

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



“DISEÑO CENTRADO EN USUARIAS DE POLÍTICAS Y MECANISMOS DE CIBERSEGURIDAD”

GABRIELA ALEJANDRA SEPÚLVEDA BRAVO

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: *Claudia López Moncada*
Profesor Correferente: *Víctor Codocedo Henríquez*
Profesor Correferente: *Paulina Santander Astorga*

Septiembre - 2021

DEDICATORIA

A mis padres, pareja y familia por todo su apoyo incondicional.
Y a todas las niñas que sueñan con hacer su carrera en las tecnologías de información, en especial la Ciberseguridad. No dejen que nadie les diga lo que pueden o no pueden hacer, solo ustedes sabrán cual es su límite.

AGRADECIMIENTOS

A mis padres, Magaly y Roberto, por haberme dado durante toda mi vida todas las condiciones y herramientas necesarias para llegar a convertirme en lo que soy hoy. Esta memoria culmina una etapa de mi vida que fue posible gracias a ustedes.

A mi pareja, Michelle, quien fue la persona que me dio el empujón necesario para entrar a la Ciberseguridad. Porque ha estado junto a mi durante todos estos años apoyándome y dándome fuerzas y amor cuando más lo necesité.

A la UTFSM por convertirse en mi casa de estudios y ser el lugar en donde me encontré a mi misma. Identificarme como sansana es una de las cosas de las que mas me siento orgullosa en esta vida.

Al DI por ver en mi un persona con potencial y apoyarme así en todos los aspectos relacionados a mi carrera profesional. Pero en especial, a las docentes del departamento, quienes durante todos estos años me han inspirado y demostrado que la mujer tiene un lugar en la informática.

Gracias totales.

RESUMEN

Resumen— Los últimos acontecimientos vividos por nuestra sociedad han acelerado la llamada transformación digital, y con ello la necesidad de proteger el activo más importante de las organizaciones: la información. Frente a lo anterior, las políticas y mecanismos de ciberseguridad son ampliamente utilizados con el fin de proteger estos activo, pero a pesar de la gran cantidad de *frameworks* que existen para implementarlos, no siempre se suelen adaptar a las necesidades de los y las usuarias. Esta memoria buscó romper con esta problemática diseñando políticas y mecanismos de ciberseguridad para la plataforma Aliadas, centrándose en las necesidades de las usuarias de ella, por medio de distintas actividades englobadas en el marco del DCU. Esto permitió construir políticas y mecanismos que consideraron aspectos que usualmente se podrían por alto y que suelen repercutir en la seguridad de las usuarias dentro de plataformas digitales.

Palabras Clave— Ciberseguridad, Diseño Centrado en Personas; Políticas de Ciberseguridad; Mecanismos de Ciberseguridad; Ciberseguridad Feminista

ABSTRACT

Abstract— Recent events in our society have accelerated the so-called digital transformation and with it the need to protect the most important asset of organizations: information. Given the above, cybersecurity policies and mechanisms are widely used to protect these assets, but despite the large number of frameworks that exist to implement them, they are not always adapted to the needs of users. This report tried to break up this problem by designing cybersecurity policies and mechanisms for the Aliadas platform, focusing on the needs of its users, through different activities within the framework of the UCD. This allowed the construction of policies and mechanisms that considered aspects that are usually overlooked and that usually have an impact on the security of users on digital platforms.

Keywords— *Cybersecurity; Human-Centered Design; Cybersecurity Policies; Cybersecurity Mechanisms, Feminist Cybersecurity*

GLOSARIO

ANID: Agencia Nacional de Investigación y Desarrollo de Chile

Activo: Recurso(hardware o software) con el que cuenta una organización o empresa

DCU: Diseño Centrado en Usuarios

DI: Departamento de Informática

NIST: *National Institute of Standards and Technology*

OEA: Organización de los Estados Americanos

OWASP: *Open Web Application Security Project*

RGDP: Reglamento General de Protección de Datos

RSA: *Rivest, Shamir y Adleman*

SI: Seguridad de la Información

SGSI: Sistema de Gestión de la Seguridad de la Información

SSH: *Secure Shell*

TD: Transformación Digital

TI: Tecnologías de Información

TIC: Tecnologías de la Información y Comunicación

UE: Unión Europea

UTFSM: Universidad Técnica Federico Santa María

WAF: *Web application firewall*

ÍNDICE DE CONTENIDOS

RESUMEN	IV
ABSTRACT	IV
GLOSARIO	V
ÍNDICE DE FIGURAS	VIII
ÍNDICE DE TABLAS	IX
INTRODUCCIÓN	1
CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA Y OBJETIVOS	2
1.1 DEFINICIÓN DEL PROBLEMA	2
1.1.1 CONTEXTO	2
1.1.2 DEFINICIÓN DEL PROBLEMA	5
1.2 OBJETIVOS	7
1.2.1 OBJETIVO GENERAL	7
1.2.2 OBJETIVOS ESPECÍFICOS	7
CAPÍTULO 2: MARCO CONCEPTUAL	9
2.1 DISEÑO CENTRADO EN USUARIAS	9
2.1.1 ETAPAS EN EL DCU	9
2.1.2 MÉTODOS EN EL DCU	10
2.2 CIBERSEGURIDAD	11
2.2.1 DEFINICIÓN DE CIBERSEGURIDAD	12
2.2.2 TRIADA CID DE LA INFORMACIÓN	13
2.2.3 FRAMEWORKS DE CIBERSEGURIDAD	14
2.2.3.1 Framework de NIST	15
2.2.3.2 ISO 27001	17
2.2.3.3 CIS	18
2.3 CIBERSEGURIDAD EN CHILE	19
2.3.1 ESTRATEGIA CHILENA DE CIBERSEGURIDAD	20
2.3.1.1 LEY DEL CIBRECRIMEN O DELITOS INFORMÁTICOS	21
2.3.1.2 LEY DE PROTECCIÓN DE DATOS	22
2.3.2 CAMBIOS DE LA CIBERSEGURIDAD EN CHILE ENTRE 2016 Y 2020	23
2.4 POLÍTICAS DE CIBERSEGURIDAD	27
2.4.1 RESPONSABLES EN LA POLÍTICA DE CIBERSEGURIDAD	28
2.4.2 CICLO DE UNA POLÍTICA DE CIBERSEGURIDAD	28
2.4.3 POLÍTICAS DE PRIVACIDAD	29
2.4.3.1 INNOVACIÓN EN LAS POLÍTICAS DE PRIVACIDAD	30
2.5 MECANISMOS DE CIBERSEGURIDAD	31

2.6 CIBERSEGURIDAD FEMINISTA	32
CAPÍTULO 3: PROPUESTA DE SOLUCIÓN	36
3.1 EXPLORACIÓN	37
3.2 VINCULACIÓN	45
3.2.1 ANÁLISIS DEL RESULTADO DEL TALLER	45
3.2.2 TRANSPARENCIA EN LA INFORMACIÓN	50
3.3 DISEÑO	52
3.3.1 PROPUESTA DE POLÍTICAS DE CIBERSEGURIDAD	53
3.3.2 POLÍTICA DE CIBERSEGURIDAD	55
3.4 VALIDACIÓN	61
3.5 IMPLEMENTACIÓN	62
3.5.1 MECANISMOS DE CIBERSEGURIDAD EN ALIADAS	63
3.5.2 ESTRATEGIA DE CONCIENTIZACIÓN	64
CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN	67
4.1 VALIDACIÓN DE POLÍTICAS Y MECANISMOS DE CIBERSEGURIDAD	67
4.2 VALIDACIÓN DE ESTRATEGIA DE CONCIENTIZACIÓN	69
CAPÍTULO 5: CONCLUSIONES	71
5.1 DISCUSIÓN FINAL	74
ANEXOS	76
5.1 ANEXO A: Política de Ciberseguridad de Aliadas	76
5.2 ANEXO B: Política de control de accesos de Aliadas	80
5.3 ANEXO C: Política de control de accesos con privilegios de Aliadas	82
5.4 ANEXO D: Política de gestión de credenciales y contraseñas de Aliadas	84
5.5 ANEXO E: Borrador de Política de gestión de y parcheo de vulnerabilidades de Aliadas	86
5.6 ANEXO F: Política de privacidad de Aliadass	88
REFERENCIAS BIBLIOGRÁFICAS	94

ÍNDICE DE FIGURAS

1	Mapa de Stakeholders.	7
2	Etapas claves del DCU.	10
3	Métodos utilizados en las etapas claves del DCU.	12
4	Triada CID.	14
5	Etapas en el <i>framework</i> de ciberseguridad de NIST y sus categorías.	15
6	Relación entre los elementos del <i>framework</i> de ciberseguridad de NIST.	17
7	Categorización de los 20 controles de CIS.	19
8	Políticas y Estrategias Cibernéticas en Chile.	25
9	Cultura Cibernética y Sociedad en Chile.	25
10	Formación, Capacitación y Habilidades de Seguridad Cibernética en Chile.	26
11	Marcos Legales y Regulatorios en Chile.	26
12	Estándares, Organizaciones y Tecnologías en Chile.	27
13	Ciclo de una política.	29
14	Evolución de resultados en el proceso de diseño iterativo.	31
15	Etapas asociadas al diseño cíclico de políticas y mecanismos de ciberseguridad en la aplicación Aliadas.	37
16	Panel en Miro para el taller de 'Modelamiento de amenazas'.	39
17	<i>Dashboard</i> en Miró durante el taller de 'Modelamiento de amenazas' con el gremio de AGEP-V	40
18	Resultados de AGEP-V ((<i>izquierda</i>) y 'Tejiendo Redes' (<i>derecha</i>) para pregunta 1 en taller de 'Modelamiento de amenazas'.	41
19	Resultados de AGEP-V ((<i>izquierda</i>) y 'Tejiendo Redes' (<i>derecha</i>) para pregunta 2 en taller de 'Modelamiento de amenazas'.	41
20	Resultados de AGEP-V ((<i>izquierda</i>) y 'Tejiendo Redes' (<i>derecha</i>) para pregunta 3 en taller de 'Modelamiento de amenazas'.	42

21 Resultados de AGEV-V ((<i>izquierda</i>) y ' <i>Tejiendo Redes</i> ' (<i>derecha</i>) no clasificados en taller de ' <i>Modelamiento de amenazas</i> '.	42
22 Representación gráfica para abordar las preguntas a) ¿Cómo podemos recordar contraseñas? y b) ¿Cómo hacer una contraseña segura?.	43
23 Representación gráfica para abordar las preguntas a) ¿Cómo saber si mi contraseña es segura? y b) ¿Cómo saber si mis cuentas han sido hackeadas?.	44
24 Propuesta de clasificación para los <i>post-it</i>	45
25 <i>Clustering</i> de los <i>post-it</i>	46
26 Resultados del <i>clustering</i> de ' <i>Datos</i> ' y etiquetado de ellos.	47
27 Resultados del <i>clustering</i> de ' <i>Vida Digital</i> ' y ' <i>Otros temas</i> ', y etiquetado de ellos.	48
28 <i>Creative matrix</i> realizado una vez concluido el análisis de los resultados del taller.	49
29 Lluvia de ideas sobre los tres pilares en las ' <i>Políticas de privacidad</i> '.	52
30 Diagrama de la organización de las " <i>Políticas de ciberseguridad de Aliadas</i> ".	54
31 Aspecto en la aplicación de las políticas de privacidad en la aplicación Aliadas.	61
32 Capturas de la presentación de las políticas de ciberseguridad de Aliadas realizada en Mayo 2021.	62
33 Capturas de las publicaciones de la estrategia de concientización (Parte I)	65
34 Capturas de las publicaciones de la estrategia de concientización (Parte II).	66
35 (a) Origen de políticas de ciberseguridad de Aliadas y (b) elección de mecanismo de ciberseguridad	69
36 Gráfico de cantidad de <i>likes</i> por publicación	70

ÍNDICE DE TABLAS

1 Stakeholders del Problema.	6
2 Madurez de la Capacidad de Ciberseguridad.	24
3 Políticas de ciberseguridad de Aliadas.	54

INTRODUCCIÓN

Hoy en día es casi imposible pensar en ámbitos en donde no se encuentren implementadas las Tecnologías de la Información y Comunicación (TIC) ¹ y es que además, producto de los diferentes acontecimientos que se han vivido como sociedad durante los últimos años, hemos podido ser testigos del auge que ha tenido la llamada Transformación Digital (TD). ² Esto se ha traducido en que actualmente nuestra sociedad esté fuertemente relacionada a las TIC, estando presentes en el día a día de millones de personas.

Es justamente bajo este contexto social de la TD en el que se han visto envueltas cientos de mujeres, quienes ven en el micro-emprendimiento una oportunidad económica para mejorar las situaciones sociales, educativas y sanitarias de ellas mismas y sus familias. Lamentablemente en nuestro país, las cifras que contrastan tanto cantidad como ingresos de los micro-emprendimientos liderados por mujeres versus los liderados por hombres, resultan mucho mas favorecedores para estos últimos, trayendo como consecuencia que las mujeres estén mas propensas al fracaso. Esta situación brinda la oportunidad de construir una solución a través de una plataforma social de mercado digital, cuyo propósito radica en apoyar a micro-emprendedoras, en una primera instancia de la región de Valparaíso, en el proceso de TD de sus micro-emprendimientos y crecimiento de ellos.

Hace sentido entonces afirmar que en la actualidad el uso de las TIC para potenciar los emprendimientos, ha tenido una gran demanda dado la necesidad de las personas por buscar y adquirir productos de forma fácil y eficiente desde la comodidad de sus *smartphones*. Pero el aumento del uso de las tecnologías, trae también como consecuencia un aumento en los problemas de seguridad de éstas, afectando a activos esenciales como la información. Es necesario entonces que las TIC estén desarrolladas desde una perspectiva de conciencia sobre la importancia de proteger los datos que se manejan en ellas.

