proceso de inmersión en el conocimiento existente correlacionado con el problema planteado, y por otro lado un producto, el marco teórico (Eds, 2005). Este paso sustenta, valida y encuadra teóricamente el estudio (Hernández Sampieri, 2009) (Rojas Soriano, 2002).

En la fase cinco, se define el fin del estudio. Además, se definen las variables que ayudarán a medir y validar el fin del estudio. La variable es una propiedad de variación que puede medirse u observarse.

En la fase seis, el investigador debe visualizar la manera práctica y concreta de medir las variables definidas en la fase anterior, para validar los objetivos específicos del proyecto. En esta fase se diseña el experimento, se fija el contexto basado en los alcances fijados para el proyecto.

La fase siete se centra en “qué o quiénes”, es decir, en los participantes, objetos, sucesos o comunidades de estudio, de las cuales depende del planteamiento del proyecto. Se define la población, se elige el método de selección de la muestra (probabilístico o no probabilístico), se define el tamaño de la muestra, el proceso de selección y la obtención de la muestra.

En la siguiente fase se recolectan los datos pertinentes sobre los atributos, conceptos o variables del caso de análisis. Recolectar los datos implica la elaboración de un plan que permita conseguir este objetivo. Para esto se debe tener en cuenta y determinar las fuentes de obtención de datos, la localización de estas fuentes, el proceso de recolección de los datos y cómo finalmente los analizaremos para responder al planteamiento del problema. Esta fase es fundamental para la obtención de resultados y cumplimiento de objetivos, se menciona el proceso de obtención de los datos.

En la fase nueve, se realiza la tarea de análisis de los datos obtenidos en la fase anterior. Actualmente, este proceso se realiza por medio de computadores y

softwares especializados. Es por esto por lo que además del análisis de los datos, esta fase se encarga de la interpretación de los resultados del análisis.

La última fase, se encarga de presentar los resultados del análisis de los datos realizados en la fase anterior. Se comunicarán los resultados mediante un reporte, el cual puede presentarse en distintos formatos: un libro, un artículo para una revista o congreso, un diario, una presentación, un documento técnico, una tesis, entre otras posibilidades. En cualquiera de los casos, debemos describir la investigación realizada y los descubrimientos producidos.

Todas estas fases estarán implícitas en el desarrollo de esta tesis.

7.2. Gantt de Actividades

Según nuestra programación, las actividades del estudio cuantitativo se desarrollan en los siguientes plazos:

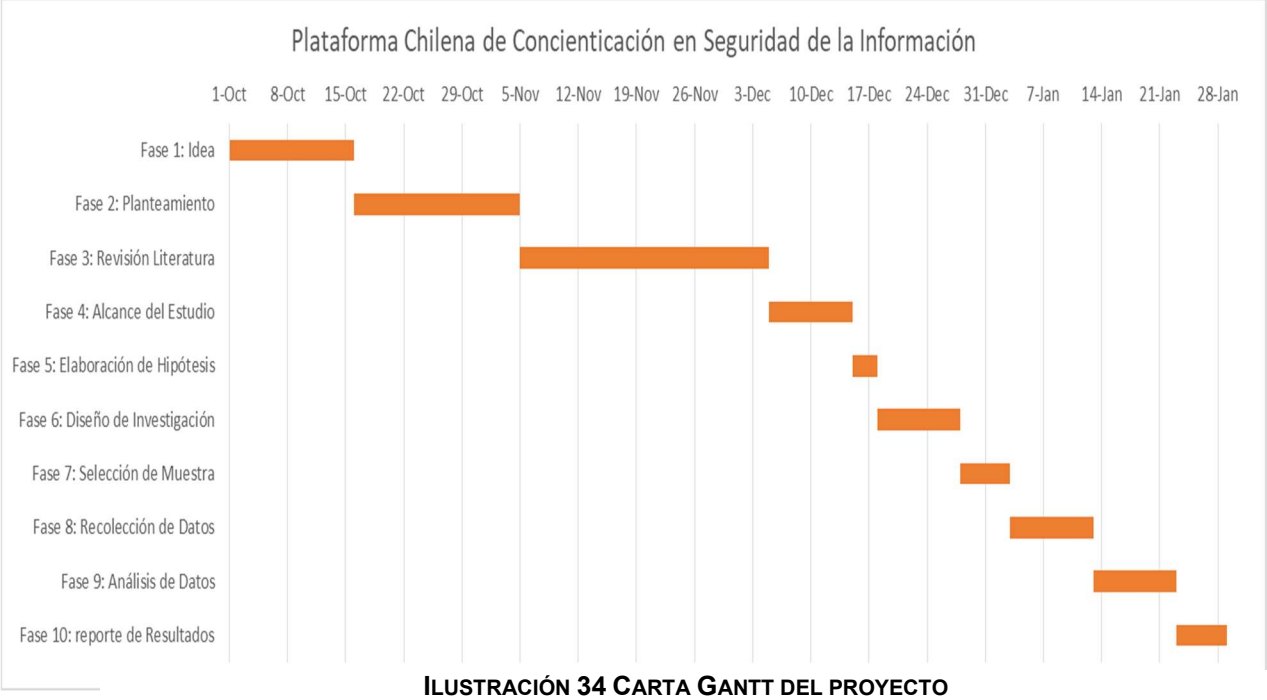


ILUSTRACIÓN 34 CARTA GANTT DEL PROYECTO

8. DEFINICIÓN DE REQUERIMIENTOS

Para el correcto diseño de la plataforma y cumplimiento de los objetivos planteados es necesario dar cobertura a los requerimientos que el desafío presenta de manera adecuada, a través de los distintos módulos que componen la PCCSI. En este apartado se establecerán los requerimientos funcionales y los requerimientos no funcionales, que serán necesarios para el desarrollo de la solución establecida en esta tesis.

8.1. Requerimientos Funcionales

A continuación, se especificarán los requerimientos funcionales de la aplicación que se está desarrollando en este proyecto de tesis. Cada cuadro describirá el detalle de los requerimientos principales para cada módulo, posteriormente estos requerimientos contendrán los paquetes de trabajo que se definieron en la EDT *(Tabla 4).*

TABLA 7 REQUERIMIENTO FUNCIONAL 01

Requerimientos Funcionales	
Identificación del Requerimiento:	RF01
Nombre del Requerimiento:	Envío de Pruebas de Phishing.
Características:	Los administradores podrán crear correos falsos y programar el envío a sus usuarios, los cuales serán registrados su apertura y registro de datos personales.
Descripción del Requerimiento:	El sistema deberá disponer de un módulo en donde se creen, editen y programen correos electrónicos a los usuarios registrados y licenciados. El módulo debe realizar seguimiento de cada correo para entender si fue abierto, o incluso si el usuario registró información personal o de la empresa.
Requerimiento No Funcional:	RNF02, RNF03, RNF04, RNF05,RNF06,RNF07, RNF08
Prioridad del requerimiento: Alta	

TABLA 8 REQUERIMIENTO FUNCIONAL 02

Requerimientos Funcionales	
Identificación del Requerimiento:	RF02
Nombre del Requerimiento:	Envío de Pruebas de Ramsonware.
Características:	Los administradores podrán crear correos falsos y programar el envío a sus usuarios, los cuales serán registrados su apertura y registro de descargas de link malicioso.
Descripción del Requerimiento:	El sistema deberá disponer de un módulo en donde se creen, editen y programen correos electrónicos a los usuarios registrados y licenciados. El módulo debe realizar seguimiento de cada correo para entender si fue abierto, o incluso si el link fue seguido por el usuario.
Requerimiento No Funcional:	RNF01, RNF02, RNF03, RNF04, RNF05. RNF06, RNF07
Prioridad del requerimiento: Alta	

TABLA 9 REQUERIMIENTO FUNCIONAL 03

Requerimientos Funcionales	
Identificación del Requerimiento:	RF03
Nombre del Requerimiento:	Módulo de Capacitación Técnica.
Características:	Módulo de despliegue de videos y contenido educativo con seguimiento para usuarios de las empresas.
Descripción del Requerimiento:	El sistema debe proporcionar un módulo educativo que permita ver vídeos, y realizar los cursos cargados para cada usuario, debe tener seguimiento e informe de estos.
Requerimiento No Funcional:	RNF01, RNF02, RNF03, RNF04, RNF05. RNF06, RNF07
Prioridad del requerimiento: Media	

TABLA 10 REQUERIMIENTO FUNCIONAL 04

Prioridad del requerimiento: Alta	
Requerimientos Funcionales	
Identificación del Requerimiento:	RF04
Nombre del Requerimiento:	Evaluaciones.
Características:	El módulo de evaluaciones permite medir el nivel de conocimiento obtenido por los usuarios mediante la programación de tests de respuestas múltiples y evaluación de casos.
Descripción del Requerimiento:	El proceso deberá presentar al usuario test de conocimientos en seguridad de la información según lo contenidos enviados y módulos de estudio realizados.
Requerimiento No Funcional:	RNF01, RNF02, RNF03, RNF04, RNF05. RNF06, RNF07, RNF08
Prioridad del requerimiento: Alto	

TABLA 11 REQUERIMIENTO FUNCIONAL 05

Requerimientos Funcionales	
Identificación del Requerimiento:	RF05
Nombre del Requerimiento:	Envío de Newsletter y Campañas.
Características:	Los usuarios podrán recibir correos programados sobre información importante, tips de seguridad o advertencias que deban conocer sobre Seguridad.
Descripción del Requerimiento:	El sistema deberá poseer un módulo que permita enviar correo electrónico válido con contenido educativo o informativo de manera recurrente y programada.
Requerimiento No Funcional:	RNF01, RNF02, RNF03, RNF04, RNF05. RNF06, RNF07, RNF08
Prioridad del requerimiento: Media	

TABLA 12 REQUERIMIENTO FUNCIONAL 06

Requerimientos Funcionales	
Identificación del Requerimiento:	RF06
Nombre del Requerimiento:	Reportes e Informes.
Características:	Los administradores de las empresas clientes podrán recibir informes de estado del avance global de la organización. Los usuarios podrán recibir informes de su estado de conocimiento sobre seguridad.
Descripción del Requerimiento:	El sistema deberá poseer un módulo que enviara reportes e informes tanto a administradores como a usuarios finales.
Requerimiento No Funcional:	RNF01, RNF02, RNF03, RNF04, RNF05. RNF06, RNF07
Prioridad del requerimiento: Media	

TABLA 13 REQUERIMIENTO FUNCIONAL 07

Requerimientos Funcionales	
Identificación del Requerimiento:	RF07
Nombre del Requerimiento:	Directorio y Licenciamiento
Características:	Se requiere administrar usuarios finales y grupos de las empresas clientes y administrar su licenciamiento
Descripción del Requerimiento:	El sistema deberá poseer un módulo que permita crear o importar los listados de usuarios de las empresas cliente, esto se puede realizar de manera automática vía Active Directory, archivos de texto plano o Excel. Posteriormente permitirá crear subgrupos internos.
Requerimiento No Funcional:	RNF01, RNF02, RNF03, RNF04, RNF05. RNF06, RNF07
Prioridad del requerimiento: Media	

TABLA 14 REQUERIMIENTO FUNCIONAL 08

Requerimientos Funcionales	
Identificación del Requerimiento:	RF08
Nombre del Requerimiento:	Infraestructura Redundante Bajo Costo
Características:	La infraestructura debe tener uptime de al menos 99,999% y su costo debe estar relacionado al uso y crecimiento de la misma.
Descripción del Requerimiento:	La infraestructura y sus costos deben crecer con relación a la necesidad de uso, para evitar una inversión inicial muy alta, y orientar los flujos de caja hacia el pago mensual de servicios.
Requerimiento No Funcional:	RNF06, RNF07, RNF08
Prioridad del requerimiento: Media	

8.2. Requerimientos No Funcionales

Posteriormente a la definición de los requerimientos funcionales, se establecerán los requerimientos no funcionales para el proyecto. Estos requerimientos serán transversales en todo el proyecto, por lo tanto, cada requerimiento no funcional estará asociado a un requerimiento funcional definido en el apartado anterior.

TABLA 15 REQUERIMIENTO NO FUNCIONAL 01

Requerimientos No Funcionales	
Identificación del Requerimiento:	RNF01
Nombre del Requerimiento:	Conexión LDAP
Características:	El sistema interactuará con sistemas de directorio de los clientes para la creación de usuarios y asignación de licencias.
Descripción del Requerimiento:	El sistema deberá tener un modelo de conexión vía ldap, radius o protocolos de autenticación para importar y crear usuarios del cliente.
Prioridad del requerimiento: Alta	

TABLA 16 REQUERIMIENTO NO FUNCIONAL 02

Requerimientos No Funcionales	
Identificación del Requerimiento:	RNF02
Nombre del Requerimiento:	Diseño modalidad SaaS
Características:	El sistema será utilizado por usuarios con distintos niveles de privilegios (administradores, usuarios finales, revendedores) desde la web sin instalar componentes.
Descripción del Requerimiento:	Se deberá soportar la modalidad de Software as a Service, en donde los clientes no necesitarán de ningún tipo de instalación o disponer de algún tipo de arquitectura.
Prioridad del requerimiento: Alta	

TABLA 17 REQUERIMIENTO NO FUNCIONAL 03

Requerimientos No Funcionales	
Identificación del Requerimiento:	RNF03
Nombre del Requerimiento:	Disponibilidad del Sistema
Características:	El sistema debe operar en un esquema de al menos cinco 9 (99,999%).
Descripción del Requerimiento:	El sistema deberá contar con alta disponibilidad, para cumplir con requerimientos y programación de clientes.
Prioridad del requerimiento: Media	

TABLA 18 REQUERIMIENTO NO FUNCIONAL 04

Requerimientos No Funcionales	
Identificación del Requerimiento:	RNF04
Nombre del Requerimiento:	Arquitectura Basada en Microservicios
Características:	El sistema tendrá sus distintos módulos que podrán ser utilizados de forma independiente por los usuarios.
Descripción del Requerimiento:	El sistema deberá ser desarrollado de forma modular que facilite el mantenimiento, permita la migración y facilite la automatización.
Prioridad del requerimiento: Media	

TABLA 19 REQUERIMIENTO NO FUNCIONAL 05

Requerimientos No Funcionales	
Identificación del Requerimiento:	RNF05
Nombre del Requerimiento:	Lenguaje de Alto Nivel
Características:	El sistema será programado en un lenguaje de programación robusto e incremental.
Descripción del Requerimiento:	Para el desarrollo del sistema se deberá utilizar el lenguaje de programación Python
Prioridad del requerimiento: Alto	

TABLA 20 REQUERIMIENTO NO FUNCIONAL 06

Requerimientos No Funcionales	
Identificación del Requerimiento:	RNF06
Nombre del Requerimiento:	Base de datos Relacional
Características:	El sistema deberá utilizar una base de datos PostgresSQL en la última versión disponible.
Descripción del Requerimiento:	El sistema utilizará una base de datos robusta y que soporte una gran cantidad de operaciones simultaneas
Prioridad del requerimiento: Alta	

TABLA 21 REQUERIMIENTO NO FUNCIONAL 07

Requerimientos No Funcionales	
Identificación del Requerimiento:	RNF07
Nombre del Requerimiento:	Interfaz de Usuario
Características:	El sistema debe ser fácil de entender y usar.
Descripción del Requerimiento:	La interface del sistema deberá ser amigable e intuitiva siguiendo estándares de UI/UX, dentro de un formato WEB.
Prioridad del requerimiento: Alta	

TABLA 22 REQUERIMIENTO NO FUNCIONAL 08

Requerimientos No Funcionales	
Identificación del Requerimiento:	RNF08
Nombre del Requerimiento:	Backup del Sistema
Características:	De Manera programada y automática se realizarán backups de todos los módulos y contenidos.
Descripción del Requerimiento:	Se deberá poseer un proceso automatizado de respaldos de los datos, estos respaldos deberán seguir el esquema 3,2,1 (tres copias, dos medios, 1 fuera del datacenter).
Prioridad del requerimiento: Alta	

8.3. Trazabilidad entre requerimientos funcionales y objetivos

A continuación, se presenta una matriz de trazabilidad entre los objetivos específicos y los requerimientos funcionales de la solución, ver Tabla 7-11.

TABLA 23 TRAZABILIDAD DE CUMPLIMIENTO DE OBJETIVOS ESPECÍFICOS

Objetivo Específico	RF01	RF02	RF03	RF04	RF05	RF06	RF07	RF08
OE01	X	X	X	X	X		X	X
OE02	X	X	X	X	X		X	X
OE03						X	X	X

9. DESARROLLO DE LA SOLUCIÓN

9.1. Descripción de la Solución

La PCCSI es una plataforma de educación automatizada en materias de seguridad de la información, que se ejecuta en infraestructura hiperconvergente de pago por uso.

9.1.1. ¿Que Posee la PCCSI?

La aplicación consiste en tres módulos principales:

- Autenticación: Consiste en la Identificación de los Clientes Internos/ Externos a nivel de Active Directory, Ldap u otros y accesos de los administradores locales, además del control de licenciamiento de toda la plataforma.
- Sitio Administrador: Este sitio es donde cargan los módulos y donde se manejan las campañas que se entregan por compañía y a los usuarios.
- Sitio Usuarios: Es donde el usuario se capacita y accede a realizar sus evaluaciones y nos entrega su Feedback.

Según se diagrama a continuación:

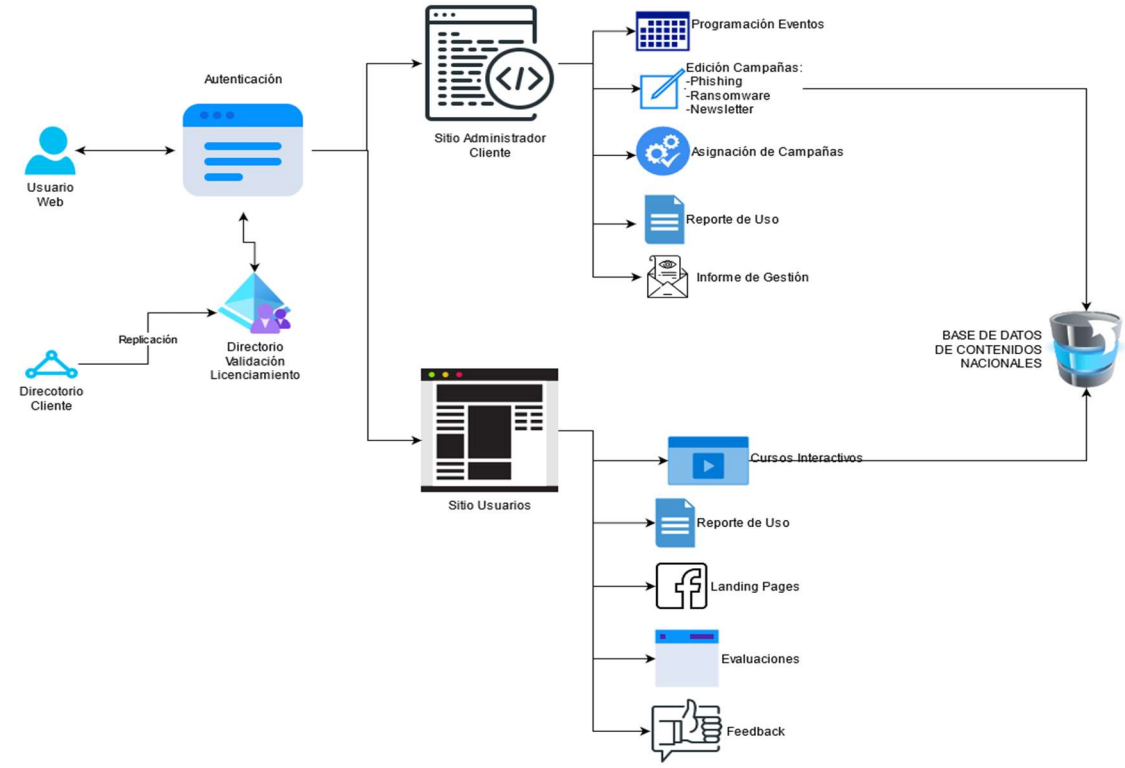


ILUSTRACIÓN 35 ESQUEMA FUNCIONAL DE PCCSI

Además, la plataforma considera los siguientes módulos de operación que confirman la plataforma.

9.1.2. Módulos Interactivos

Los Módulos Interactivos combinan diversos métodos de interacción, de contenido multimedia con contenido nacional y contingente a la realidad local, esto permite a los usuarios de una organización asimilar de una forma fluida y entretenida los diferentes tópicos de capacitación.

Dichos tópicos son diseñados sobre la base de la actualidad local que sucede en Chile además y que busca captar el interés del usuario con algunos temas predefinidos como política, deporte, salud, viajes, religión entre otros, además de contar con buena calidad de todo el contenido que está pedagógicamente preparado para lograr cambios de hábitos permanentes.

Universidad Andrés Bello

Todos los módulos presentan contenidos desarrollados por expertos en Seguridad de la Información y periodistas que se mantienen siempre actualizados para que los usuarios siempre mantengan el interés con contenido real y local.