Siendo entonces las TIC una base importante de la plataforma digital que será desarrollada, se hace indispensable buscar la forma de proteger los activos de información que se manejan en ella. La manera tradicional de abordar este punto es elaborando un plan que contemple las políticas y mecanismos de ciberseguridad necesarios para proteger todos estos activos. Pero resulta interesante dar cuenta de que muchas veces estas políticas se elaboran en base a estándares o *frameworks* muy genéricos que no se adecuan del todo a las necesidades reales de los proyectos, o incluso los mecanismos que usualmente son implementados por defecto, terminan resultando engorrosos para los usuarios. Lo que propone esta memoria es diseñar e implementar un plan que comprenda políticas y mecanismos de ciberseguridad centrándose en las necesidades tanto de las usuarias como las del equipo de desarrollo del proyecto.

¹Conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro.

²Aplicación de capacidades digitales a procesos, productos y activos para mejorar la eficiencia, mejorar el valor para el cliente, gestionar el riesgo y descubrir nuevas oportunidades de generación de ingresos.

CAPÍTULO 1

DEFINICIÓN DEL PROBLEMA Y OBJETIVOS

1.1. DEFINICIÓN DEL PROBLEMA

1.1.1. CONTEXTO

La Transformación Digital (TD) ha brindado la posibilidad de otorgarle a la sociedad una mejora en las Tecnologías de la Información y Comunicación (TIC), implicando un aumento en los avances tecnológicos. Esta transformación se ha visto fuertemente acelerada por el acontecer actual que se vive, y es que la *Pandemia de COVID-19*³ ha obligado a reducir los aforos de las distintas localidades a nivel mundial. Esto ha traído como consecuencia la necesidad de buscar formas de digitalizar los distintos procesos que se realizaban antes de manera presencial.

La situación actual ha impulsado a que cientos de mujeres vean en el emprendimiento, tal como dice [Giner, 2020], una oportunidad (frente a la necesidad) de mejorar la calidad de vida de ellas y sus familias. Tal como se mencionó en la introducción, esta situación abre la oportunidad de construir una plataforma social de mercado digital, que les permita a las micro-emprendedoras realizar una TD de sus emprendimientos. En específico, esta oportunidad es abordada en el proyecto ANID-COVID, que bajo el apoyo de ANID y la UTFSM han logrado el desarrollo de la plataforma Aliadas,⁴ la cual busca no solo impulsar los emprendimientos de mujeres, sino que también incentivar la colaboración entre ellas.

Pero tal como menciona [D'Antonio y Olías de Lima, 2019], la TD conlleva una serie de nuevos riesgos que tienen un impacto mayor a los que tradicionalmente se conocen. Estos riesgos podrían causar una serie de situaciones negativas que los autores han decidido llamar *Digital Chaos* (caos digital), y el énfasis lo ponen en que éste debe ser abordado desde una perspectiva de redefinición de la ciberseguridad, ya que esta tal y como la entendemos hoy en día, no es capaz de abordar las necesidades de seguridad que implican este paradigma de TD.

Hemos visto como a lo largo de los años se han introducido distintos tipos de procedimientos y controles de seguridad que buscan garantizar que toda la información sensible esté dentro de un sistema que sea capaz de protegerla, asegurando los tres pilares fundamentales de la información: confidencialidad, integridad y disponibilidad [Dhillon y Backhouse, 2001]. Estos tres pilares en su conjunto forman lo que se conoce como triada CID, la cuál será discutida en

³La pandemia de COVID-19 es una pandemia derivada de la enfermedad por coronavirus 2019 (COVID-19), ocasionada por el virus SARS-CoV-2. La afectación de esta enfermedad infecciosa se ha dado a nivel mundial durante los años 2020 y 2021.

⁴Más información en <https://aliad.as>

mayor detalle en el siguiente capítulo. La forma de aplicar estos procedimientos y controles es mediante la utilización de una serie de directrices que buscan minimizar el riesgo mencionado anteriormente. Es aquí donde surgen los mecanismos y políticas de ciberseguridad, las que dan las directrices para aplicar los procedimientos y controles, respectivamente. El desafío está entonces en comprender como enfocar estas directrices en pos de abordar las necesidades de seguridad que trae la TD.

Sumado a lo anterior, en el ámbito del desarrollo de software hemos visto como con el pasar de los años se ha adquirido la conciencia de que el tiempo utilizado en la calidad de software no es tiempo perdido, sino más bien una inversión a futuro. Lamentablemente, si bien hemos sido testigos de cómo los aspectos de ciberseguridad han ido ganando año a año la importancia que se merecen, aún hay cierta resistencia a considerarla como uno de los pilares de un desarrollo exitoso.

Bajo este último punto, para comprender bien la importancia que tiene la ciberseguridad en los desarrollos, se hace interesante conocer ciertas estadísticas a nivel mundial sobre ella y los riesgos relacionados [Sobers, 2020]:

- Las filtraciones de datos expusieron 4.100 millones de registros en la primera mitad de 2019.⁵ Si cada registro equivaliera a una persona, se podría decir que estos registros son equivalentes al 53 % de la población mundial.⁶
- El 52 % de las brechas fueron por hackeos, el 28 % relacionadas a malware y el 32-33 % al phishing o a la ingeniería social, respectivamente.⁷
- Las brechas de seguridad han aumentado un 11 % desde 2018 y 67 % desde 2014.⁸
- El 43 % de las víctimas de las brechas de datos son pequeñas empresas u organizaciones (de 1 a 50 empleados).⁹
- Para el 2021, los daños del cibercrimen le costarán al mundo 6 billones de dólares anuales.¹⁰ Esto corresponde aproximadamente al 17 % de lo que facturó la industria del software durante el 2020.¹¹

Estas cifras dan cuenta de como el aumento de las brechas de datos ha sido bastante explosivo, dando cuenta de lo importante que resulta la información de las empresas u organizaciones y/o los clientes o usuarios de ellas. Podría incluso predominar la tendencia de

⁵Recuperado en <https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report>

⁶Recuperado en <https://www.worldometers.info/es/poblacion-mundial>

⁷Recuperado en <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

⁸Recuperado en <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>

⁹Recuperado en <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

¹⁰Recuperado en <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

¹¹Recuperado en <https://forbes.co/2021/07/09/red-forbes/industria-del-software-un-sector-con-vision-de-crecimiento/>

pensar que los mayores objetivos de los ciberdelincuentes resultarían ser las grandes empresas, por los altos costos asociados, pero un porcentaje no menor de pequeñas empresas y/o organizaciones son víctima de estos ataques.

Además, en cuanto a las causas de las brechas de seguridad podemos dar cuenta de la importancia de por un lado desarrollar software de forma segura, y por otro lado de incentivar la concientización sobre la ciberseguridad a los desarrolladores y usuarios finales de estos desarrollos.

Cabe entonces preguntarse el por qué aún frente a un aumento de políticas y mecanismos de ciberseguridad, las estadísticas muestran que año a año los ataques aumentan y las consecuencias económicas crecen a billones de dólares al año a nivel mundial ¿En qué se está fallando? ¿Se están implementando estas medidas de forma correcta? ¿Se están enfocando en lo realmente necesario?

Sabemos que las principales políticas y mecanismos de ciberseguridad existentes están estandarizados y apuntan a transformar los software y/o organizaciones en verdaderas "Fortalezas Digitales", pero tal parece ser que algo está fallando. Esta memoria propone buscar una metodología que permita desarrollar e implementar políticas y mecanismos que se adapten a las necesidades del software que se desea desarrollar, tomando como hipótesis que centrarse en los usuarios de éste podría ser el enfoque necesario.

En el contexto del desarrollo de la plataforma social de mercado digital Aliadas, aparecen nuevos desafíos en torno a la ciberseguridad que resultan interesantes de abordar a lo largo de esta memoria, pero para poder comprender estos desafíos es necesario estar al tanto de los aspectos técnicos de la plataforma.

Aliadas es una aplicación móvil tanto para Android como iOS, desarrollada en *React Native*, con una arquitectura basada en microservicios (siendo *javascript* y *python* los principales lenguajes de programación utilizados en ellos). Esta arquitectura podría explicarse aludiendo a que la aplicación se construye a partir de pequeñas piezas de software que realizan un conjunto de tareas definidas, siendo cada una de estas piezas componentes autónomos. Si bien se despliegan de forma independiente, se comunican entre sí de tal manera que trabajan en conjunto para cumplir un objetivo específico.

En líneas generales, es relativamente sencillo establecer los límites de los microservicios (respecto a lo que pueden o no pueden hacer), pero dado que existe una fuerte comunicación entre ellos, se hace necesario una base sólida de confianza y planificación entre el desarrollo de las diferentes piezas. Lamentablemente en este aspecto, las consideraciones de seguridad se suelen pasar por alto, lo que conlleva a que fallas de seguridad en un microservicio repercutan en otro o incluso en el desarrollo completo.

Otro aspecto importante en el contexto del desarrollo de la plataforma son los y las usuarias finales de ella; y es que tal como se discutió en la sub-sección anterior, éstos están relacionados con los problemas de seguridad que puedan existir. En este punto cabe preguntarse

cuáles son las principales problemática que le preocupan a las usuarias ¿Es la seguridad de sus datos personales? ¿Es la reputación de su emprendimiento? ¿De qué manera podemos determinar estas preocupaciones?

Lo anterior es un punto interesante ya que muchas veces los mecanismos estandarizados de ciberseguridad que se implementan no se adecúan a las verdaderas necesidades de los usuarios. Por ejemplo, en una plataforma con usuarios que tienen poca alfabetización digital ¹² no tendrían sentido implementar un *login* que obligue al usuario a utilizar contraseñas complejas o los obligue a cambiarlas periódicamente; sino mas bien tendría sentido permitirle al usuario hacer un *logueo* desde un proveedor de identidades, como por ejemplo Google o Facebook, ya que esto les permitiría desde una única cuenta poder acceder a distintos servicios o sistemas.

Esto nos demuestra que no solo necesitamos enfocarnos en los aspectos técnicos de la plataforma que se desea desarrollar, como lo sería su arquitectura, sino que también es importante enfocarse en las interacciones humanas involucradas en ella.

1.1.2. DEFINICIÓN DEL PROBLEMA

Lo anterior lleva a realizar una definición más formal del problema que se desea abordar en esta memoria:

¿De qué manera podemos diseñar un modelo de políticas y mecanismos de ciberseguridad que busquen proteger la información y necesidades de las usuarias de Aliadas, y se adapte a la arquitectura del sistema que se desea implementar?

Dado el problema y dentro del contexto en que será desarrollada esta memoria, podemos encontrar los siguientes *stakeholders* que se verán involucrados de alguna u otra manera (la Tabla 1 refleja en detalle a estos actores):

- Emprendedoras
- Compradoras y compradores
- Equipo de desarrollo de Aliadas
- UTFSM

También podemos encontrar otros *stakeholders*, que si bien no se relacionan directamente con el problema en cuestión, si se relacionan con el desarrollo de esta plataforma, ya que

¹²Habilidad de un individuo para realizar tareas efectivamente en un ambiente digital.

Tabla 1: Stakeholders del Problema.

Fuente: Elaboración Propia.

Stakeholder	Descripción	Relación
Emprendedoras	Mujeres microemprendedoras de la región de Valparaíso, que serán usuarias finales de la plataforma.	Toda la información relacionada a sus datos personales y emprendimientos supondrán uno de los activos más importantes del proyecto.
Compradoras/es	Personas que buscarán adquirir los emprendimientos de la plataforma, siendo estos también usuarios finales de ella.	Toda la información de sus datos personales supondrá un activo importante del proyecto.
Equipo de desarrollo de Aliadas	Todas las personas involucradas en el desarrollo de este proyecto.	La implementación de las políticas y mecanismos de ciberseguridad involucra a todo el equipo de desarrollo.
UTFSM	Institución a la que pertenece gran parte del equipo de desarrollo	Todo impacto que tenga la plataforma, conllevará a la afectación (positiva o negativa) de la institución.

se verán afectados de alguna u otra manera con la inclusión de ésta. Entre estos actores indirectos encontramos:

- Patrocinadores
- Comunidad
- Municipalidades
- SERNAMEG
- Organizaciones que son competencia
- Organizaciones relacionadas al emprendimiento femenino

En la Figura 1 se puede observar una relación mas visual de los *stakeholders* mencionados anteriormente. Nótese como se hace la distinción entre aquellos que se ven directamente impactados por el problema y aquellos que se ven más bien involucrados por el desarrollo de la plataforma.

Además, como Aliadas es una plataforma diseñada principalmente para mujeres, es que esta memoria acuñará el término de "usuarias" para referenciar el plural de usuarios y usuarias.

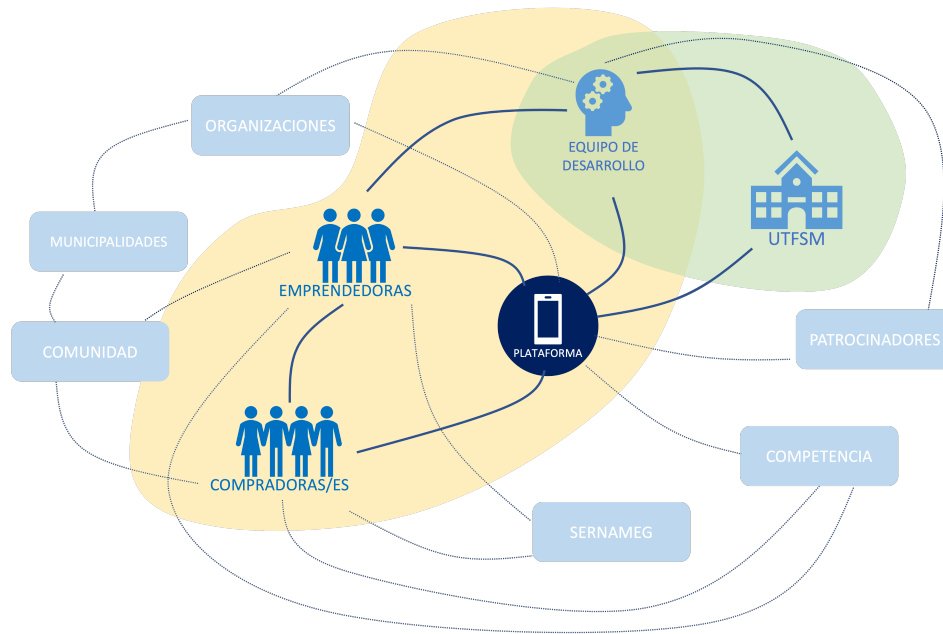


Figura 1: Mapa de Stakeholders.
Fuente: Elaboración Propia.

Dada la hipótesis de tomar como marco de trabajo el diseño centrado en usuarias y teniendo claridad del problema que se desea abordar (junto con los *stakeholders* involucrados en él), es posible plantear los objetivos generales y específicos que guiarán el desarrollo de esta memoria.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

- Diseñar e implementar políticas y mecanismos de ciberseguridad para una plataforma de mercado digital de emprendimientos de mujeres a través de un enfoque centrado en usuarias.

1.2.2. OBJETIVOS ESPECÍFICOS

- Explorar las necesidades y condiciones relevantes a la ciberseguridad de las mujeres emprendedoras que serán usuarias de la plataforma de mercado digital.
- Investigar y comparar políticas y mecanismos de ciberseguridad que actualmente son utilizadas en plataformas digitales.

- Vincular las necesidades identificadas al diseño de un plan de ciberseguridad, incluyendo la selección de políticas y mecanismos de ciberseguridad para la plataforma de mercado digital.
- Implementar el plan diseñado en la plataforma de mercado digital de emprendimientos de mujeres.

CAPÍTULO 2

MARCO CONCEPTUAL

2.1. DISEÑO CENTRADO EN USUARIAS

Antes de hablar de ciberseguridad, es necesario conocer el concepto que resulta ser el pilar fundamental para la elaboración de esta memoria: el diseño centrado en usuarias (también conocido por sus siglas DCU ¹³).

Este concepto tiene sus orígenes en 1975, pero fue durante la década de los 80's cuando fue popularizado por Donald Norman en la Universidad de California luego de la publicación de su libro *User-Centered System Design: New Perspectives on Human-Computer Interaction* [Norman y Draper, 1986], que luego junto con la publicación del libro *The Psychology Of Everyday Things* [Norman, 2013] sentaron las bases de lo que posteriormente sería ampliamente conocido como DCU.

Tal como plantea [López, 2019], podemos resumir los fundamentos del DCU en el siguiente listado:

- El diseño se basa en el entendimiento de las usuarias, sus tareas y su contexto.
- Las usuarias están involucradas en el proceso de diseño y desarrollo.
- El diseño es guiado y refinado por evaluaciones centradas en usuarias.
- El proceso es iterativo.
- El diseño apunta a la experiencia de las usuarias.

2.1.1. ETAPAS EN EL DCU

Basándose en la ISO 13407, existen cinco procesos esenciales que deben llevarse a cabo para incorporar de manera exitosa los requisitos de usabilidad en el proceso de desarrollo de software. Ahora, tal como se mencionó anteriormente, el DCU no se limita solo a esto, por lo que estas etapas pueden ser adaptadas para el diseño de un proceso. Las etapas y sus relaciones (Figura 2) son las siguientes:

- Planificar el proceso de DCU.
- Comprender y especificar el contexto de uso.

¹³El término en inglés se puede encontrar como *User Centered Design* (UCD)

- Especificar los requisitos de la usuaria y de la organización.
- Elaborar diseños y prototipos.
- Llevar a cabo una evaluación basada en usuarias.



Figura 2: Etapas claves del DCU.

Fuente: Traducción del diagrama en [Maguire, 2001] pag. 589

De esta manera, podemos definir el DCU como un *framework*¹⁴ en donde los objetivos y decisiones de los procesos están basados en las necesidades, objetivos, expectativas, motivaciones y capacidades de las usuarias; y algo que resulta bastante interesante en este marco de trabajo es que lo anterior no limita su uso a interfaces y/o tecnologías. Dicho en otras palabras, el DCU permite optimizar el proceso en torno a la forma en que las usuarias pueden, quieren o necesitan utilizarlo, lo que trae como consecuencia que las usuarias no se vean obligadas a cambiar su comportamiento y sus expectativas para adaptarse al proceso.

Ahora bien, para llevar a cabo cada una de las etapas del DCU es necesario conocer los distintos métodos que pueden ser aplicados al momento de utilizar este marco de trabajo.

2.1.2. MÉTODOS EN EL DCU

Si bien el listado de métodos conocidos es extenso, serán mencionados aquellos que fueron utilizados durante el desarrollo de esta memoria:

¹⁴Conjunto estandarizado de prácticas y criterios que sirven para enfocar una problemática particular como referencia, para enfrentar y resolver problemas de índole similar.

- **Statement starters:** Ubicándose dentro de la etapa del DCU que planifica el proceso de diseño, este enfoque permite redactar los enunciados que hacen referencia a los problemas, de una manera tal que invita a realizar una amplia exploración (a través del pensamiento en equipo), y dónde se pone foco en buscar las *preguntas correctas*, para poder llegar así a las *mejores soluciones*. Lo anteriormente mencionado puede simplificarse en la utilización del iniciador HMW; "*How*" (cómo), "*Might*" (podríamos) y "*We*" (nosotros). Este iniciador lleva a poder elaborar de mejor forma las preguntas que se necesitan responder.
- **Affinity Diagram:** Durante las investigaciones es posible encontrarse frente a una gran cantidad de información, y frente a ello es necesario poder realizar una búsqueda de patrones (*finding patterns*) que nos permita reducir la complejidad de toda la información con la que se cuenta. Ubicado en la etapa que permite comprender y especificar el contexto de uso, la utilización de los *affinity diagram* son una forma de organizar la información en grupos lógicos (*clustering*), haciendo esta agrupación en base a la similitud entre los ítems de información.
- **Creative matrix:** Dentro de la etapa que busca la elaboración de diseños y prototipos, Las matrices de creatividad sirven para generar nuevas ideas en el cruce de distintos temas. Esto es posible lograrlo manejando una matriz que cruce aspectos como lo son las soluciones generales, con aspectos como preguntas, desafíos, oportunidades y/o segmentos de usuarias.
- **Think-aloud testing:** Finalmente, en la etapa que busca evaluar la solución planteada aparecen este tipo de prueba que se enfoca no solo en ver lo que hace la usuaria, sino que también en solicitar que cuente sus pensamientos mientras usa el prototipo. Dentro de las ideas que se esperan escuchar está qué quiere hacer, qué espera de ello y cómo toma las decisiones.

En la Figura 3 se puede apreciar dónde están ubicados estos métodos dentro de las etapas claves del DCU.

Una vez entendido el concepto de centrar el diseño en las personas, es necesario comprender el significado de ciberseguridad y los conceptos que engloba y que están relacionados a esta memoria.

2.2. CIBERSEGURIDAD

El término 'ciberseguridad' ha sido objeto de la literatura académica y popular a lo largo de muchos años, pero ha ido tomando mayor importancia durante la última década. Y es que hoy en día no se puede concebir hablar de TIC sin hablar de ciberseguridad.

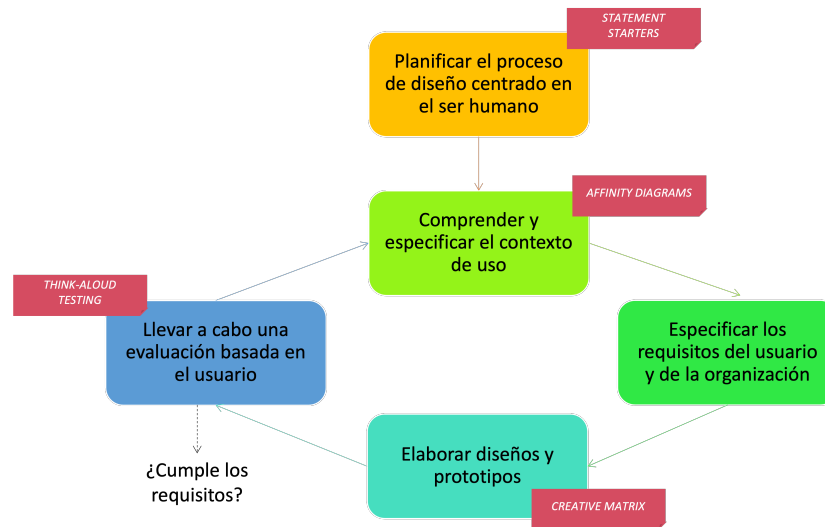


Figura 3: Métodos utilizados en las etapas claves del DCU.

Fuente:Elaboración propia basada en la Figura 2.

2.2.1. DEFINICIÓN DE CIBERSEGURIDAD

A lo largo de la literatura se puede comprobar que el término se utiliza en un sentido amplio. Para efectos prácticos, se analizaron las definiciones abordadas por [Craigen *et al.*, 2014] en el estudio titulado '*Defining Cybersecurity*'. Entre estas definiciones, se destacan las siguientes:¹⁵

- '*La Ciberseguridad consiste en gran medida en métodos defensivos utilizados para detectar y frustrar a los posibles intrusos*' [Kemmerer, 2003]
- '*La Ciberseguridad implica la protección de las redes informáticas y de la información que contienen, contra la penetración y el daño o la interrupción maliciosa*' [Lewis, 2006]
- '*La Ciberseguridad es el conjunto de instrumentos, políticas, conceptos de seguridad, mecanismos de seguridad, directrices, enfoques de gestión de riesgos, medidas, capacitación, prácticas óptimas, garantías y tecnologías que pueden utilizarse para proteger el entorno cibernético y los activos de la organización y del usuario*' [ITU, 2009]
- '*La Ciberseguridad es la actividad o el proceso, la capacidad o habilidad, o el estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos se protegen y/o defienden contra el daño, el uso o la modificación no autorizados, o la explotación.*' [NICCS, 2014]

¹⁵La definiciones han sido traducidas desde su idioma original al español.

Si bien estas definiciones resultan útiles para el entendimiento general de la Ciberseguridad, no proporcionan necesariamente una visión holística que apoye suficientemente la interdisciplinariedad de la misma. Bajo esa perspectiva [Craig et al., 2014] buscó una definición nocional que se base en la objetividad, frente a la suposición. En esa búsqueda fue capaz de definir una serie de *Key Terms* que deberían estar presentes (aunque no en su totalidad) en una definición, y en base a ellos fue capaz de crear la siguiente:

Conjunto de recursos, procesos y estructuras utilizados para la protección de activos de información que viven en el ciberespacio, por medio del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

La Ciberseguridad muchas veces se ha utilizado como sinónimo de **Seguridad de la Información** (SI). Es necesario aclarar que si bien ambos conceptos están relacionados, no significan lo mismo. La SI según NIST ¹⁶ (*National Institute of Standards and Technology*) se define como "La protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar confidencialidad, integridad y disponibilidad"[Nieles et al., 2017]. Podemos decir entonces que el concepto de SI está involucrado dentro del macro-concepto de Ciberseguridad.

2.2.2. TRIADA CID DE LA INFORMACIÓN

Pero no se puede seguir hablando de ciberseguridad sin conocer bien el concepto de la Triada CID ¹⁷ (Figura 4), ya que ésta supone un modelo en ciberseguridad en el cual enfocar las políticas y mecanismos que debe aplicar una organización en pos de proteger la información.

Las iniciales presentes en el nombre hacen referencia a los tres principios en los que se debe basar la Ciberseguridad. En esta memoria utilizaremos las definiciones de [Samonas y Coss, 2014]:

- **Confidencialidad:** Trata sobre cómo una organización mantiene el acceso a la información protegida. Esto implica limitar el acceso a ella, garantizando así que su uso se limite solo a las personas y/o procesos autorizados a ello.
- **Integridad:** Es el principio que garantiza que la información no ha sido manipulada de forma accidental o maliciosa por terceros, y por tanto implica que ésta es correcta, auténtica y fiable.

¹⁶Más información en <https://www.nist.gov>

¹⁷Conocida en inglés como CIA ("Confidentiality, Integrity, Availability")

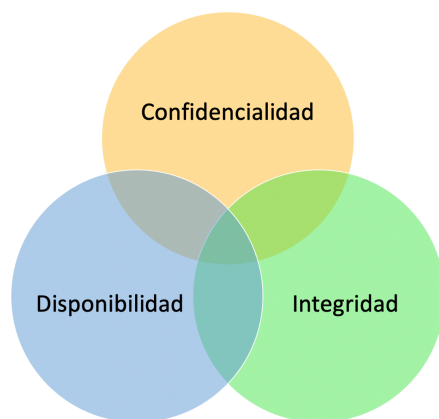


Figura 4: Triada CID.
Fuente: Elaboración Propia.

- **Disponibilidad:** Hace referencia a garantizar que tanto información, sistemas y aplicaciones sean accesibles a las personas o procesos autorizados cuando estos los necesitan.

Dado que existe una estrecha relación entre estos tres principios, es muy común encontrar esta relación representada mediante un diagrama de Venn (Figura 4).

Existen una gran cantidad de situaciones que pueden poner en peligro cada uno de estos principios, pero también existen contramedidas que permiten asegurarlos. Mediante la aplicación de políticas y mecanismos de ciberseguridad es que las organizaciones buscan asegurar estos principios, y es aquí donde los *frameworks* de ciberseguridad juegan un rol relevante.

2.2.3. FRAMEWORKS DE CIBERSEGURIDAD

Los *frameworks* (también conocidos como 'marcos de trabajo'), son un conjunto estandarizado de conceptos, prácticas y criterios utilizados para enfocar un tipo de problemática en particular como base y referencia para enfrentar y resolver problemas que resulten similares [Pérez y Gardey, 2020].