A continuación, se detallan algunos de los módulos que posee nuestra plataforma:

TABLA 24 DESCRIPCIÓN DE MÓDULOS DE LA PLATAFORMA

1.- Seguridad General	
Descripción	Cumplimiento
Introduce a sus usuarios en los conceptos básicos de Seguridad de la Información. Da a conocer el papel de ellos en la seguridad de la organización.	ISO 27002 7.2.2 Día de la seguridad de la información u otros días 7.2.2 Reporte de incidentes

2.- Ingenieria Social	
Descripción	Cumplimiento
Concientiza a sus usuarios acerca de la existencia de esta disciplina y los instruye en la prevención y correcta reacción frente a los diversos tipos de ataque que un Ingeniero Social malintencionado puede realizar en su contra.	ISO 27002 16.1.2 Errores humanos

3.- Phishing	
Descripción	Cumplimiento
Capacita a sus usuarios en la prevención de este tipo de trampas mediante su identificación y reporte. A su vez entrena a sus usuarios en la correcta reacción en caso de ser víctimas de ellas.	ISO 27002 13.2.4 Notificación de divulgación o fugas de información

4.- Ransomware	
Descripción	Cumplimiento
Explica a sus usuarios qué es el Ransomware y cómo prevenir una infección de este tipo haciendo foco en aquellas vías de infección que necesitan de la interacción del usuario final para hacerse efectiva.	ISO 27002 6.2.1 Malware 6.2.2 Malware 7.2.2 Malware 13.2.1 Malware

9.1.3. Los Newsletters

Los Newsletters son correos electrónicos o publicaciones utilizados para concientizar a cada usuario según sus temas de interés (política, deporte, salud, viajes, religión y otros), el cual se relacionará a la vez entre temas de contingencia nacional y de seguridad de la información que busca generar un cambio de

comportamiento a través de la presentación de la información que el usuario eligió ver y es de su interés.

Nuestra plataforma al igual que otras del mercado le permite establecer un cronograma de envío de publicaciones que mantendrá a los usuarios atentos y conscientes de los riesgos a los que se exponen, pero relacionándolo con temas de interés elegidos por los mismos usuarios lo que además de afianzar conceptos claves sobre Seguridad de la Información le permitirá estar familiarizado con la información que va recibiendo, implicando un esfuerzo mínimo de su parte dado que es información real y de interés.

La plataforma permite realizar seguimiento y medición de la eficiencia de sus envíos a través de los reportes y pruebas que brinda nuestra plataforma.

9.1.4. Simulación de Phishing

Nuestra plataforma permite planificar y personalizar campañas de correos electrónicos de Phishing simulado que tendrán relación con los temas de interés de cada grupo de usuarios, estas campañas se configuran en un par de pasos y se envían fácilmente.

A través de esta herramienta podrá conocer las acciones de riesgo que ponen en peligro la seguridad de la información de su organización, e identifica a los usuarios que están más vulnerables en cuanto a conocimiento.

El envío de nuestros contenidos de preferencia va personalizado según el grupo de usuarios, pero también contamos con los típicos contenidos predefinidos que utilizan otras plataformas, lo importante es que para ambos casos se mantienen actualizados y cubren las técnicas y temáticas de Phishing más frecuentes y novedosas utilizadas por los ciberdelincuentes.

La finalidad de esta simulación es identificar los grupos de riesgo entre sus usuarios con reportes y estadísticas del estado actual y avance de los usuarios

en relación con la asimilación de los hábitos seguros, para luego iniciar la concientización que le permitirá bajar las incidencias de seguridad.

A continuación, se entrega un Ejemplo Predefinido de Netflix:

Envío de correo:

ILUSTRACIÓN 36 SIMULACIÓN DE PHISHING

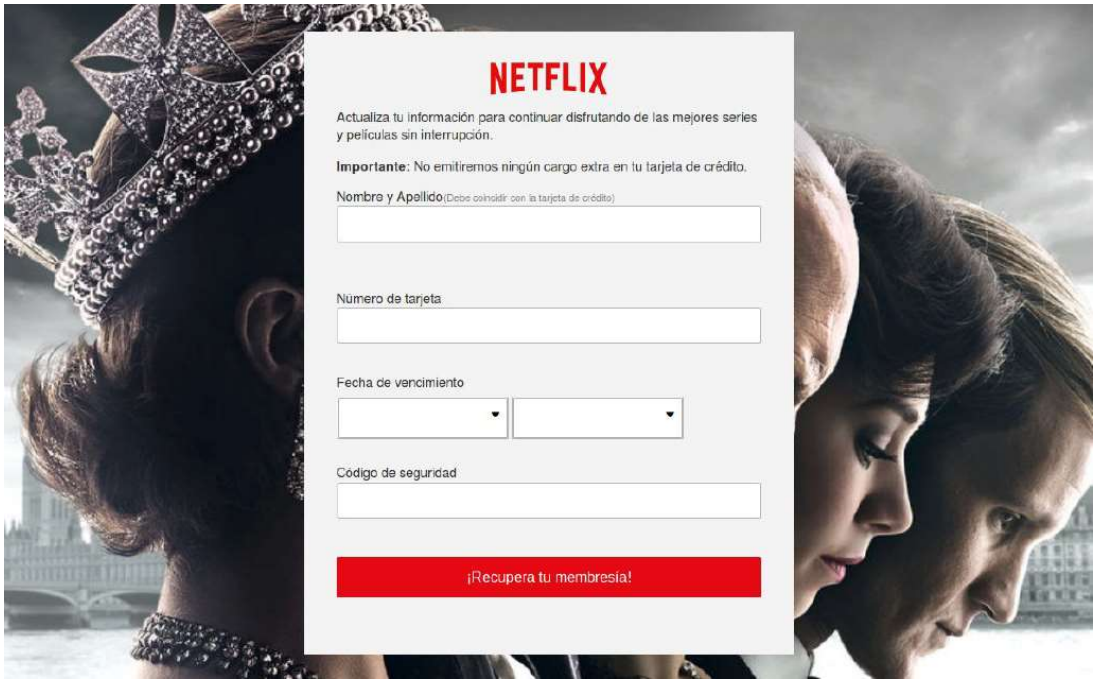


ILUSTRACIÓN 37 PÁGINA DE DESTINO DE UN PHISHING

9.1.5. Simulación de Ransomware

Nuestra plataforma permite planificar y personalizar campañas de correos electrónicos de Ransomware simulado que tendrán relación con los temas de interés de cada grupo de usuarios, estas campañas se configuran en un par de pasos y se envían fácilmente.

A través de esta herramienta podrá conocer las acciones de riesgo que ponen en peligro la seguridad de la información de su organización, e identifica a los usuarios que están más vulnerables en cuanto a conocimiento.

El envío de nuestros contenidos de preferencia va personalizado según el grupo de usuarios, pero también contamos con los típicos contenidos predefinidos que utilizan otras plataformas, lo importante es que para ambos casos se mantienen actualizados y cubren las técnicas y temáticas de Ransomware más frecuentes y novedosas utilizadas por los ciberdelincuentes.

La finalidad de esta simulación es identificar los grupos de riesgo entre sus usuarios con reportes y estadísticas del estado actual y avance de los usuarios en relación con la asimilación de los hábitos seguros, para luego iniciar la concientización que le permitirá bajar las incidencias de seguridad.

A continuación, se entrega un Ejemplo Predefinido de una actualización Urgente de Seguridad:

Envío de correo:

Estimado $name,

Desde el departamento de Tecnología solicitamos descargue URGENTE la actualización que se envía adjunta.

Los pasos a seguir son sumamente simples:

1. Descargue el archivo adjunto
2. Haga doble clic en el mismo

La actualización se realizará de manera automática.

Por favor, realizar este procedimiento de manera URGENTE, de lo contrario, la información de su equipo podría ser robada por un ciberdelincuente.

Muchas gracias.

ILUSTRACIÓN 38 SIMULACIÓN DE RAMSONWARE

ILUSTRACIÓN 39 PÁGINA DE DESTINO RANSOMWARE

9.1.6. Concientización Express

Nuestra plataforma contiene una serie de plantillas que dan la opción de iniciar el proceso de concientización en modo abreviado, justo cuando el usuario es

víctima de la simulación de Phishing o Ransomware que hemos planificado, esto generalmente le permitirá al usuario asimilar de mejor forma que ha incurrido en acto inseguro que compromete la seguridad de la información de su organización o propia.

Esta Concientización Express es 100% voluntaria y depende de cada administrador si quiere activarla o no al momento en que los usuarios incurres en actividades inseguras.

9.1.7. Evaluaciones y Feedback de los Usuarios

Como dijo el físico y matemático William Thomson (Thomson, 1952), *"Lo que no se define no se puede medir. Lo que no se mide no se puede mejorar. Lo que no se mejora, se degrada siempre".*

Seria Impensado tener una plataforma de concientización de seguridad de la información sin definir los puntos de evaluación e ir midiendo los conocimientos de los usuarios con respecto a los contenidos de concientización desde que se inicia el proceso hasta que termina cada etapa, para luego tomar acciones sobre cada medición que nos permitan poner foco en los temas más críticos e ir mejorando los resultados futuros.

Por otra parte, es clave el feedback de los usuarios para tener una mirada completa de cómo es su percepción de la plataforma y donde puedan indicar que temas podemos agregar o mejorar para lograr una mejor asimilación del contenido entregado en cada módulo.

Nuestra plataforma incluye los módulos de Evaluaciones y Feedback de los usuarios, con informes y gráficos que facilitan su entendimiento y presentación a la alta gerencia.

9.2. Solución Tecnológica

9.2.1. Arquitectura de Hardware

El diseño de nuestra Plataforma requiere de alta disponibilidad en todo momento, además debe ser tolerante a fallas en un ambiente hibrido, donde podamos realizar replicas entre Datacenters y hacia la nube publica de manera simple basado en un modelo de pago por uso para no disparar nuestros costos iniciales y tener flexibilidad cuando necesitemos más recursos, con esto, todos los clientes internos de nuestra organización y clientes externos que requieran de los servicios que ofrecemos, tendrán asegurada la disponibilidad y confiabilidad de los recursos que necesiten.

9.2.1.1. Características de los Productos

Nuestra solución está compuesta por los servicios de Nube de HPE GreenLake, Software Vmware, Microsoft, Red Hat y Veeam para Backup en Nube, lo cual se integra con los desarrollos propios de los sistemas que ofrecemos.

Detalle del Hardware:

- ✓ Switches Core
- ✓ Switches SAN para conectar el Storage con los Chasis.
- ✓ Storages de alta Gama tolerante a fallos con 100% de disponibilidad.
- ✓ Chasis con hojas de Cómputo y Cajones de Almacenamiento para la Hyperconvergencia con VSAN.
- ✓ Chasis con hojas de Computo para Escritorios Virtuales – VDI.

Software

- ✓ Licenciamiento Vmware:
    - vSphere, vCenter.
    - vSan, NSX.

- Horizon.
- Cloud Foundation.

✓ Licenciamiento Microsoft:

- Windows para Estaciones de Trabajo.
- Microsoft 365.

✓ Licenciamiento Red Hat:

- Red Hat Enterprise Linux Server
- Docker

✓ Licenciamiento y Almacenamiento para Backup:

- Veeam Backup & Replication Enterprise Plus
- Espacio en la Nube Wasabi para Backup 60 TB.