Los marcos de trabajo son muy utilizados en el desarrollo de software ya que fácilmente pueden servir de base para la organización y desarrollo de éstos; pero tienen la particularidad de que su alcance no se limita solo a ello. Esto permite poder abstraer el concepto y aplicarlo a la ciberseguridad.

En ciberseguridad, los *frameworks* suponen un lenguaje común de estándares que provee a las organizaciones un marco para poder diseñar e implementar procedimientos, mitigar

riesgos y/o solucionar problemas organizacionales. Serán sujeto de estudios los principales marcos de trabajo de ciberseguridad que son utilizados hoy en día y aquellos que eventualmente puedan ser utilizados en la aplicación de Aliadas.

2.2.3.1. Framework de NIST

Entre los *frameworks* de ciberseguridad se encuentra aquél desarrollado por NIST. Esta es una entidad que ayuda a pequeñas y grandes organizaciones a comprender mejor sus riesgos de ciberseguridad, para de esta manera lograr que las organizaciones puedan administrar y reducir sus riesgos, y en consecuencia proteger sus datos y redes.

El *framework* de ciberseguridad de NIST se compone de un ciclo de 5 etapas, también llamadas funciones, las cuáles a su vez se dividen en categorías que hacen referencia a las actividades dentro de estas funciones (Ver Figura 5):

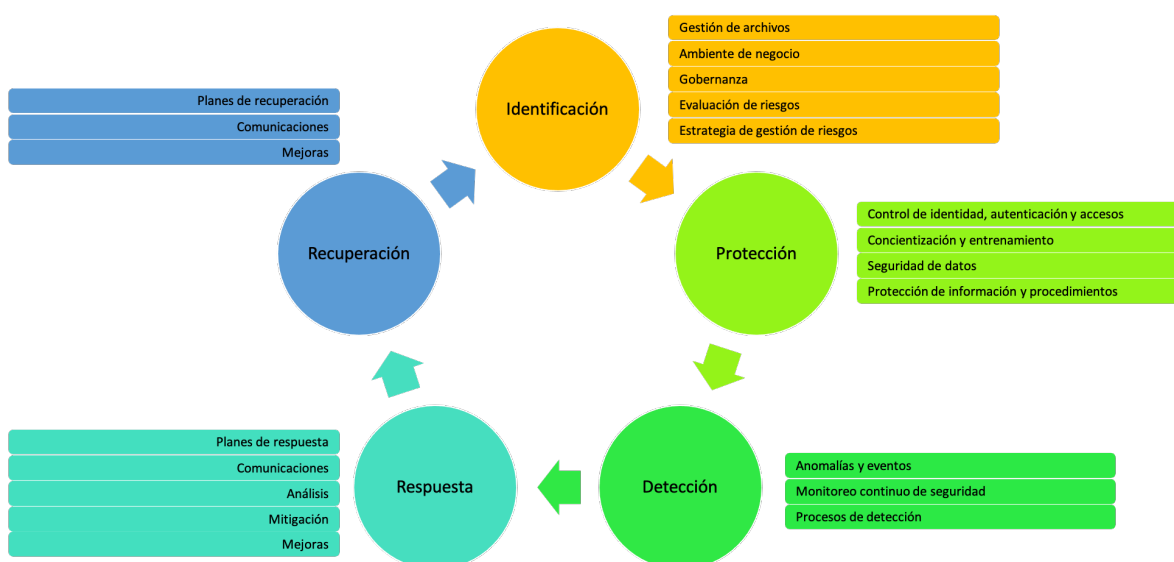


Figura 5: Etapas en el *framework* de ciberseguridad de NIST y sus categorías.

Fuente: Elaboración propia.

- **Identificación:** Busca entender la organización para lograr gestionar el riesgo de la ciberseguridad en cuanto a las personas, activos, sistemas, datos y capacidades. Dentro de esta etapa se pueden encontrar las siguientes categorías:

- Gestión de archivos
- Ambiente de negocio
- Gobernanza
- Evaluación de riesgos
- Estrategia de gestión de riesgos

- **Protección:** Se busca implementar medidas de ciberseguridad que garanticen la entrega del servicio de la organización. También se busca determinar como limitar o contener un posible incidente de ciberseguridad. Entre las categorías de esta etapa se encuentran:
 - Control de identidad, autenticación y accesos
 - Concientización y entrenamiento
 - Seguridad de datos
 - Protección de información y procedimientos
- **Detección:** Busca implementar acciones que lleven a identificar oportunamente eventos asociados a incidentes de ciberseguridad. Dentro de la etapa se distinguen las siguientes categorías:
 - Anomalías y eventos
 - Monitoreo continuo de seguridad
 - Procesos de detección
- **Respuesta:** Intenta tomar medidas con respecto a un incidente de ciberseguridad detectado, con el fin de contener su impacto. Entre las categorías están:
 - Planes de respuesta
 - Comunicaciones
 - Análisis
 - Mitigación
 - Mejoras
- **Recuperación:** Contempla planes de resiliencia y el restablecimiento de los servicios o procesos que hayan sido afectados por un incidente de ciberseguridad. Las categorías de esta etapa incluyen:
 - Planes de recuperación
 - Comunicaciones
 - Mejoras

Ahora bien, hay que destacar que dentro de estas **categorías**, existen **sub-categorías** que definen resultados específicos de estas actividades técnicas o de gestión. Y paralelamente encontramos lo que se denomina como **referencias informativas** que involucran normas, directrices y/o prácticas que permiten lograr los resultados asociados a cada sub-categoría (Ver Figura 6).

Es importante comprender que este marco de trabajo no es obligatorio, pero si es ampliamente reconocido dentro de la comunidad de ciberseguridad por su adaptación a todo tipo de organizaciones [Almagro, 2019].

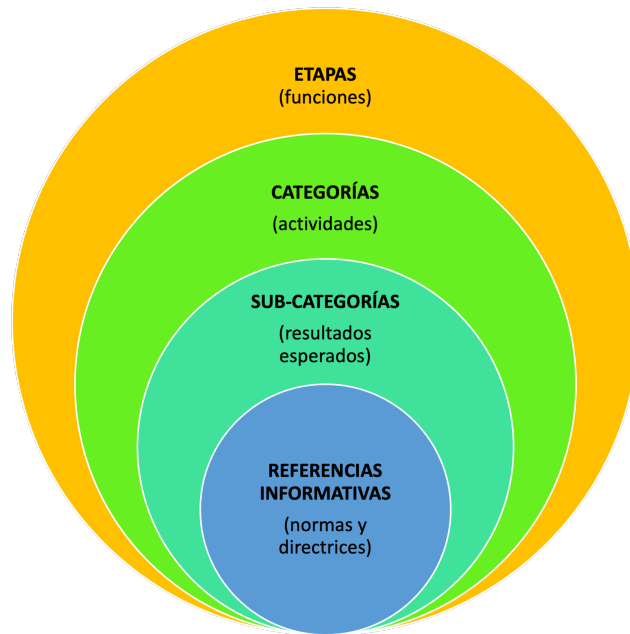


Figura 6: Relación entre los elementos del *framework* de ciberseguridad de NIST.

Fuente: Elaboración propia.

2.2.3.2. ISO 27001

Si bien las normas ISO proporcionan normativas certificables, en ciberseguridad también se podría hablar de ellos como *frameworks* puesto que pueden ser utilizados como marcos de trabajo para diseñar e implementar procedimientos relacionados a la ciberseguridad.

La ISO 27001¹⁸ permite asegurar y proteger la información dentro de una organización, a nivel físico y digital. Esto lo hace, por medio de una serie de requisitos que deben ser cumplidos con tal de poder efectuar una gestión de la seguridad de la información de la organización.

El foco principal de la ISO 27001 recae en adoptar un **Sistema de Gestión de Seguridad de la Información** (SGSI), que es la vía para lograr un sistema que integre políticas, procedimientos y acciones para proteger la información. Debido a esto, los SGSI tienen un fuerte enfoque en los procesos, ya que busca controles que se usen para asegurar que la operación del negocio se haga de forma segura en la medida que además agregue valor.

El documento contiene 14 cláusulas y 114 controles que deben ser implementados para cumplir con la normativa y así implementar un SGSI. Por otra parte, existe la ISO 27002 que determina cómo llevar a cabo la normativa anterior, es decir, cómo llevar a la práctica los 114 controles de seguridad de la ISO 27001.

¹⁸Recuperado en <https://www.normas-iso.com/iso-27001/>

2.2.3.3. CIS

Los controles de CIS ¹⁹ son un conjunto de mejores prácticas en ciberseguridad y acciones defensivas que pueden ayudar a evitar incidentes de ciberseguridad. Estos controles proporcionan entonces un marco de trabajo para alcanzar metas y objetivos, considerando marcos jurídicos, reglamentarios y normativos, por lo que también puede ser considerado un *framework* dentro de la ciberseguridad.

Dentro de la estructura de los controles de CIS (Ver Figura 7) encontramos un total de 20 recomendaciones (llamados controles) que se dividen en tres categorías:

- **Controles de CIS básicos:** Controles de uso general que una organización debería implementar para garantizar la disponibilidad de una defensa. Entre estos controles se encuentran:
 - C1: Inventario y control de activos de hardware
 - C2: Inventario y control de activos de software
 - C3: Gestión continua de vulnerabilidades
 - C4: Uso controlado de privilegios administrativos
 - C5: Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores
 - C6: Mantenimiento, monitoreo y análisis de logs de auditorías
- **Controles de CIS fundamentales:** Controles que una organización debería implementar para contrarrestar amenazas técnicas que son más específicas. Entre estos controles se encuentran:
 - C7: Protección de correo electrónico y navegador web
 - C8: Defensas contra malware
 - C9: Limitación y control de puertos de red, protocolos y servicios
 - C10: Funciones de recuperación de datos
 - C11: Configuraciones para dispositivos de red, tales como firewalls, routers y switches
 - C12: Protección perimetral
 - C13: Protección de datos
 - C14: Control de accesos
 - C15: Control de acceso inalámbrico
 - C16: Monitoreo y control de cuentas

¹⁹Recuperado en <https://www.cisecurity.org/controls/>

- **Controles de CIS organizacionales:** Controles que se enfocan en aspectos más técnicos, tomando como foco las personas y procesos involucrados en la ciberseguridad. Una organización debería implementarlos para garantizar una madurez de ciberseguridad a largo plazo. En esta última categoría se encuentran los siguientes controles:

- C17: Implementar un programa de concientización y capacitación en seguridad
- C18: Seguridad del software de aplicación
- C19: Respuesta y gestión de incidentes
- C20: Pruebas de penetración y ejercicios de *Red Team*



Figura 7: Categorización de los 20 controles de CIS.
Fuente: Elaboración propia.

Si bien estos *frameworks* facilitan la adecuación de procedimientos, buenas prácticas y procesos; no siempre estos logran cubrir las necesidades de las personas a las que busca alcanzar el procedimiento o proceso en cuestión. Frente a ello resulta interesante lograr combinar tanto el DCU con los *frameworks* en ciberseguridad, para lograr políticas y mecanismos que sean lo suficientemente eficaces.

2.3. CIBERSEGURIDAD EN CHILE

Es importante también entender el panorama actual que se vive en Chile frente al concepto de ciberseguridad. Para ello el análisis se realizó en base a dos aspectos:

- Los aspectos legales y estatales que envuelven a la ciberseguridad en Chile hoy en día.
- La mirada sobre los cambios que han sufrido los países de América Latina y el Caribe respecto a la ciberseguridad desde 2016 a 2020 [BID y OEA, 2020].

2.3.1. ESTRATEGIA CHILENA DE CIBERSEGURIDAD

Chile es un país que no cuenta de manera oficial con una estrategia de ciberseguridad que pueda ser seguida por el sector privado para mejorar sus capacidades de defensa en el ciberespacio; pero actualmente se puede encontrar una "Política Nacional de Ciberseguridad", que plantea un mapa de acción y compromisos del Estado con una visión que apunta al año 2022 [de Chile, 2017].

Esta política tiene como ejes centrales:

- Prevención y Sanación
- Sensibilización, formación y difusión
- Infraestructura e Información
- Institucionalidad de la ciberseguridad
- Cooperación y relaciones internacionales

Siendo estos ejes la base para definir los siguientes objetivos generales y secundarios [de Chile, 2017]:

- "El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos
 - Concepto. Identificación y gestión de riesgos
 - Protección de la infraestructura de la información
 - Identificación y jerarquización de las infraestructuras críticas de la información
 - Contar con equipos de respuesta a incidentes de ciberseguridad
 - Implementación de mecanismos estandarizados de reporte, gestión y recuperación de incidentes
 - Exigencia de estándares diferenciados en materia de ciberseguridad
- El Estado velará por los derechos de las personas en el ciberespacio
 - Prevención de ilícitos y generación de confianza en el ciberespacio

- Establecimiento de prioridades en la implementación de medidas sancionatorias
- Prevención multisectorial
- Respeto y promoción de derechos fundamentales
- Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales
 - Una cultura de la ciberseguridad
 - Sensibilización e información a la comunidad
 - Formación para la ciberseguridad
- El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales
 - Principios de política exterior chilena
 - Cooperación y asistencia
 - Reforzar la participación en instancias multilaterales y en instancias de múltiples partes interesadas (*multistakeholder*)
 - Fomentar normas internacionales que promuevan la confianza y seguridad en el ciberespacio
- El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégico
 - Importancia de la innovación y desarrollo en materia de ciberseguridad
 - Ciberseguridad como medio para contribuir al desarrollo digital de Chile
 - Desarrollo de la industria de ciberseguridad en Chile
 - Contribuir a la generación de oferta por parte de la industria local
 - Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado”

Si bien lo anterior suma y aplica para poder desarrollar una estrategia de ciberseguridad que sea eficaz, es necesario conocer los aspectos legales que envuelven a la ciberseguridad y cómo estos pueden eventualmente afectar en el desarrollo de políticas y mecanismos de ciberseguridad dentro de una organización.