9.2.1.2. Características de la Plataforma

La plataforma tecnológica está compuesta por hardware físico ubicado en 2 datacenters distintos dentro del territorio nacional, ambos sitios tienen la misma capacidad de cómputo y conectividad configurados en modo Activo-Activo conectados en Layer 2 vía fibra oscura redundante en anillo a 40Gbps con una latencia menor a 1 mS, estos sitios contienen máquinas virtuales las cuales entregan servicios a la red interna de usuarios locales y las aplicaciones que requiere nuestra plataforma PCCSI, para operar con todos sus módulos con una cantidad de hasta 15.000 usuarios en forma simultánea sin que esto genere una degradación en la entrega del servicio.

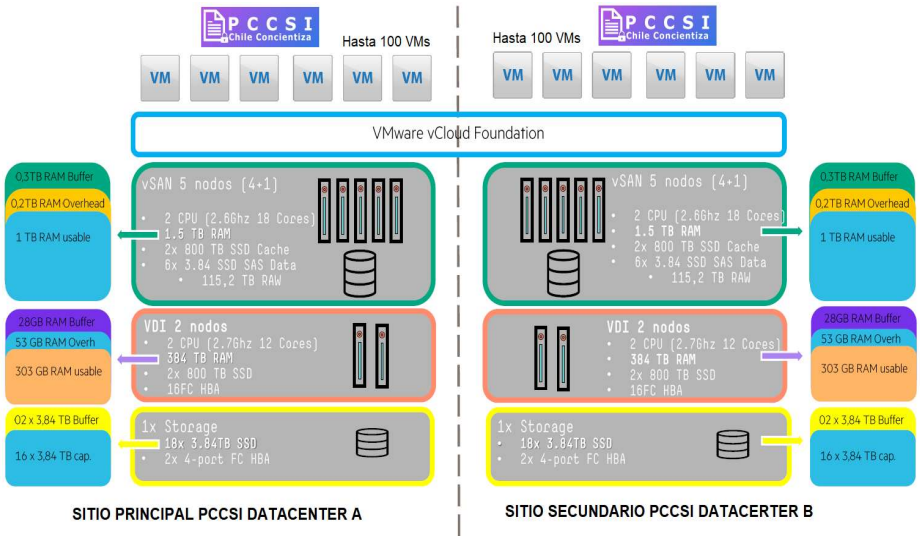


ILUSTRACIÓN 40 PLATAFORMA DE HARDWARE REQUERIDA

9.2.1.3. Diseño Distribuido

La siguiente imagen muestra la arquitectura de Hardware de la solución:

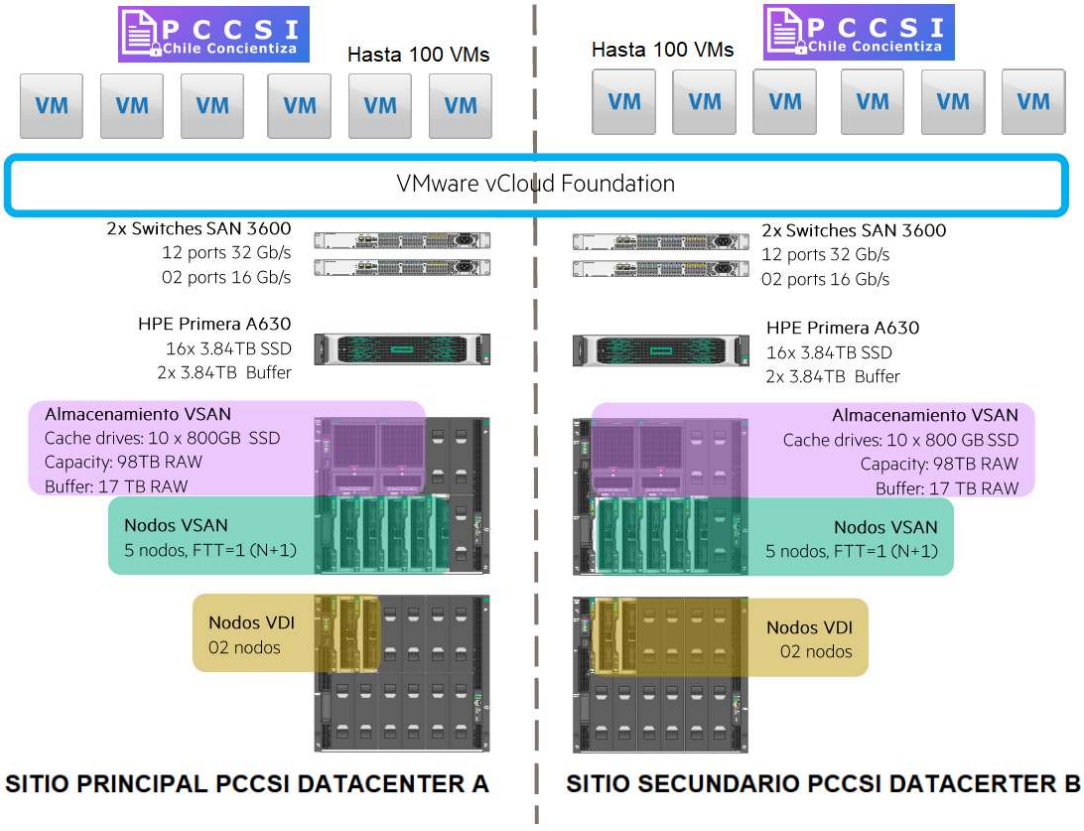


ILUSTRACIÓN 41 IMPLEMENTACIÓN DE LA ARQUITECTURA

A continuación, se detalla el Hardware que compone esta arquitectura:

- ✓ Switches Core de los datacenters de 40Gbps.
- ✓ Switches HPE SAN SN 3600B. (HPE SN3600B, 2020)
- ✓ Storages HPE Primera A630. (HPE Primera, 2021)
- ✓ Chasis HPE Synergy 12000 (HPE SYNERGY, 2021)
    a. 05 Hojas de Computo HPE Synergy 480 Gen10 (HPE SG 480 , 2020)
    b. 02 cajones de Discos HPE 3940 (HPE D3940 , 2021)
- ✓ Chasis HPE Synergy 12000 (HPE SYNERGY, 2021)
    a. 05 Hojas de Computo HPE Synergy 480 Gen10 (HPE SG 480 , 2020)
    b.

9.2.1.4. Solución de Almacenamiento

La infraestructura elegida para el almacenamiento de las Bases de datos e información de los módulos Interactivos, Newsletters y la plataforma PCCSI en general estará compuesta por 2 Storages HPE Primera 630 2N, cada uno con 52,63 TB usables sin considerar Deduplicación ni Compresión y con 100% de disponibilidad garantizada por el fabricante (HPE Primera, 2021).

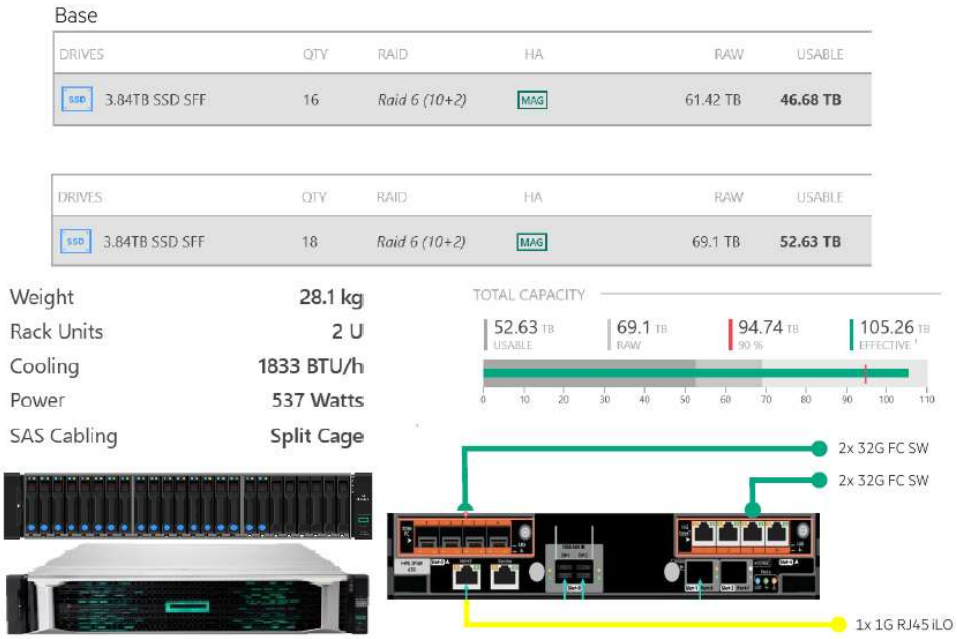


ILUSTRACIÓN 42 STORAGES HP PRIMERA

9.2.1.5. Esquema de Conectividad

A continuación, se muestra como estará conectado todo el Hardware en cada Datacenter.

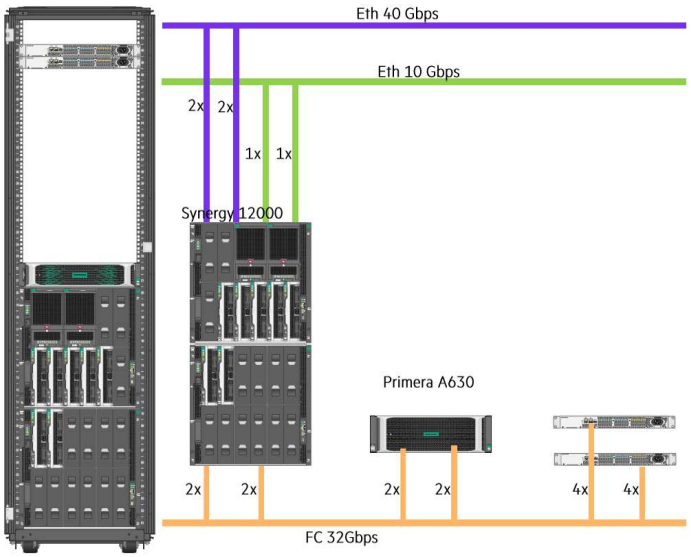


ILUSTRACIÓN 43 ESQUEMA DE CONECTIVIDAD LOCAL

9.2.1.6. Centros de Datos

Los data centers donde se encuentra la infraestructura de nuestra plataforma son centros de datos nacionales certificados TIER III y se encuentran acreditados bajo las normas:

- ISO/IEC 27001
- SOC 1 y SOC 2/SSAE 16/ISAE 3402 (Previamente SAS 70 Tipo II)
- PCI Nivel 1

9.2.2. Arquitectura de Software

Todo el backend de la aplicación se encuentra desarrollado en lenguaje Python, utiliza el framework Django e incorpora las mejores prácticas en desarrollo web seguro (OWASP), y cuenta con las siguientes características:

- El Frontend hace uso de HTML5, CSS3, Bootstrap y JQuery.
- Como servidor de Base de Datos se utiliza PostgreSQL
- Los correos electrónicos se envían a través de un servidor de correos propio con registros SPF, DKIM y DMARC válidos.
- Tanto el motor de base de datos como los motores de microservicios de aplicación se encuentran alojados en la plataforma de virtualización de nuestros Datacenter.
- Los archivos estáticos (javascripts, css, imágenes) se encuentran almacenados en Los Storages HPE Primera que cuentan con 100% de Disponibilidad

Según el siguiente diagrama:

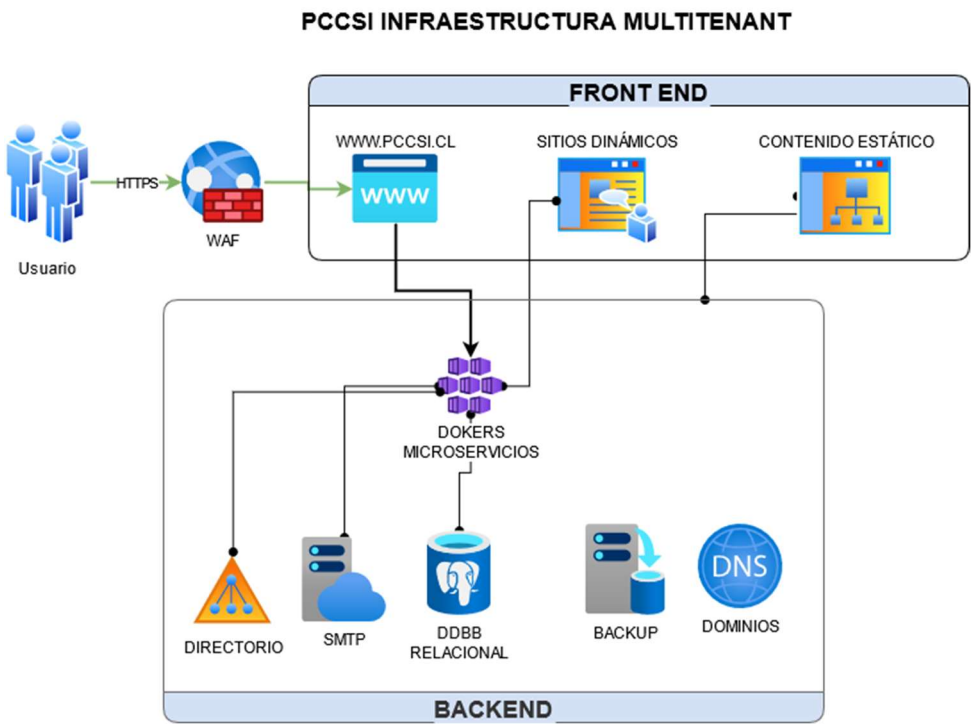


ILUSTRACIÓN 44 DISEÑO INFRAESTRUCTURA

9.2.3. Backup y Réplica a la Nube Pública

Para realizar nuestros Backup utilizamos la aplicación Veeam Backup & Replication Enterprise Plus por instancia (Veeam B&R, 2021), por tiene un precio **de USD 8 dólares por instancia virtual / mes** (96 dólares por Vm / Año aprox) esta licencia nos permite realizar copias en forma local y hacia la nube de todas nuestras máquinas virtuales que definamos.

TABLA 25 PRECIOS REFERENCIAL ANUAL POR VM'S (USD) – VEEAM B&R

Item	Qty	Description	Item Notes	Unit Price	Amount
V-VBRVUL-0I-SU1YP-00	5	Veeam Backup & Replication Universal License. Includes Enterprise Plus Edition features. - 1 Year Subscription Upfront Billing & Production (24/7) Support	Protege hasta 50 VMs	984.00	4,920.00

Elegimos la nube de Wasabi Hot Cloud Storage (Wasabi, 2021) para realizar los Backup por que tiene un precio **de 0,0059 dólares por GB / mes** (5,99 dólares

por TB / mes). Además, a diferencia de Microsoft Azure, Amazon S3 y servicios comparables de Google Cloud Platform, Wasabi no cobra por las solicitudes de salida o API.

Para realizar un cálculo de costos por utilización de espacio en la nube hemos considerado un total de 60TB con un porcentaje de descarga mensual de 25%, lo cual nos entrega la siguiente comparativa:

ILUSTRACIÓN 45 PRECIOS MENSUAL POR TB (USD) – WASABI

Como se aprecia en la ilustración anterior el ahorro en almacenamiento de datos anual entre las nubes más populares es sobre un 85% lo cual nos reafirma la decisión de utilizar la plataforma de Wasabi para Backup, ya que todas las transacciones de producción se realizarán en la Infraestructura alojada en nuestros Datacenters.

9.3. Condiciones Económicas

9.3.1. Pago por Uso Hardware de Ambos Sitios

A continuación, se entrega una valorización mensual en USD, basado en un compromiso mínimo de uso el cual asegura el funcionamiento actual de la plataforma:

TABLA 26 PRECIOS MENSUALES (USD) – HPE GREENLAKE

Configuración	Tier	Minimo Comprometido o Base	Valor Unitario	Unidad de Medida	Total por Mes
Sitio A	VSAN Computo Site 1	5.120	$ 0,80	Compute Unit	$ 4.096
	VDI Computo Site 1	606	$ 1,39	Compute Unit	$ 842
	Storage Capacity VSAN Site 1	98	$ 18,11	TB	$ 1.775
Sitio B	VSAN Computo Site 2	5.120	$ 0,80	Compute Unit	$ 4.096
	VDI Computo Site 2	606	$ 1,39	Compute Unit	$ 842
	Storage Capacity VSAN Site 2	98	$ 18,11	TB	$ 1.775
Storage	Primera Site 1	62	$ 55,61	TB	$ 3.448
	Primera Site 2	62	$ 55,61	TB	$ 3.448
	Switches SAN	4	$ 462,88	Switch	$ 1.852
				TOTAL	**$ 22.173**

Si el consumo aumenta la plataforma estará en condiciones de entregar los recursos necesarios para continuar operando, pero también los costos base aumentarán según la banda de sobre consumo en la cual se mantenga el funcionamiento de la plataforma, entre mayor sea la banda de consumo, más bajo será el valor unitario que pagar, como se aprecia en la siguiente tabla de Bandas:

Configuration	Billing Tier	UoM		Band 1	Band 2	Band 3	Band 4
Sitio A	VSAN Computo Site 1	Compute Unit	Volume	0 - 6,424	6,425 - 7,729	7,730 - 9,035	9,036+
			Price	$0,80	$0,77	$0,72	$0,69
Sitio A	VDI Computo Site 1	Compute Unit	Volume	0 - 819	820 - 1,033	1,034 - 1,248	1,249+
			Price	$1,39	$1,37	$1,34	$1,32
Sitio A	Storage Capacity VSAN Site 1	TB	Volume	0 – 140	141 - 183	184 - 227	228+
			Price	$18,11	$16,96	$15,82	$14,65
Sitio B	VSAN Computo Site 2	Compute Unit	Volume	0 - 6,424	6,425 - 7,729	7,730 - 9,035	9,036+
			Price	$0,80	$0,77	$0,72	$0,69
Sitio B	VDI Computo Site 2	Compute Unit	Volume	0 – 819	820 - 1,033	1,034 - 1,248	1,249+
			Price	$1,39	$1,35	$1,32	$1,30
Sitio B	Storage Capacity VSAN Site 2	TB	Volume	0 – 140	141 - 183	184 - 227	228+
			Price	$18,11	$16,90	$15,68	$14,46
Storage	Primera Site 1	TB	Volume	0 – 74	75 - 87	88 - 99	100+
			Price	$55,61	$54,37	$53,13	$51,88
Storage	Primera Site 2	TB	Volume	0 – 74	75 - 87	88 - 99	100+
			Price	$55,61	$54,37	$53,13	$51,88
Storage	Switches SAN	Switch	Volume	0 - 4			
			Price	$462,88			

TABLA 27 TABLA DE PRECIOS POR BANDA (USD) – HPE GREENLAKE

Sin duda la solución de HPE Greenlake nos permite evitar una gran inversión inicial determinando un consumo base y luego según la necesidad de aumento de recursos ir pagando solo por lo que se usa.

9.3.2. Resumen Pago por Uso Mensual de la Solución

Si consideramos todos los costos estimados que se utilizan por utilización mensual tenemos el siguiente resumen:

TABLA 28 COSTOS ESTIMADOS TOTALES POR MES (USD) – PLATAFORMA PCCSI

Ítem	Descripción de Productos y Servicios	Costo Mensual USD Aprox
1	Costos de Datacenters (Rack, Energía, Enlaces de Datos, Enlaces de Internet, Firewall, Balanceadores)	USD 5.000
2	Hardware HPE GreenLake (Hardware HPE, Servicios de Habilitación, Soporte y Mantención, Licencias Vmware, Licencias Microsoft, Licencias Red Hat	USD 22.173
3	Licencias de Backup Veeam para 100 Máquinas Virtuales	USD 800
4	Pago de Almacenamiento a la Nube de Wasabi para 60TB	USD 359
Valor Total Mensual Estimado en USD$		**USD 28.332**

10. REALIZACIÓN DE PRUEBAS DE LA SOLUCIÓN

10.1. Simulación de Phishing

Durante el periodo noviembre 2020 y enero 2021 se realizó un proceso de evaluación de detección de correo malicioso a 100 personas de la empresa WOM, el cuales fueron seleccionados al azar por selección simple, basado en su correo electrónico entre los 2533 trabajadores de la empresa. El Proceso consistió en la ejecución de dos campañas de correos maliciosos simulados, con procesos previos de concientización vía correo electrónico y workplace (intranet corporativa). Durante la segunda campaña se envió previamente información de concientización personalizada y cercana al grupo objetivo de prueba. La realización de la campaña fue aprobada por el Gerente de Core Platform de WOM.

10.1.1. Campaña Inicial de Concientización

Durante el mes de noviembre de 2020 se realizó un primer envío de correos de concientización basados en las campañas propuestas por el Instituto Nacional de Ciberseguridad Español (INCIBE), que ofrece un kit de concientización para realizar campañas de seguridad en las empresas. (Instituto Nacional de Ciberseguridad Español, s.f.). El material se presentó tal como se descargó desde la fuente, por tiempo y no recursos no se realizó ninguna personalización a la información utilizada.

ILUSTRACIÓN 46 MENSAJES UTILIZADOS DURANTE CAMPAÑA DE CONCIENTIZACIÓN INICIAL

10.1.2. Email enviado Campaña Inicial

Una vez finalizado el proceso de concientización inicial, se realizó el envío de phishing a 100 personas seleccionadas al azar, el cual contenía algunos indicadores de phishing como faltas de ortografía y una promoción atractiva para los usuarios, el cual buscaba obtener información personal del usuario.

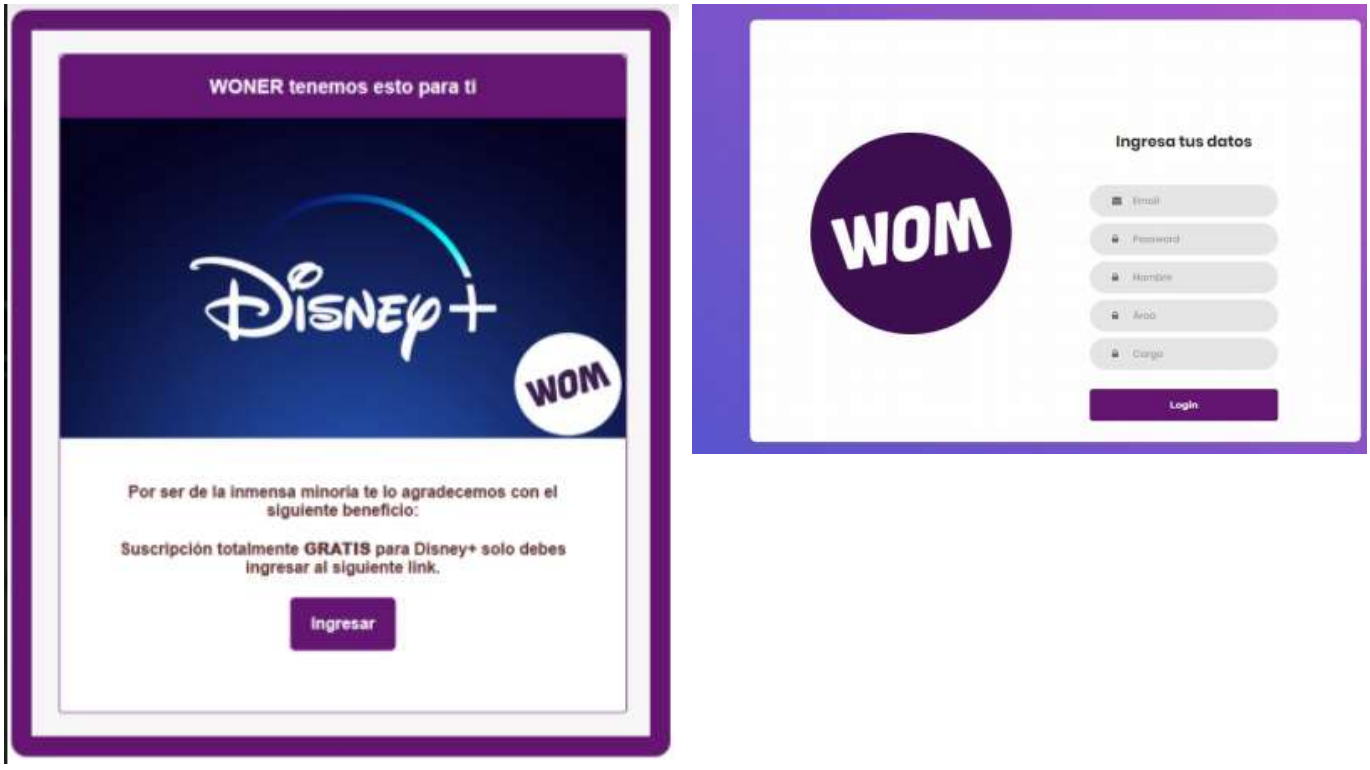


ILUSTRACIÓN 47 CORREO ELECTRÓNICO MALICIOSO INICIAL

10.1.3. Campaña Final

A finales de diciembre se comenzó una campaña de concientización que contó con el apoyo del área de Valor Humano de la compañía, quienes ofrecieron su apoyo para personalizar el contenido y hacerlo más cercano a los usuarios seleccionados y de esta manera mejorar la recepción de la información. Se realizaron seis envíos distintos de correos y publicaciones vía workplace y además se ejecutó una encuesta buscando evaluar si los trabajadores habían recibido la información y aprendido al respecto.

ILUSTRACIÓN 48 EJEMPLO DE CAMPAÑA DE CONCIENTIZACIÓN PERSONALIZADA

10.1.4. Email enviado Campaña Final

Finalmente, con el fin de probar la campaña de concientización realizada se realizó un último envío de correo malicioso, el cual contenía indicadores de phishing y presentaba una oferta atractiva para lograr que los usuarios ingresaran sus datos personales en la página especialmente creada para la captura de datos.

ILUSTRACIÓN 49 CORREO MALICIOSO CAMPAÑA FINAL

10.2. Resultados de las Pruebas

Tras la realización de los dos procesos de concientización y test se obtuvo los siguientes datos:

10.2.1. Resultados Campaña inicial

Tras la realización de la primera campaña y envío de correo falso se obtuvieron los siguientes datos:

- 74% de los usuarios abrieron el correo fraudulento

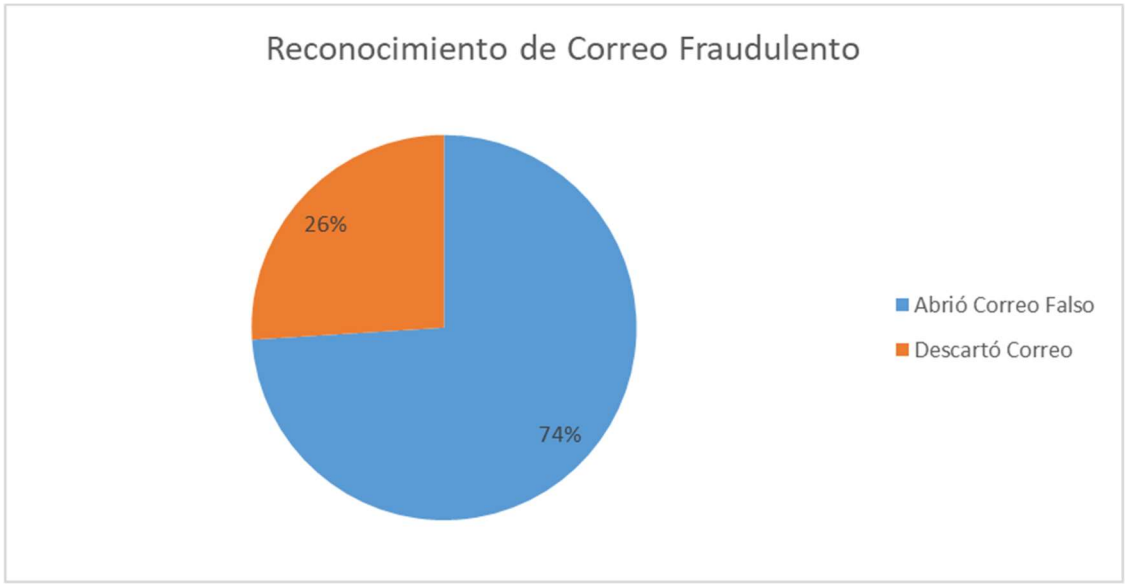


ILUSTRACIÓN 50 PORCENTAJE DE CORREOS ABIERTOS EN CAMPAÑA INICIAL

Del total de personas que abrieron el correo falso, un 39% ingresó datos personales. Lo cual se indica que hubo 29 eventos de seguridad

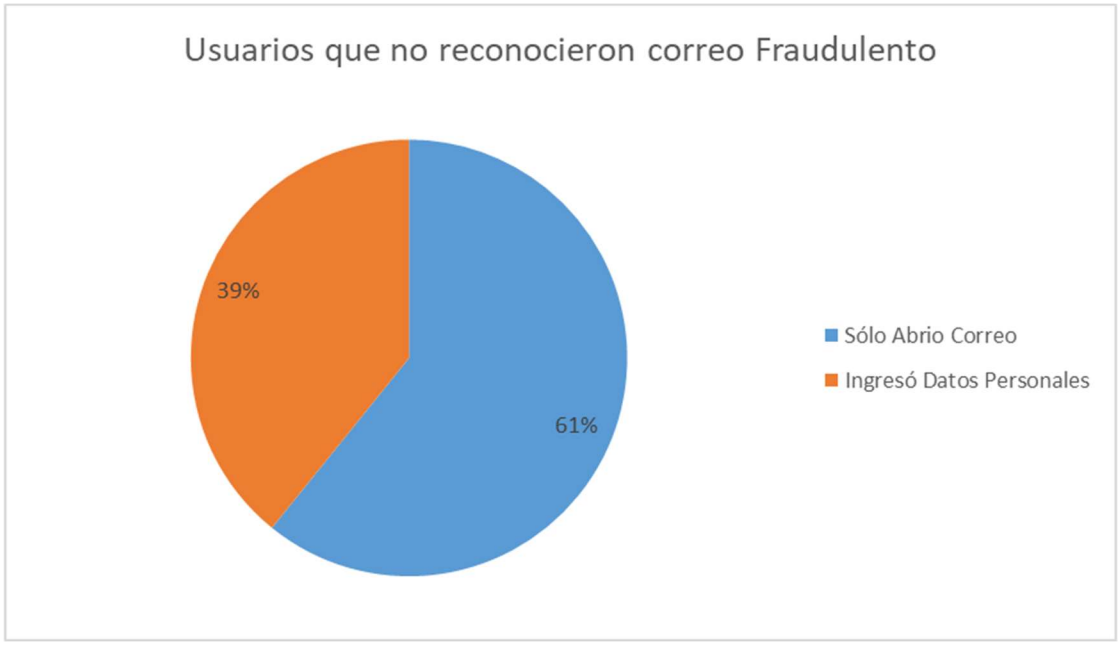
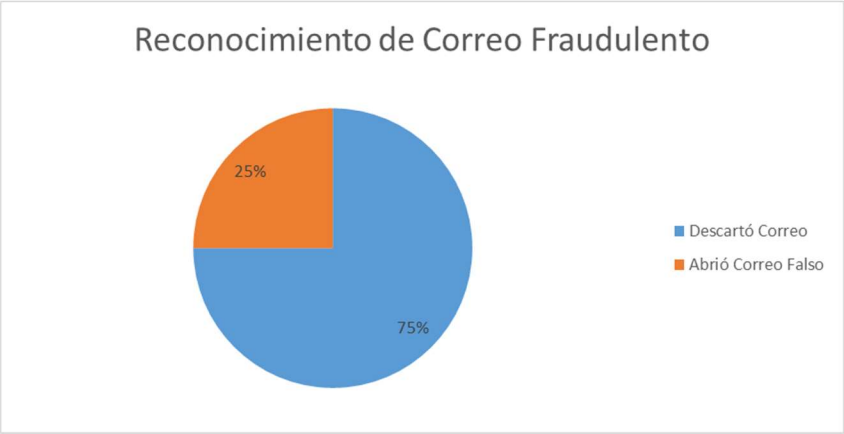