2.3.1.1. LEY DEL CIBRECRIMEN O DELITOS INFORMÁTICOS

Actualmente rige la Ley 19.223 ²⁰ la cual fue promulgada en 1993, y hasta la fecha no

²⁰Más información en <https://www.bcn.cl/leychile/navegar?idNorma=30590>

ha sufrido modificaciones. Esta es una ley que en sus tiempos fue bastante visionaria puesto que buscó castigar con cárcel los delitos informáticos en una época en que no se hablaba mucho de ellos. Lamentablemente al no haber sido modificada en el tiempo, muchos de los términos utilizados resultan hoy en día ser poco claros. Estas indefiniciones (por ejemplo, hablar de actos "maliciosos", sin definir lo que se considera como un acto malicioso) provoca que sea muy fácil escapar de esta ley.

Pero actualmente gracias tanto a la creación de la anteriormente mencionada "Política Nacional de Ciberseguridad", como también la firma del "Convenio de Budapest"²¹ (también conocido como "Convenio sobre la ciberdelincuencia"), se logró impulsar el "Proyecto de Ley de Delitos Informáticos"²² cuyo propósito radica por una parte en mejorar las definiciones para cada hito penal mencionado en la ley que rige actualmente, y también incorpora nuevos delitos informáticos que anteriormente no fueron considerados (como la falsificación informática, fraude informático, abuso de dispositivos, etc). Este proyecto a la fecha se encuentra en tercer trámite constitucional.

2.3.1.2. LEY DE PROTECCIÓN DE DATOS

Otra ley importante respecto a ciberseguridad es la Ley 19.628 ²³, promulgada en 1999, que habla sobre la protección de la vida privada, y por ende, toca aspectos sobre la protección de datos. Si bien esta ley ha sufrido modificaciones durante este último tiempo (su última modificación fue durante el año 2020), cae en el mismo error de contener muchas indefiniciones que permiten caer en vacíos legales.

Ahora bien, el acontecer de los últimos años respecto a distintos incidentes de ciberseguridad a nivel nacional (como lo son lo acontecido en Gobierno Digital ²⁴, Banco Estado ²⁵, Banco de Chile ²⁶, entre otros), han impulsado que la normativa avance en vías de mejorar esta ley, mediante el "Proyecto de Ley de Protección de Datos Personales"²⁷. Este proyecto a la fecha se encuentra en primer trámite constitucional.

Las nuevas leyes que buscan reemplazar a las que actualmente rigen, tienen principalmente como propósito mejorar las definiciones (para no caer en vacíos legales), y fortalecer las sanciones, haciéndolas mucho más estrictas.

²¹Más información en <https://www.bcn.cl/leychile/navegar?idNorma=1106936>

²²Más información en <https://www.camara.cl/legislacion/ProyectosDeLey> Boletín: 12192-25

²³Más información en <https://www.bcn.cl/leychile/navegar?idNorma=141599>

²⁴Más información en <https://laopiniondechiloe.cl/gobierno-confirma-hackeo-a-sitio-de-gobierno-digital-y-descarta-filtracion-a-claves-unicas/>

²⁵Más información en <https://www.fayerwayer.com/2020/09/banco-estado-hackeo-ransomware/>

²⁶Más información en <https://www.elmostrador.cl/dia/2018/07/18/hackeo-en-el-banco-de-chile-informatico-robo-475-millones-de-pesos/>

²⁷Más información en <https://www.camara.cl/legislacion/ProyectosDeLey> Boletín: 11144-07

2.3.2. CAMBIOS DE LA CIBERSEGURIDAD EN CHILE ENTRE 2016 Y 2020

El reporte elaborado por la OEA [BID y OEA, 2020] considera cinco dimensiones (enumeradas desde D1 a D5) que tratan de abarcar distintos aspectos en los que tiene cabida la ciberseguridad:

- **D1, "Políticas y estrategias de seguridad cibernética":** Aspectos que se enfocan en el diseño de estrategias y la resiliencia de la ciberseguridad)
- **D2, "Cultura cibernética y sociedad":** Aspectos que buscan fomentar una cultura de ciberseguridad responsable en la sociedad.
- **D3, "Educación, capacitación y habilidades en de seguridad cibernética":** Aspectos relacionados al desarrollo del conocimiento de la ciberseguridad.
- **D4, "Marcos legales y regulatorios":** Aspectos relacionados a la creación de marcos legales y regulatorios efectivos.
- **D5, "Estándares, organizaciones y tecnologías":** Aspectos relacionados al control de riesgos a través de estándares, organizaciones y tecnología.

A estas dimensiones se les evaluó la madurez de la capacidad de ciberseguridad. Los niveles de madurez son cinco y son llamados inicial, formativa, consolidada, estratégica y dinámica. Estos van desde un nivel donde hay ausencia de madurez a un nivel donde la madurez se encuentra más completa (Ver Tabla 2).

En cuanto a la primera dimensión evaluada, **"Políticas y estrategias de seguridad cibernética"**, se puede ver una clara tendencia a la mejora en los aspectos de 'Estrategia Nacional de Seguridad Cibernética', 'Respuesta frente a Incidentes' y 'Defensa cibernética'. No así en los aspectos de 'Protección de la infraestructura crítica', 'Manejo de crisis' y 'Redundancia de comunicaciones', donde se puede ver que los niveles de madurez han variado muy poco o simplemente se han mantenido (Ver Figura 8).

Lo anterior tiene sentido si se considera que Chile presentó su estrategia nacional de seguridad en abril del 2017, con miras al 2022. Si bien solo queda un año para mejorar los niveles de seguridad, se espera que a esta fecha exista una mejora en todos los aspectos de esta dimensión.

En cuanto a la segunda dimensión, **"Cultura cibernética y sociedad en Chile"**, podemos ver que también han existido mejoras. Esto se refleja ya que todos los aspectos de la dimensión ('Mentalidad de seguridad cibernética', 'Confianza y seguridad en internet', 'Comprensión del usuario de la protección de la información en línea', 'Mecanismos de denuncia' y 'Medios y redes sociales') se encuentran en un nivel de maduración consolidada (Ver Figura 9).

Si bien lo anterior es un paso enorme, sigue siendo sumamente importante trabajar en la concientización no solo de los usuarios, sino también de todas las personas involucradas en

Tabla 2: Madurez de la Capacidad de Ciberseguridad.

Fuente: Elaboración basada en [BID y OEA, 2020].

Nivel de Madurez	Descripción
Inicial	No existe madurez en ciberseguridad o bien se encuentra en un estadio muy embrionario
Formativa	Algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos
Consolidada	Los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos
Estratégica	Se han tomado decisiones sobre qué indicadores son importantes y cuáles no para la organización o el Estado en particular.
Dinámica	Existen mecanismos claros para alterar la estrategia en función de las circunstancias prevalentes, como la sofisticación tecnológica del entorno de amenaza, el conflicto global o un cambio significativo en un área de preocupación (por ejemplo, delito informático o privacidad).

las organizaciones y/o equipos de desarrollos de las plataformas. Y esto principalmente se debe a que cerca del 95 % de los ciberataques que tienen éxito viene precedidos de errores humanos [Bernal, 2020]. Este punto resulta realmente interesante considerando que el objetivo de esta memoria busca trabajar con las usuarias y el equipo de desarrollo de la plataforma.

En cuanto a la tercera dimensión, "**Formación, capacitación y habilidades de seguridad cibernética**", se puede observar una leve mejora respecto al año 2016, destacando un aumento de los programas de sensibilización y mejores marcos para la capacitación profesional (Ver Figura 10). A la fecha, es posible al realizar una rápida búsqueda en un motor de búsqueda como Google y encontrarse con numerosas opciones tanto de títulos de pre-grado, post-gradados, magísteres y certificaciones en Ciberseguridad. Esto resulta positivo a la hora de buscar oportunidades para mejorar las capacidades técnicas de un profesional en materias de ciberseguridad.

Por otra parte, al hablar de la cuarta dimensión, "**Marcos legales y regulatorios**", se puede observar una clara mejora en varios aspectos como lo son las legislaciones respecto a variados temas y la cooperación (formal e informal) para combatir el delito cibernético. Se destaca dentro de esta dimensión los saltos de maduración que tuvieron las legislaciones relacionadas al consumidor y la protección intelectual que fueron del nivel inicial de maduración al estratégico. Algo similar ocurre con los puntos relacionados a los 'Marcos de cooperación formales e informales para combatir el delito cibernético', pasando de un nivel de maduración inicial a uno consolidado (Ver Figura 11).



Figura 8: Políticas y Estrategias Cibernéticas en Chile.

Fuente:[BID y OEA, 2020] pag. 77

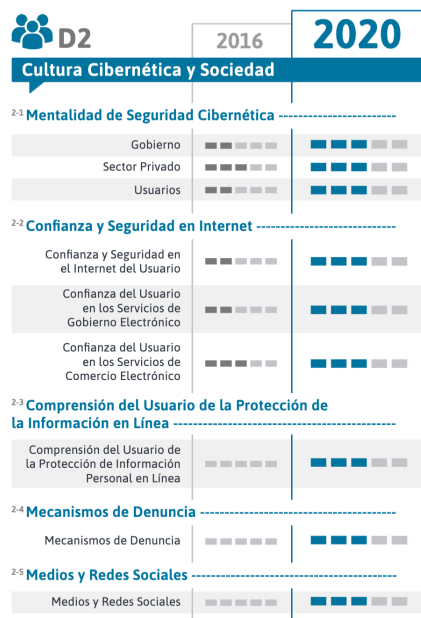


Figura 9: Cultura Cibernética y Sociedad en Chile.

Fuente:[BID y OEA, 2020] pag. 77



Figura 10: Formación, Capacitación y Habilidades de Seguridad Cibernética en Chile.
Fuente:[BID y OEA, 2020] pag. 78



Figura 11: Marcos Legales y Regulatorios en Chile.
Fuente:[BID y OEA, 2020] pag. 78

Finalmente en cuanto a la quinta dimensión, **"Estándares, organizaciones y tecnologías"**, a grandes rasgos también se puede visualizar una mejora con respecto al 2016. Cuando se habla del cumplimiento de los estándares, hay mejoras en cuanto a los estándares de seguridad, pero no así respecto a los estándares en el desarrollo de software que se mantiene tal como el año anterior. Este punto no dejar de ser relevante para la memoria, dado que un desarrollo seguro es un aspecto fundamental a la hora de desarrollar software. No se pue-

de pensar en implementar mecanismos de seguridad en los software, si la construcción de estos estará sujeta a errores que puedan derivar en vulnerabilidades. Además, se destaca el aumento a una madurez formativa de los controles técnicos y criptográficos (Ver Figura 12).

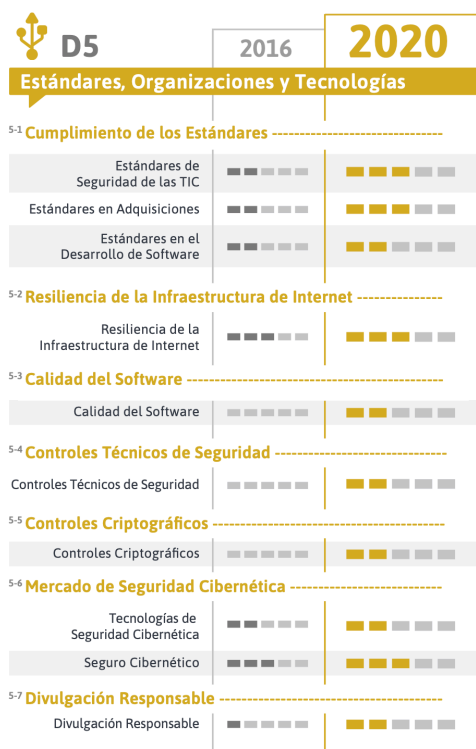


Figura 12: Estándares, Organizaciones y Tecnologías en Chile.

Fuente:[BID y OEA, 2020] pag. 78

Conociendo entonces como está la ciberseguridad en Chile y cuales son los tres principios fundamentales en que se basa la ciberseguridad, podemos dar pie a hablar de uno de los puntos centrales de esta memoria: las políticas y mecanismos de ciberseguridad.

2.4. POLÍTICAS DE CIBERSEGURIDAD

Una política de ciberseguridad es una declaración que busca establecer los lineamientos para llevar a cabo los controles y actividades de ciberseguridad en una organización. Se debe comprender, tal como plantean [Harknett y Stever, 2011], que una política no especifica cuál es la solución tecnológica, sino que lo que hace es especificar el conjunto de condiciones e intenciones que ayudarán a proteger los activos de la organización bajo los 3 principios de la triada CID.

Lo ideal es que la política de ciberseguridad pueda traducirse en objetivos específicos y medibles, y que se encuentre en un documento que sea fácilmente accesible por los miembros

de la organización, es decir, la sugerencia es que esta se encuentre escrita en la documentación de la organización. En el fondo, debe ofrecer una rápida orientación tanto sobre qué tipos de comportamientos y uso de recursos se requieren por parte de los miembros de la organización, como también sobre lo que está prohibido seguir.

2.4.1. RESPONSABLES EN LA POLÍTICA DE CIBERSEGURIDAD

El desarrollo de una política de ciberseguridad no es algo que surge desde la perspectiva de un solo equipo dentro de una organización. Tanto si se habla de organizaciones grandes u organizaciones de menor tamaño, esta resulta ser una operación colectiva que busca involucrar a todas las entidades de la organizaciones que se vean afectadas por estas políticas [Barman, 2002].

Si se piensa en una organización relativamente de mayor tamaño, podemos identificar típicamente a las siguientes entidades involucradas:

- **Altos cargos de la organización:** La política debe ser aprobada o revisada por aquellas personas que se encuentran en los cargos más altos de la organización.
- **Equipo TI:** Todos los miembros de los distintos equipos relacionados a las tecnologías de información (ej. equipo de desarrolladores, ingenieros, diseño, etc.), son quienes se verán afectados en mayor medida por las políticas de ciberseguridad, ya que como fue mencionado, lo que se busca es establecer normas sobre el uso de los sistemas de información.
- **Equipo jurídico:** A lo largo de la memoria se va a notar que hay ciertos puntos de las políticas que requieren un punto de vista que vaya desde lo legal. Debido a esto, es necesario que un equipo legal pueda revisar el documento final.
- **Equipo de RRHH:** Este equipo debe ser capaz de llevar un registro de todos aquellos empleados o colaboradores, que leyeron y entendieron la política estipulada; ya que en el eventual caso de infringir las normas estipuladas en el documento, es este equipo quien se ocupa de los castigos a aplicar.

Se puede decir entonces que una política exitosa será aquella que se adapte de la mejor manera a las necesidades de cada una de estas entidades.

2.4.2. CICLO DE UNA POLÍTICA DE CIBERSEGURIDAD

Otro punto abordado por [Barman, 2002] es la mirada que se hace al ciclo que sufre una política. Barman plantea un ciclo de 5 etapas (Ver Figura 13) en donde asegura que la elección de la política resulta ser una tarea sencilla si se compara con la validación de que la

política resulta eficaz. El enfoque implica las siguientes etapas: (1) Recogida de requisitos, (2) Definición de la propuesta, (3) Desarrollo de la política, (4) Aprobación de la política y (5) publicación de la política.

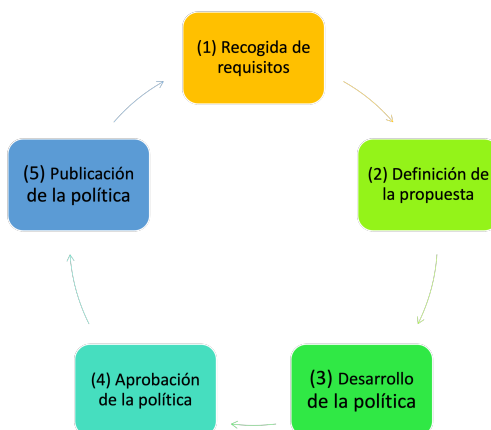


Figura 13: Ciclo de una política.

Fuente: Elaboración propia.

2.4.3. POLÍTICAS DE PRIVACIDAD

Dentro de las políticas de ciberseguridad, existe una política en particular que tiene una estrecha relación con el manejo de los datos de los y las usuarias (o clientes/as) dentro de la organización; y es que hay ciertos aspectos legales que deben ser considerados cuando se tratan datos personales y privados de terceros.

Esta relación queda estipulada en la 'Política de privacidad', la cual es un documento cuya legalidad depende del país en que se encuentre, y que plantea el cómo una organización retiene, procesa y maneja los datos de los y las usuarias. Las políticas de privacidad suponen un contrato entre el o la usuaria y la organización, donde esta última entidad es la que promete proteger los datos personales de el o la usuaria.

Ahora bien, al ser un contrato, la responsabilidad de leerla y aceptarla recae exclusivamente en el o la usuaria; mientras que la responsabilidad de cumplir lo estipulado en ella recae en la organización.

A la fecha, en Chile, no existe una legislación que sea fuertemente aplicable en cuanto a políticas de privacidad. La ley actual contiene muchas indefiniciones que permite caer en vacíos legales. Sin embargo, el panorama es diferente para otros países, y resulta interesante conocer la situación de Estados Unidos y la Unión Europea, pues pueden ser tomados como ejemplo.

- **Estados Unidos:** En Estados Unidos no existe una ley de aplicación general, pero si

hay leyes a nivel estatal que regulan las políticas de privacidad en circunstancias específicas, como lo son la COPPA ²⁸ (*Children's Online Privacy Protection Act*), la Ley Gramm-Leach-Bliley ²⁹ o la HIPAA ³⁰ (*The Health Insurance Portability and Accountability Act*).

- **Unión Europea:** La Unión Europea (UE) está mucho más desarrollada en el ámbito jurídico. Durante el año 2018, reemplazaron la anteriormente conocida 'Directiva de Protección de Datos', por el 'Reglamento General de Protección de Datos' ³¹ RGDP), que logró unificar todas las normas de privacidad que regían en todos los estados miembros de la UE. El RGDP impone reglas mucho más estrictas en cuanto a la protección de datos de los ciudadanos residentes de la UE, donde se hace énfasis en tener políticas de privacidad que sean mas precisas, claras y transparentes. Y algo relevante es que se incluye el apartado de dar la posibilidad a las personas de poder portar y eliminar sus datos en determinadas circunstancias si así lo desean.

2.4.3.1. INNOVACIÓN EN LAS POLÍTICAS DE PRIVACIDAD

Sin duda alguna, uno de los principales desafíos identificados cuando se habla de políticas de privacidad, es el hecho de lograr que los y las usuarias sean capaces de leer una política, entenderla y así dar un informado consentimiento en cuanto al uso de sus datos [Korunovska *et al.*, 2020]. Y si se considera que cada vez son más los países que tratan de adoptar normas similares a la RGDP, va a llegar un momento en que en Chile se van a tener que plantear políticas claras, concisas y transparentes.

Esta temática ha sido estudiada en varias investigaciones. Dentro de ellas una en particular resulta llamativa puesto que los investigadores realizaron un proceso de diseño iterativo (Ver Figura 14) para lograr desarrollar una política de privacidad que en forma de 'etiquetado nutricional' tuvo más aceptación de los y las usuarias [Kelley *et al.*, 2009]. De esta manera al mejorar la presentación visual y la comprensibilidad de la política de privacidad, es posible mejorar la experiencia de los y las usuarias frente a una política de privacidad.

Algo que ayudó al desarrollo de esta investigación fue el hecho de poder determinar tres pilares fundamentales que deben ser abordados en una política de privacidad, los cuales fueron derivados de lo que plantea el RGDP:

- **Qué:** qué información es recolectada
- **Cómo:** cómo es utilizada esta información

²⁸Más información en <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

²⁹Más información en <https://www.ftc.gov/es/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act>

³⁰Más información en <https://www.hhs.gov/hipaa/index.html>

³¹Más información en <https://gdprinfo.eu/es>

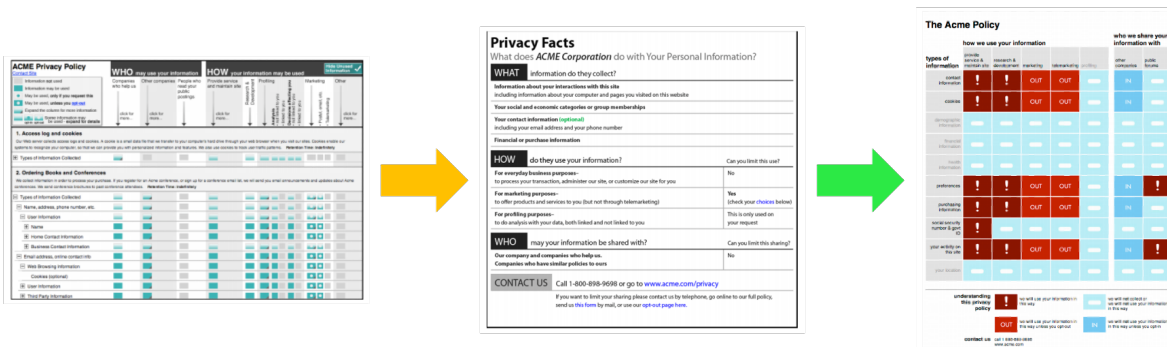


Figura 14: Evolución de resultados en el proceso de diseño iterativo.

Fuente: [Kelley *et al.*, 2009].

- **Quiénes:** con quiénes es compartida esta información

El hecho de presentar una política de privacidad provocó en los participantes una sensación de mayor seguridad frente a la protección de sus datos [Kelley *et al.*, 2009]. Lo anterior puede ser atribuido al hecho de que si se comprende que es lo que se está leyendo, se puede generar un vínculo de confianza entre la organización y el o la usuaria.

Retomando lo que son las políticas de ciberseguridad, se puede decir finalmente que éstas describen lo que se debe hacer, pero no describe el cómo hacerlo. En ese sentido, son los mecanismos de ciberseguridad los que realizan la implementación técnica de las políticas, es decir, el cómo hacerlo.

2.5. MECANISMOS DE CIBERSEGURIDAD

Los mecanismos de ciberseguridad son técnicas, métodos o procesos que se utilizan para implementar los lineamientos de ciberseguridad que plantean las políticas. Un mecanismo puede funcionar por sí mismo, o junto a otros, para proporcionar un aspecto de ciberseguridad en concreto [McLaughlin, 2020].

El listado de mecanismos de ciberseguridad existente es bastante amplio, y crece a medida que la tecnología va evolucionando, pero se pueden encontrar distintas formas de categorizar estos mecanismos. Una forma de agrupar estos mecanismos es basándose en sus atributos [Sangchoolie *et al.*, 2020]. Esta categorización incluye los siguientes grupos de mecanismos: (1) control de accesos, (2) control de autenticación, (3) autenticación de dispositivos, (4) firewalls, (5) redes virtuales, (6) encriptación, (7) redes virtuales privadas, (8) auditoría de logs, (9) sistemas de detección de intrusos, (10) sistemas de detección de malwares, (11) sistemas de escaneo de vulnerabilidades, (12) sistemas operativos, (13) tecnologías web, (14) controles de seguridad física, (15) firmas digitales y (16) particionado y separación.

El mismo autor propone una serie de características generales que tienen los mecanismos

de ciberseguridad y que vale la pena nombrar puesto que tienen relación con la propuesta de esta memoria:

- Los mecanismos pueden ser sistemáticos o aplicables. Esto quiere decir que pueden aplicarse sin conocer el sistema a proteger, o pueden adaptarse en base al conocimiento de éste. El contar con mecanismos que son aplicables permite, por ejemplo, poder hacer esa aplicación en base a las necesidades de los y las usuarias.
- Los mecanismos pueden funcionar de forma paralela al resto del sistema, o en momentos concretos. Este punto cobra importancia cuando tenemos equipos dentro de la organización que pueden estar dando un soporte continuo al mecanismo o cuando solo tenemos la capacidad humana para realizar este soporte cada cierto tiempo.
- Los mecanismos pueden tener como objetivo general el impedir que un atacante acceda al sistema o detectar al atacante una vez realizada la intrusión. Esto permite pensar en mecanismos que sean proactivos en contraste con mecanismos reactivos.

Ahora bien, se ha mencionado como la literatura clásica de ciberseguridad ha abordado su definición, cómo ésta se encuentra en Chile desde la perspectiva de la OEA, sus implicancias legales, y las definiciones de las políticas y mecanismos de ciberseguridad; pero es imposible no mencionar una tendencia que si bien no se ha popularizado aún, si resulta importante de analizar puesto que comparte muchos aspectos con el DCU. Esta tendencia es la que se conoce en algunos medios como 'Ciberseguridad feminista' (*Feminist cybersecurity*).

2.6. CIBERSEGURIDAD FEMINISTA

El concepto surge dada las limitaciones que muchas veces ofrecen los enfoques convencionales de la ciberseguridad. Bajo esa perspectiva, Julia Slupska y Scarlet Dawson Duckworth, mediante la investigación titulada *re:CONFIGURE Feminist Action Research in Cybersecurity* [Slupska y Duckworth, 2021] buscaron explicar el por qué es necesario un método alternativo de ciberseguridad feminista, explorando nuevas metodologías para llevarlo a cabo. Los estereotipos que siguen estando fuertemente asociados a la cultura de la ciberseguridad, como por ejemplo el hombre blanco con capucha, el informático socialmente inadaptado o el genio de la computación, se siguen reflejando en la industria según las autoras, y por consecuencia, en los enfoques dominantes de la ciberseguridad.

Dar cuenta como el etiquetar a las personas corrientes como el eslabón más débil de la cadena de seguridad (o incluso llegar a hablar de que son un factor humano que debe ser mitigado) ha provocado un alejamiento o incluso un temor por parte de algunas personas de utilizar las tecnologías, es una de las críticas mas fuerte que hace esta investigación.

Las investigadoras hicieron una búsqueda de información en dónde detectaron un punto fundamental: la forma en que los investigadores y defensores tradicionales abordan la segu-

ridad personal, es recurrir con demasiada frecuencia a la jerga técnica y a la culpabilización de las víctimas, es decir, se tiende a reprochar a aquellos usuarios por elegir contraseñas débiles o hacer click en enlaces de phishing.³²

Luego de ello, durante un período de 10 meses, se invitó a participantes a reflexionar y trabajar en base a los siguientes puntos:

- La definición de sus propias amenazas de ciberseguridad
- Que cambios podrían implementar en su vida para protegerse de estas amenazas
- El papel que cumple la ciberseguridad en sus vidas

Para trabajar estos puntos, la investigación se organizó en torno a *workshops* que siguieron los siguientes pasos: (1) Introducción, (2) Cuestionario demográfico, (3) Taller de modelamiento de amenazas, (4) Taller de apoyo técnico, (5) Análisis y (6) Discusión final.

En los pasos de introducción y cuestionario demográfico, se buscó principalmente dar a entender a participantes de que trataría la investigación y realizar una pequeña encuesta demográfica. De esta encuesta se destaca que aproximadamente un 65 % de participantes se identificaban como mujer, el 82 % era de raza blanca, el 79 % tenía entre 16 y 35 años, y cerca del 58 % consideraba que tenía muy poco conocimiento en privacidad y ciberseguridad.

Luego, durante el taller de modelamiento de amenazas, se realizó una jornada de *brainstorming* en donde se buscaban determinar los siguientes agentes dentro del ciclo de una amenaza: el activo, la amenaza como tal, y su mitigación.