ILUSTRACIÓN 51 USUARIOS QUE INGRESARON DATOS PERSONALES

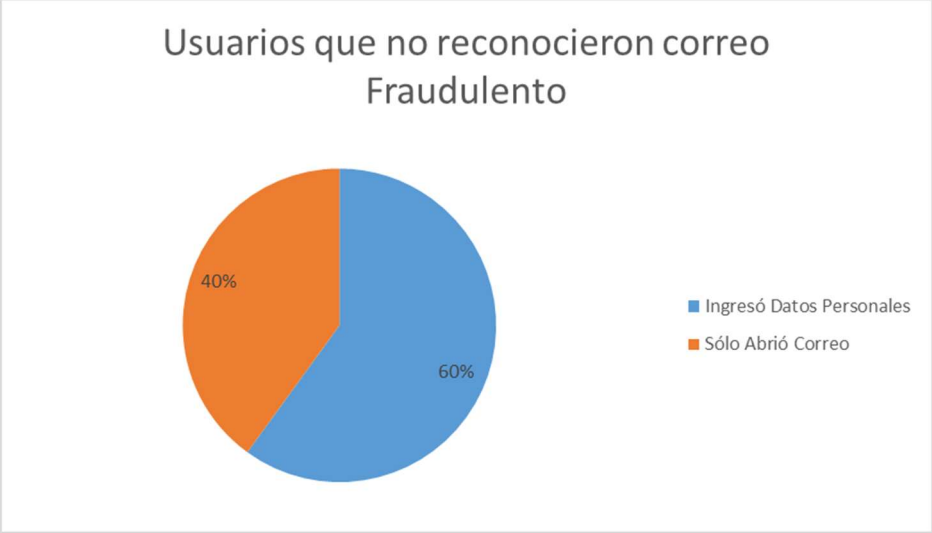
10.2.2. Resultados Campaña Final

Posteriormente tras realizar una campaña de concientización con contenidos más cercanos a las personas de la muestra, se obtuvieron los siguientes indicadores.

- El número de usuarios que abrieron el correo fraudulento disminuyó a un 25%



Del total de personas que abrieron el correo falso, un 60% ingresó datos personales. Lo cual se indica que hubo sólo 15 eventos de seguridad.



11. RESULTADOS OBTENIDOS

Luego de realizar las pruebas de Simulación de la solución y proyectar una plataforma distribuida en 2 datacenters con Backup hacia la nube es posible analizar el cumplimiento de los objetivos específicos planteados en la sección 5.2 y que se detallan a continuación:

- OE1 Disminuir la Alta tasa de Desconocimiento de información
- OE2 Disminuir la Alta tasa de Incidentes
- OE3 Disminuir los Altos costos de Implementación

11.1. Validación de Objetivo Especifico OE01

Tal como se define en Tabla 4, el OE01 busca disminuir la alta tasa de Desconocimiento de información. Con las primeras pruebas de Phishing realizadas, se envió a un total de 100 usuarios. De estos, el 74% abrió el correo, de los cuales 29 usuarios cayeron en el ataque simulado ingresando datos personales y fueron derivados al sitio de aprendizaje para realizar una concientización express.

Al realizar una nueva simulación enviada a los mismos 100 usuarios el correo esta vez fue abierto por el 25% y solo 15 cayeron en el ataque simulado.

Dado lo anterior podemos validar que se cumple el Objetivo específico que disminuir a la alta tasa de desconocimiento de la información y los usuarios con relación a los ataques, ya que los usuarios fueron capaces de distinguir el correo malicioso y descartarlo sin abrirlo, lo cual demuestra que existió un proceso de aprendizaje

11.2. Validación de Objetivo Especifico OE02

Tal como se define en Tabla N°4, el OE02 busca disminuir la alta tasa de Incidentes. Al igual que el punto anterior podemos evidenciar que en las pruebas iniciales y finales de Phishing realizadas, a los 100 usuarios seleccionados aleatoriamente tenemos el siguiente resultado:

Campaña Inicial:

74% abrió el correo, de los cuales 29 usuarios cayeron en el ataque simulado ingresando datos personales y fueron derivados al sitio de aprendizaje para realizar una concientización express.

Campaña Final:

Al realizar una nueva simulación enviada a los mismos 100 usuarios el correo esta vez fue abierto por el 25% y solo 15 cayeron en el ataque simulado.

Dado lo anterior podemos validar que se cumple el Objetivo específico que busca Disminuir la Alta tasa de Incidentes con relación a los ataques simulados. Si consideramos que cualquier correo electrónico abierto es un posible vector de ataque a la seguridad de la empresa y por lo tanto un posible incidente de seguridad, podemos indicar que se cumple el Objetivo de bajar la tasa de incidentes.

11.3. Validación de Objetivo Especifico OE03

Tal como se define en Tabla N°4, el OE03 busca disminuir los altos costos de Implementación, lo que se logra sin problemas dado que para la Implementación de la solución hemos considerado la utilización de un servicio de nube hibrida con modelo de pago por uso, que plantea pagar solo lo que se consume en forma mensual, lo que nos permite ir captando clientes para ir cubriendo estos costos mensuales.

Podemos apreciar que el costo inicial mensual requerido para mantener en operación toda la solución bordea los USD$ 28.000 siendo que en un sistema tradicional de compra con inversión inicial necesitaríamos al sobre USD 1.600.000 Aprox solo en Hardware y Software de la solución.

En cuanto a las empresas que contraten los servicios de nuestra plataforma PCCSI pagaran USD$ 24 por usuario anual y quedaran con un servicio de concientización de calidad y con alta disponibilidad a un costo muy bajo versus implementar una solución como nuestra plataforma PCCSI.

12. CONCLUSIONES

En la actualidad nuestro país no cuenta con ninguna empresa especialista y dedicada a este tipo de servicios con contenido local, sino que actúan como canales comerciales de las plataformas internacionales existentes en el mercado, esto nos abre una puerta para posicionar la marca a nivel nacional con temas de concientización de usuarios.

El estudio de mercado nos permitió reforzar que la gran mayoría de los usuarios consideran que la seguridad de la información y capacitar a los usuarios es clave para bajar las incidencias de seguridad, pero hay un desconocimiento general en cuanto a los valores de este tipo de soluciones o el presupuesto que destinan sus empresas para cubrir esta brecha de seguridad de la información que sin duda como se repite en esta tesis cada día se confirma más que el usuario es el eslabón más débil (Mitnick & Simón, 2005).

El hecho de mantener un modelo de gastos de pago por uso nos permitirá ir creciendo según la demanda que se requiera en la medida que se van sumando nuevos usuarios.

Las pruebas realizadas de envío de phishing en un entorno real confirman que, tras un periodo de concientización estándar sin contenidos personalizados, si bien logró bajar la cantidad de incidentes de seguridad, el número de correos abiertos y datos ingresados fue el suficiente para causar un potencial daño tanto económico como reputacional a la empresa. Tras realizar una campaña de concientización con contenidos locales y cercanos a los usuarios, la tasa se redujo desde un 74% hasta un 25% lo cual se considera exitoso. Es necesario indicar que el proceso de concientización debe ser mantenido en el tiempo y reforzado constantemente para obtener mejores resultados y que estos sean consistentes en el tiempo ya que la forma de atacar o engañar a los usuarios evolucionan constantemente, por este motivo se requiere una plataforma que actualice sus contenidos, permita educar y finalmente testear el éxito de las campañas.

Finalmente podemos concluir que utilizando la Plataforma Chilena de Concientización de Seguridad de la Información - PCCSI que hemos presentado en esta Tesis, todas las empresas que se suscriban al servicio ofertado podrían aumentar el conocimiento de sus usuarios en temas de seguridad de la información, lo cual les permitirá bajar en un alto porcentaje los incidentes de seguridad a un bajo costo, por lo tanto, se valida la hipótesis planteada.

ILUSTRACIÓN 52 LOGO PROPUESTO PARA PCCSI

13. BIBLIOGRAFÍA

HPE D3940 . (2021). Obtenido de https://h20195.www2.hpe.com/v2/GetPDF.aspx/c04815141.pdf

Katie Lenahan. (2018). Obtenido de https://community.hpe.com/t5/Alliances/HPE-GreenLake-Hybrid-Cloud-with-Azure-Stack-implement-operate/ba-p/7019259#.YBYsc-hKiUk

Ackoff, R. L. (1967). *Management Misinformation Systems. Management Sciences, Vol. 14, No. 4.*

Asociación Española de Normalización. (2016). *ISO/IEC 27000:2016 VIsión de Conjunto y Vocabulario.* Madrid: Aeonor Internacional S.A.U.

Bacian, G. F. (2020). *Ransomware: del acceso inicial al compromiso de la red.* Santiago: CSRIT.

Budge, J., & O'Malley, C. (2020). *The Forrester Wave™: Security Awareness And Training Solutions.* The Forrester.

Daniel Newman. (Enero de 2020). Obtenido de https://assets.ext.hpe.com/is/content/hpedam/documents/a00095000-5999/a00095228/a00095228ese.pdf

Eds, R. G. (2005). *Social work: Research and evaluation.* New York, NY, EE.UU: Oxford University.

Equipo de Respuesta ante Incidentes de Seguridad informática. (s.f.). *Boletín de Seguridad Cibernética*. Obtenido de https://www.csirt.gob.cl: https://www.csirt.gob.cl

Fortinet. (Q1-2020). *Fortinet Threat Intelligence Insider Latin America para el primer trimestre de 2020*. Obtenido de https://www.fortinetthreatinsiderlat.com/es/Q1-2020/landing

HCI Simplivity, HPE. (s.f.). *HCI Simplivity*. Obtenido de www.hpe.com: https://www.hpe.com/lamerica/es/integrated-systems/simplivity.html

Hernández R., &. F. (2010). *Metodología de la Investigación (5ta. Edición).* Mexico: Ed. Mc Graw Hill.

Hernández Sampieri, R. y. (2009). *Marco teórico.* Guanajuato, México: Universidad de Celaya.

HPE GreenLake. (2021). Obtenido de https://www.hpe.com/lamerica/es/greenlake.html

HPE GreenLake. (s.f.). *GreenLake*. Obtenido de https://www.hpe.com/es/es/greenlake.html

HPE Primera. (2021). *HPE Primera*. Obtenido de https://www.hpe.com/lamerica/es/storage/hpe-primera.html

HPE SG 480 . (2020). Obtenido de https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=a00008520enw

HPE SN3600B. (2020). *Datasheet HPE B-series SN3600B Fibre Channel Switch*. Obtenido de https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=a00000578enw

HPE SYNERGY. (2021). Obtenido de https://www.hpe.com/lamerica/es/integrated-systems/synergy.html

IBM.com. (abril de 2020). *IBM X-Force Threat Intelligence Index*. Obtenido de ibm.com/downloads/cas/DEDOLR3W

Instituto Nacional de Ciberseguridad de España (INCIBE). (16 de 01 de 2020). Obtenido de https://www.incibe.es: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

Instituto Nacional de Ciberseguridad Español. (s.f.). *www.incibe.es*. Obtenido de https://www.incibe.es/protege-tu-empresa/kit-concienciacion

ISO/IEC 27001:2013(E). (2013). *Information technology — Security techniques — Information security management systems — Requirements*.