Para poder determinar estos agentes, la actividad fue guiada planteando las siguientes preguntas: ¿Qué es lo de tu identidad digital que más deseas proteger?, ¿Qué te hace sentir amenazada en línea? ¿Cuándo fue la última vez que te sentiste insegura en línea? y ¿Qué te gustaría mejorar de tu seguridad digital?. Estas preguntas no utilizaron (de forma intencional) conceptos como 'ciberseguridad' o 'privacidad de datos', para evitar restringir las definiciones.

La gran diferencia de este modelamiento de amenazas, frente a otros más convencionales, es que éste se centra en los y las usuarias, y no en el sistema. Esto se puede evidenciar al leer las respuestas que daban las personas que participaron, destacando:

- Se mencionaban aspectos como la información personal, privada y financiera, imágenes e incluso los miedos, como aquellas partes de la identidad digital que más deseaban proteger.

³²Conjunto de técnicas que buscan engañar a una víctima ganándose su confianza al hacerse pasar por una persona, empresa o servicio reconocido, para manipularla y hacer que realice acciones que no debería realizar.

- La presencia de bots, información compartida entre aplicaciones, malas experiencias en videollamadas y el racismo, eran algunas de las situaciones que eran percibidas como amenazas.
- La utilización de canales de comunicación seguros, el almacenamiento en nube, contraseñas seguras, protección contra virus, cuidado en los eventos online y seguridad de sus participantes, eran mencionados como algunas de los aspectos que las personas deseaban mejorar de su vida digital.

Una vez recopilada y analizada la información del taller anterior, se realizó una segunda actividad de apoyo técnico. El objetivo de ésta buscaba crear un espacio social, abierto y seguro; donde se erradicaran malas acciones como el avergonzar a la persona por una mala práctica y/o reprochar lo que se debe o no debe hacer. Todos los puntos abordados en esta actividad, toman como base las respuestas de las preguntas realizadas en el taller anterior.

Posterior a esto, mediante la utilización de técnicas como los *Affinity diagram* y el *clustering* de información, las investigadores fueron capaces de determinar, entre otras cosas, un conjunto de potenciales nuevas herramientas de ciberseguridad. Entre ellas se destacan herramientas que permitan la eliminación de datos, herramientas educativas y de anonimización, e incluso se mencionaron controles de ciberseguridad.

Finalmente, dentro de las principales conclusiones derivadas de esta investigación activa, se destaca:

- La falta de conocimientos y el lenguaje técnico impiden que la gente sienta una cercanía por la ciberseguridad.
- Los y las usuarias no solo quieren preocuparse de su propia privacidad, sino que también de la sus familiares y cercanos.
- Las prácticas de ciberseguridad están condicionadas a dos aspectos muy distintos entre sí. Por una parte el privilegio, y por otra parte la opresión.
 - Mientras que la riqueza y la educación ayudan a las personas a acceder a los conocimientos sobre ciberseguridad,
 - las experiencias de abuso/acoso por motivos de identidad de género, raza o sexualidad, provocan que las personas adopten conocimientos en ciberseguridad para protegerse.
- La ciberseguridad es un tema comunitario, ya que las acciones de las personas afectan a su entorno (y viceversa). Debatir estos temas en comunidad, hace que sea más fácil tomar medidas de mitigación en torno a las amenazas.
- El cambio a nivel cultural y legislativo es crucial cuando hablamos de ciberseguridad.

Otro recurso a mencionar es el *Holistic Security Manual* [Technology, 2020] que basa que el entendimiento de la ciberseguridad es un concepto personal, subjetivo y de género. Este manual adopta un enfoque explícitamente holístico de las estrategias de ciberseguridad y la protección de los derechos humanos. ¿Qué quiere decir esto? Que en lugar de considerar la ciberseguridad personal, el bienestar psicosocial y la ciberseguridad organizacional de forma aislada, lo que hace es buscar la manera de integrarlos y destacar su interrelación. De esta manera el manual está diseñado para guiar un proceso de establecimiento o mejora de las estrategias de ciberseguridad para un individuo, colectivos y organizaciones. Se destaca además el hecho de que este manual divide el proceso en cuatro etapas: (1) preparación, (2) exploración, (3) creación de la estrategia y (4) el actuar; de manera que se tiene un proceso evolutivo y cíclico, y que debe ser abordado de forma periódica.

Todo lo mencionado en este capítulo permitió estructurar una propuesta de solución que consideró el diseño centrado en usuarias para diseñar, definir e implementar las políticas y mecanismos de ciberseguridad que fueron utilizados en Aliadas.

CAPÍTULO 3

PROPUESTA DE SOLUCIÓN

Para poder abordar la problemática de determinar y diseñar políticas y mecanismos de ciberseguridad que sean capaces de cubrir las necesidades de las usuarias de Aliadas y el equipo de desarrollo de esta plataforma se propuso aplicar distintos métodos de DCU en combinación con lo planteado por los principales y más reconocidos *frameworks* de ciberseguridad. Sumado a lo anterior, y en orden de poder cumplir con los diferentes objetivos de esta memoria, el proceso de diseño fue dividido en distintas etapas (Ver Figura 15), las que en su conjunto forman un proceso cíclico y cada etapa tuvo actividades claves:

- **Exploración:** Se buscó detectar y determinar aquellas necesidades y condiciones relevantes a la ciberseguridad de las mujeres emprendedoras que serán usuarias de la plataforma Aliadas.
- **Vinculación:** Por un lado se realizó una investigación de tipo comparativa de los actuales *frameworks* de ciberseguridad, y a su vez, se vincularon las necesidades detectadas en la etapa anterior a un plan estratégico de ciberseguridad.
- **Diseño:** Se trabajó con mayor detalle la información recopilada en etapas anteriores, elaborando los documentos formales que darán vida a las políticas y mecanismos de ciberseguridad de Aliadas.
- **Validación:** Se buscó validar aquellas decisiones de las políticas y mecanismos que involucren directamente a las usuarias de la plataforma.
- **Implementación:** Se buscó implementar lo que fue diseñado y validado durante las etapas anteriores, en lo que es considerado una primera versión de las políticas de ciberseguridad y los mecanismos utilizados para aplicarlas.

Si bien la propuesta se planteó como una metodología cíclica para poder iterar con el tiempo sobre este proceso, durante el desarrollo de esta memoria se realizó una sola iteración.

Como nota parte, cabe destacar que dado que durante el desarrollo de esta memoria el mundo se encontraba en el contexto de la *Pandemia de COVID-19*, fue necesario adaptar las actividades a una modalidad remota. Es decir, realizar actividades en donde las usuarias pudieran participar desde la comodidad de sus hogares.

A continuación se detallará lo realizado en cada una de las etapas mencionadas.

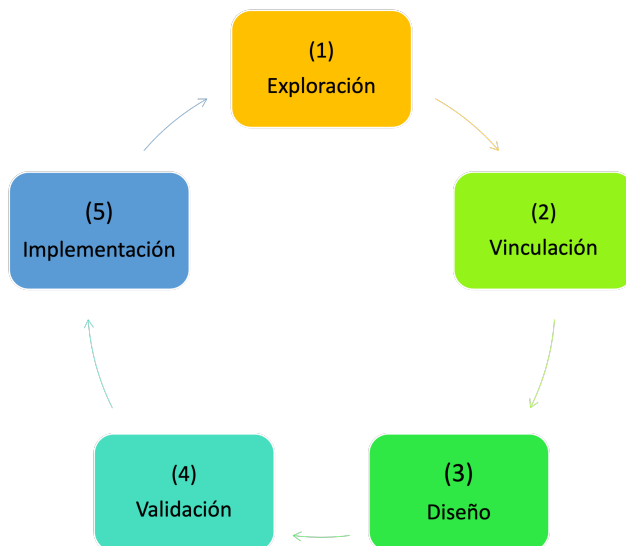


Figura 15: Etapas asociadas al diseño cíclico de políticas y mecanismos de ciberseguridad en la aplicación Aliadas.

Fuente: Elaboración propia.

3.1. EXPLORACIÓN

Esta primera etapa es sin lugar a dudas resulta ser la más importante dentro del desarrollo de esta memoria, puesto que el núcleo del DCU es lograr identificar las necesidades los y las usuarias. En este caso en particular, será explorar las necesidades de las mujeres emprendedoras que resultarán usuarias de la plataforma Aliadas.

Para poder abordar entonces la exploración de las necesidades, esta investigación se apoyó tanto en algunas metodologías del DCU, como también de los planteado por la ciberseguridad feminista. Esto permitió, desarrollar una actividad que sirvió de base para la identificación de las necesidades.

Se desarrolló, de manera remota, un taller denominado 'Modelamiento de amenazas', inspirado en [Slupska y Duckworth, 2021]. El taller consistió en una sesión de trabajo que se dividió en dos partes:

- La primera consistió en discutir con las participantes sobre qué es lo que ellas consideran y perciben como amenazas en el mundo digital y qué es lo que quieren proteger de su vida digital y emprendimientos.
- La segunda consistió en una pequeña sesión de educación digital dónde se presentaron problemáticas relacionadas a cómo construir una contraseña, cómo recordarlas y cómo conocer su fortaleza. El enfoque utilizado fue dar pie a que las participantes pudieran conversar sobre estas enseñanzas sin ser juzgadas.

Dado que el desarrollo de Aliadas se ha fundamentado gran parte en el trabajo centrado en las usuarias, ya habían sido seleccionado grupos de participantes en otras actividades asociadas a otras etapas del desarrollo de la aplicación. Se decidió trabajar con dos de estos grupos, correspondiente a gremios de mujeres emprendedoras de la región de Valparaíso, AGEP-V³³ y Tejiendo Redes³⁴, ya que dada su experiencia en actividades anteriores, fue más fácil adoptar el taller a una modalidad remota.

En la actividad con la asociación AGEP-V participaron 6 emprendedoras, mientras que en la actividad con el gremio Tejiendo Redes participaron tres emprendedoras, aunque solo dos lo hicieron de forma activa durante toda la actividad. La edad de las participantes se encontraba en el rango de +40 años. En cuanto al manejo de las tecnologías, una de las participantes evidenciaba un alto grado de conocimientos, pero el resto acusó tener los conocimientos mínimos necesarios para desenvolverse en el mundo digital.

Para llevar a cabo de manera efectiva esa actividad, y recopilando experiencias aprendidas de otras investigaciones, se tuvieron las siguientes consideraciones:

- Evitar el uso de términos técnicos. Por ejemplo, no se habló de 'ciberseguridad', sino más bien de 'seguridad en la vida digital'.
- Dar ejemplos cuando la pregunta no se entienda. Estos ejemplos fueron determinados previo a la actividad, y se trató de que no fueran tan comunes -para no guiar la actividad hacia esa respuesta- pero sí que pudiera dar a entender de qué se está hablando.
- Llevar la conversación de forma fluida, invitando a participar a todas, y controlando los tiempos de respuesta.

La primera parte del taller buscaba hacer el primer acercamiento de las participantes a la ciberseguridad. Se plantearon las siguientes preguntas abiertas:

- ¿Qué es lo que más deseas proteger de tu identidad digital? ¿Qué es lo que más deseas proteger de tu emprendimiento a nivel digital?
- ¿Qué te hace sentir amenazada en línea? ¿Cuándo fue la última vez que te sentiste así?
- ¿Qué te gustaría mejorar de tu seguridad digital? ¿Qué obstáculos has sentido en ello?

Estas preguntas fueron planteadas de forma abierta a las participantes, y se dieron entre 10 a 15 minutos de conversación en ellas.

³³Más información en <https://agepv.cl>

³⁴Más información en <https://www.facebook.com/TEJIENDO-REDES-203427999732236>

La manera de trabajar estas preguntas fue mediante un *dashboard* colaborativo (Ver Figura 16) en la plataforma Miro.³⁵ Dado que había diversidad entre las participantes, y no se podía predecir el cómo iban a interactuar con esta plataforma, se decidió contar con la ayuda de otros miembros del equipo de Aliadas para hacer la bajada de los temas y conceptos que fueran mencionando las participantes al *dashboard* mediante *post-it*, y así desligarlas de la responsabilidad de anotar lo que piensan, y solo hacerlas conversar del tema.

MODELAMIENTO DE AMENAZAS

Objetivo: Determinar las principales amenazas de nuestra identidad digital y emprendimientos.



Figura 16: Panel en Miro para el taller de 'Modelamiento de amenazas'.

Fuente: Elaboración propia.

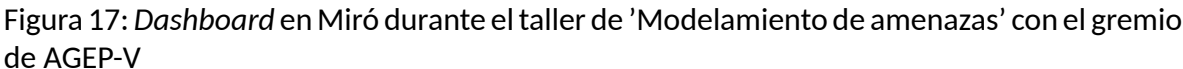
En la Figura 17 se puede ver un ejemplo de cómo a medida que se iba conversando con las participantes respecto a las preguntas, iban saliendo distintas situaciones, acciones y/o conceptos que iban siendo asignados a las respectivas preguntas. Cabe considerar que durante las conversaciones, hubieron conceptos que no caían a primera vista dentro de ninguna de las 3 preguntas, por lo que esos *post-it* fueron dejados a un costado.

Dado que la proporción de participantes entre cada grupo varió de forma notoria, la cantidad de información que pudo ser recopilada resultó ser bastante dispar:

- En la pregunta 1 se obtuvieron 15 *post-it* con la asociación de AGEV-V, en contraste a los 3 que pudieron ser recogidos del gremio Tejiendo Redes (Ver Figura 18).
- En la pregunta 2 esta brecha se tiende a mantener al tener 19 *post-it* versus 6 (Ver Figura 19).

³⁵Miro es una plataforma que permite realizar esquemas, plantillas y diagramas visuales de forma colaborativa mediante una pizarra o tablero digital. <https://miro.com/>

Objetivo: Determinar las principales amenazas de nuestra identidad digital y emprendimientos.