Jazdzewski, S., & Jazdzewski, C. (Enero de 1995). *The JArgon Files*. Obtenido de http://www.jargon.net/

Kaspersky Labs. (2019). *https://www.kaspersky.com/enterprise-security/security-awareness*. Obtenido de https://media.kaspersky.com/en/business-security/enterprise/cyber-security-awareness-training-whitepaper.pdf

kepler. (s.f.). *https://kepler.cl/producto/concientizacion-en-ciberseguridad/*. Obtenido de https://kepler.cl/producto/concientizacion-en-ciberseguridad/.

Krugera, H., & Kearney, W. (2006, junio). A prototype for assessing information security awareness. (E. H. Spafford, Ed.) *Computers & Security*, 289-296.

Microsoft. (2019). Curso Oficial AZ900. https://bit.ly/az900-training.

Microsoft Azure - Container. (2020). *Microsoft Azure - Container*. Obtenido de https://azure.microsoft.com/es-es/overview/what-is-a-container/

Microsoft Azure - Serverless. (2020). Obtenido de https://azure.microsoft.com/es-es/solutions/serverless/

Microsoft Azure - VMS. (2020). *Virtial Machines*. Obtenido de https://azure.microsoft.com/es-es/services/virtual-machines/

Microsoft. (s.f.). *Microsoft Digital Defense Report*. Obtenido de https://www.microsoft.com/en-us/security/business/security-intelligence-report

Ministerio de Economía Fomento y Turismo. (octubre de 2015). *www.economia.gob.cl*. Obtenido de https://www.economia.gob.cl/wp-content/uploads/2015/10/Informe-de-resultados-TIC-en-las-empresas.pdf

Mitnick, K. D., & Simón, W. L. (2005). *El Arte de la Intrusion.* Wiley Publishing inc.

Najar Pacheco, J. C., & Suárez Suárez, N. E. (2015). .La seguridad de la información: un activo valioso de la organización. *Revista Vínculos, 12(1), 89-97.*

Oznet. (s.f.). *https://oznet.cl/ciberseguridad-defensiva/concientizacion-de-seguridad*. Obtenido de https://oznet.cl/ciberseguridad-defensiva/concientizacion-de-seguridad.

PCI DSS GUIDE. (s.f.). *PCI DSS GUIDE*. Obtenido de https://www.pcidssguide.com/pci-dss-requirement-12/

privacy-regulation.eu. (s.f.). *EU General Data Protection Regulation*. Obtenido de https://www.privacy-regulation.eu/en/article-47-binding-corporate-rules-GDPR.htm

Rojas Soriano, R. (2002). *Guía para realizar investigaciones sociales 34ª Ed.* México: Plaza y Valdés.

Selltiz, J. D. (1980). *Métodos de investigación en las relaciones sociales.* Madrid: Rialp.

Servicio de Impuestos Internos. (Septiembre de 2019). *SII.cl*. Obtenido de http://www.sii.cl/sobre_el_sii/estadisticas_de_empresas.html

Stega. (s.f.). *https://www.stega.cl/smartfense*. Obtenido de https://www.stega.cl/smartfense.

The Register. (12 de 2016). *https://www.theregister.com.* Obtenido de https://www.theregister.com/2016/12/21/ukraine_electricity_outage/

Thomson, W. (1952). *https://es.wikipedia.org/wiki/William_Thomson*.

Veeam B&R. (2021). Obtenido de https://www.veeam.com/es/vm-backup-recovery-replication-software.html

VMCloudFdtn. (2021). *Vmware Cloud Foundation*. Obtenido de https://www.vmware.com/cl/products/cloud-foundation.html

vSAN, V. (2021). *https://www.vmware.com/cl/products/vsan.html*. Obtenido de VMvware.

Wasabi. (2021). *Wasabi Technologies, Inc.* Obtenido de https://wasabi.com/cloud-storage-pricing/#three-info

Wikipedia. (02 de Agosto de 2019). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/PCI_DSS

Wikipedia.org. (s.f.). *Wikipedia.org*. Obtenido de https://es.wikipedia.org/wiki/Estafa_nigeriana

www.sii.cl. (2019). *Servicio de Impuestos Internos*. Obtenido de http://www.sii.cl/sobre_el_sii/estadisticas_de_empresas.html

14. ANEXOS

14.1. DNS y NIC Chile

Para la implementación de un mockup de pccsi.cl se adquirió el dominio en Nic chile

pccsi.cl	
Titular:	Computación e Ingeniería S. A.
Agente Registrador:	NIC Chile
Fecha de creación:	2020-08-06 20:11:05 CLT
Fecha de última modificación:	2020-08-06 20:16:31 CLT
Fecha de expiración:	2021-08-06 20:11:05 CLT
Servidor de Nombre:	ns1-07.azure-dns.com
Servidor de Nombre:	ns2-07.azure-dns.net
Servidor de Nombre:	ns3-07.azure-dns.org
Servidor de Nombre:	ns4-07.azure-dns.info

ILUSTRACIÓN 53 DOMINIO ADQUIRIDO EN NIC CHILE

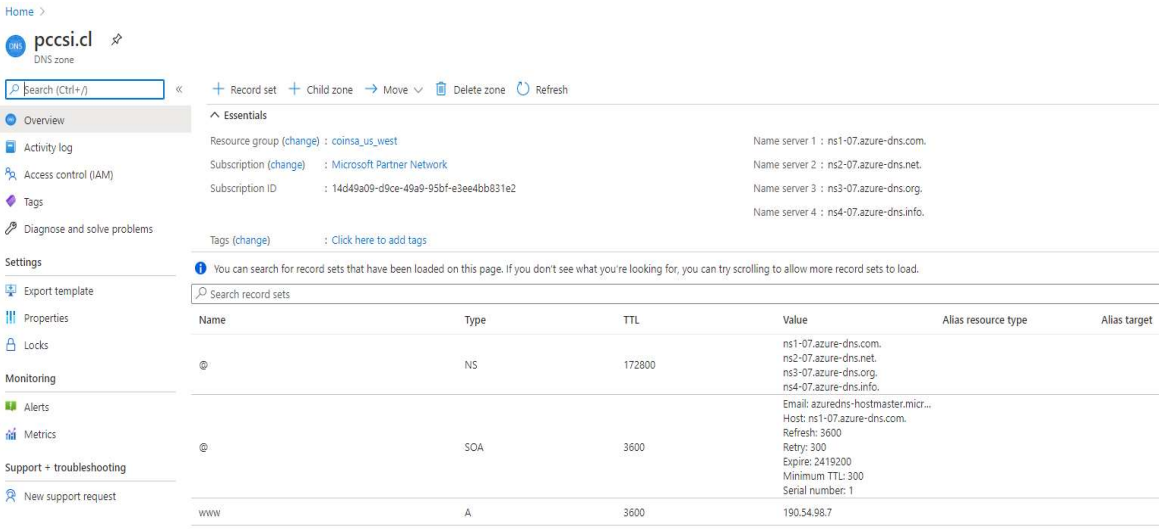


ILUSTRACIÓN 54 CONFIGURACIÓN DE DNS DE PCCSI.CL

14.1. Página WEB PCCSI

Para la elaboración del mockup se estableció una propuesta digital inicial que permitiese modelar la plataforma a nivel de diseño

www.pccsi.cl

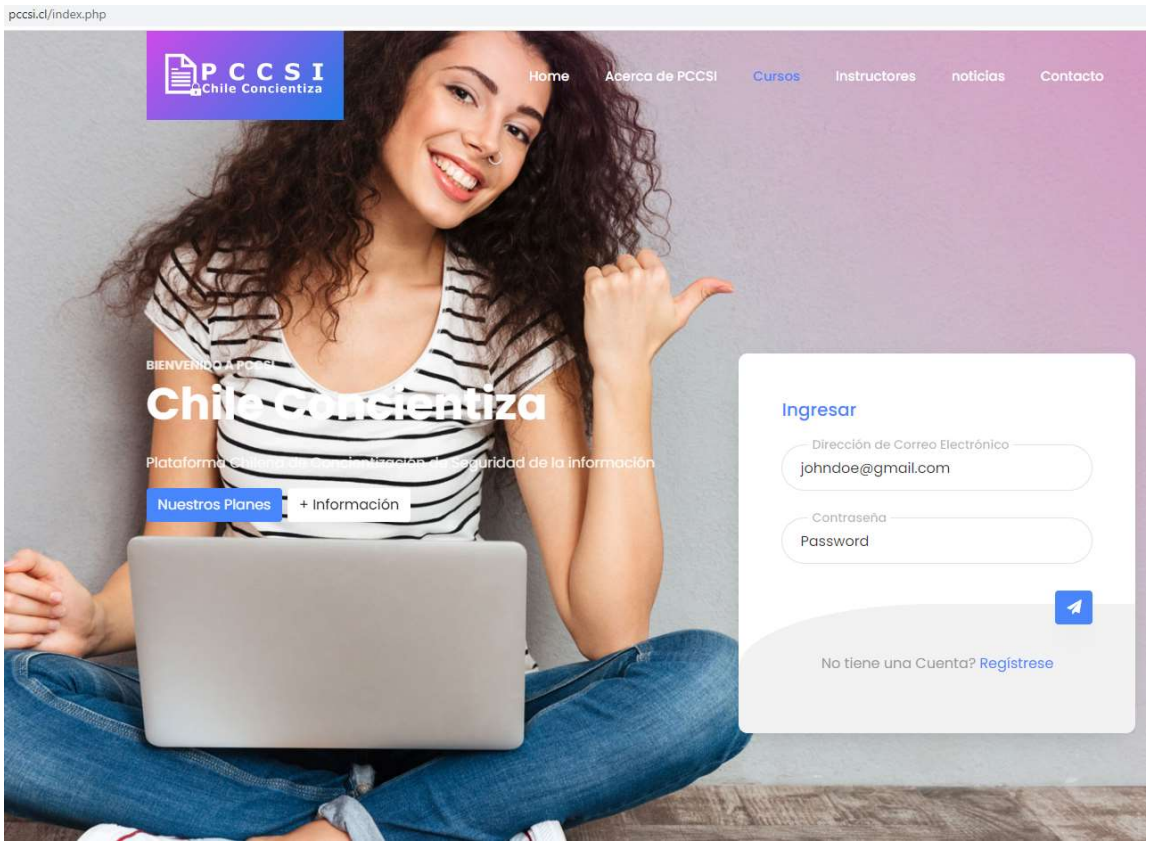


ILUSTRACIÓN 55 SITIO WEB INICIAL PCCSI.CL