Hay ciertas consideraciones que podrían explicar esta aparente diferencia en la participación, más allá de la cantidad de participantes que hubo en cada grupo. Por una parte, con la asociación AGEV-V se pudo contar con el apoyo de dos personas que fueron anotando los comentarios que hacían las participantes, pero cuando se trabajó con el gremio Tejiendo Redes, se contó con el apoyo de solo una persona. Además es importante agregar que la participante de la asociación AGEV-V con un manejo amplio de las tecnologías, incentivó activamente la participación de las otras participantes.

En la segunda parte se trabajaron aquellos *post-it* que hacían referencia a problemas que suelen ser recurrentes cuando se habla de seguridad digital y otros problemas propuestos. Las problemáticas seleccionadas fueron trabajadas con el apoyo de representaciones gráficas del problema y su solución propuesta.

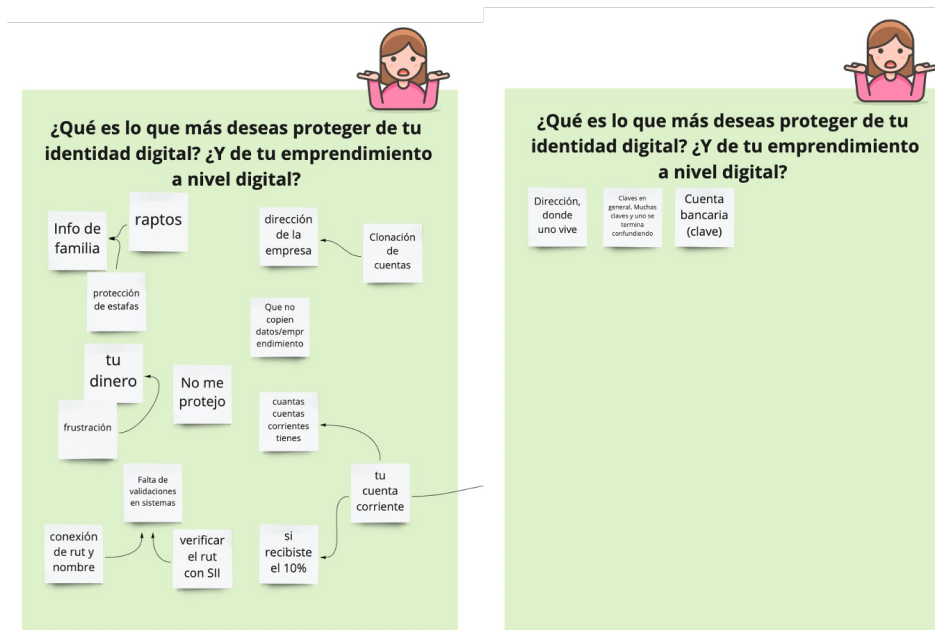


Figura 18: Resultados de AGEP-V (izquierda) y 'Tejiendo Redes' (derecha) para pregunta 1 en taller de 'Modelamiento de amenazas'.

Fuente: Elaboración propia.

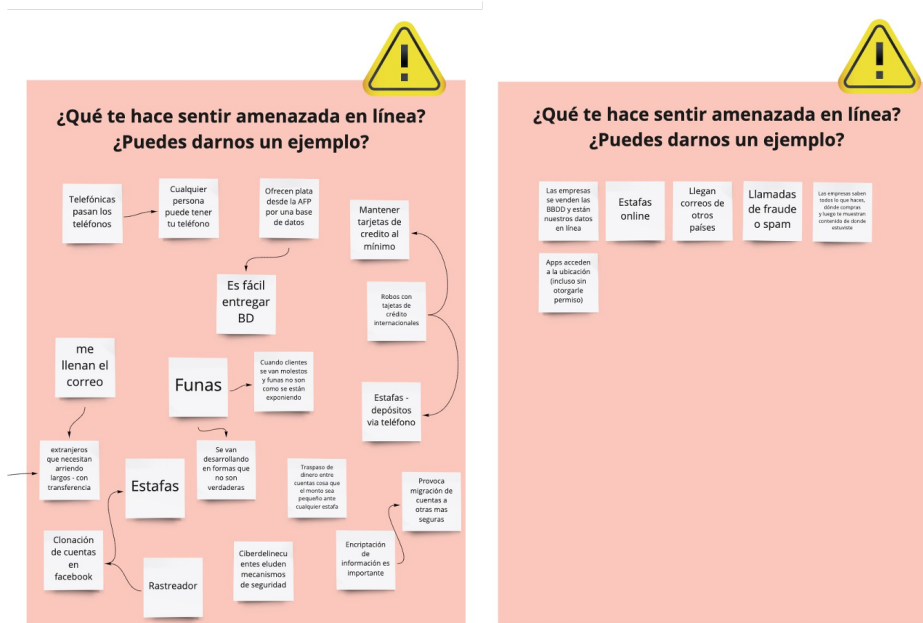


Figura 19: Resultados de AGEP-V (izquierda) y 'Tejiendo Redes' (derecha) para pregunta 2 en taller de 'Modelamiento de amenazas'.

Fuente: Elaboración propia.

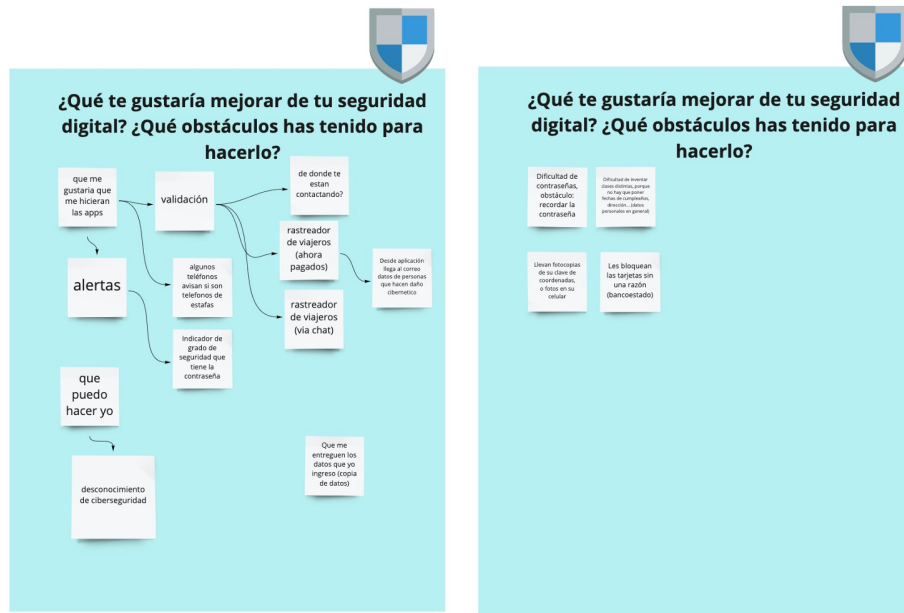


Figura 20: Resultados de AGEP-V (*izquierda*) y 'Tejiendo Redes' (*derecha*) para pregunta 3 en taller de 'Modelamiento de amenazas'.

Fuente: Elaboración propia.

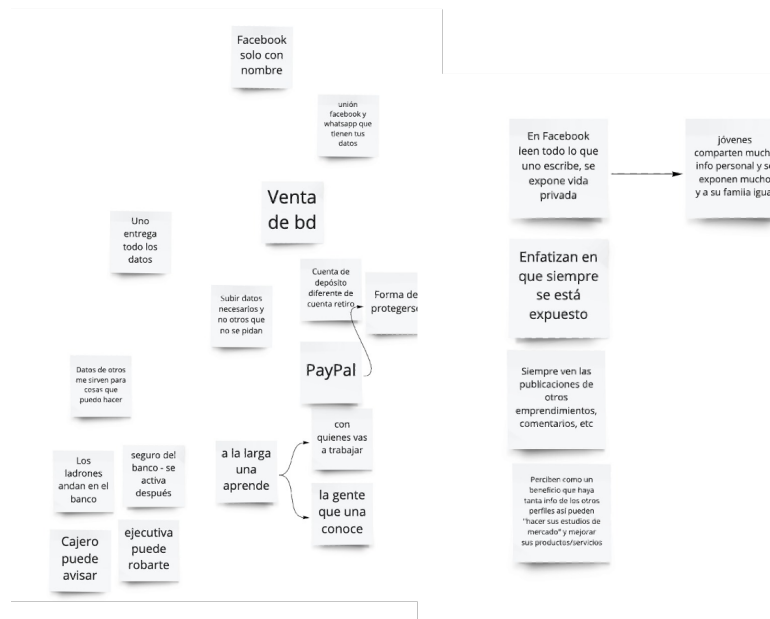


Figura 21: Resultados de AGEP-V (*izquierda*) y 'Tejiendo Redes' (*derecha*) no clasificados en taller de 'Modelamiento de amenazas'.

Fuente: Elaboración propia.

Entre las problemáticas que finalmente fueron abordadas durante la actividad se encuentran:

- **¿Cómo podemos recordar contraseñas?:** Esta fue una problemática que surgió en la discusión, sobre todo considerando que cada vez van apareciendo sitios que tienen distintas exigencias respecto a las contraseñas. Las participantes, casi en su totalidad, mencionaron recurrir a métodos poco seguros como, por ejemplo, anotar en un papel sus contraseñas. Esto llevó a enfocar la conversación en 'Gestores de contraseñas', sin utilizar ese nombre técnico como tal, sino que hablando de aplicaciones o funcionalidades de los dispositivos móviles (principal fuente de trabajo de las emprendedoras), para que pudieran recordar contraseñas de manera segura. La recepción de la recomendación fue bastante positiva, ya que era algo nuevo para ellas (Ver Figura 22.a).
- **¿Cómo hacer una contraseña segura?:** Esta es otra problemática comentada, ya que constantemente se utiliza el concepto de contraseñas fuertes, robustas o seguras, pero muchas veces las personas no saben (porque nunca se les mostró cómo) hacer contraseñas seguras. Como recomendación a este problema, se discutió una técnica que permite la construcción de contraseñas de una manera en que la contraseña pueda ser recordada, pero a la vez sea segura (Ver Figura 22.b).



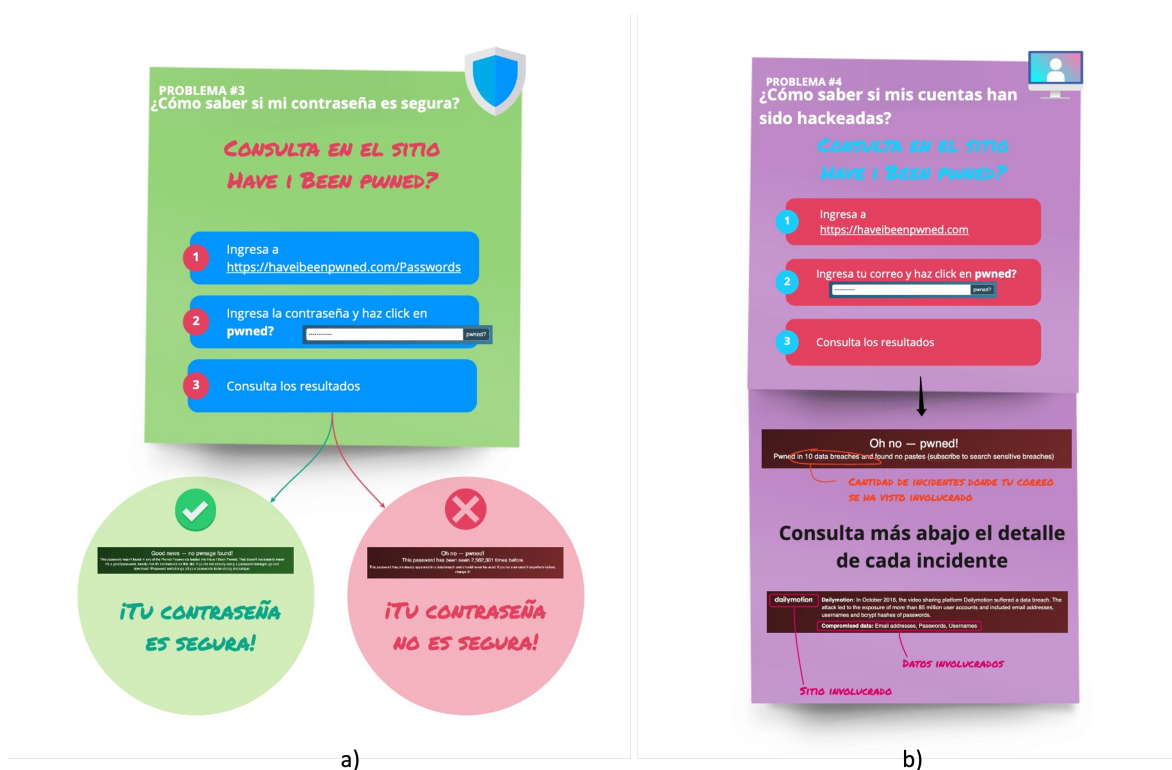
Figura 22: Representación gráfica para abordar las preguntas a) ¿Cómo podemos recordar contraseñas? y b) ¿Cómo hacer una contraseña segura?.

Fuente: Elaboración propia.

- **¿Cómo saber si mi contraseña es segura?:** Esta fue otra de las preguntas que surgió durante la primera parte de la actividad. Si bien existen soluciones muy reconocidas y

validadas en la comunidad para descubrir que tan segura es una contraseña, lamentablemente resultan ser herramientas que se encuentran en inglés, siendo la barrera del idioma un factor importante que provocó que no hubiera buena recogida por parte de las participantes (Figura 23.a).

- **¿Cómo saber si mis cuentas han sido hackeadas?:** A pesar de que este problema no fue explícitamente mencionado por las participantes, si se mostró interés en ellas al ser comentado. La solución propuesta para este problema era basado en la misma herramienta que la pregunta anterior, por lo que ocurrió el mismo problema de baja recepción (Ver Figura 23.b). Si bien se sabía con antelación que esto podía pasar (dado que la actividad primero se realizó con un grupo, y a los días siguientes con el otro), fue imposible encontrar alternativas que cumplieran una función similar en español.



Fuente: Elaboración propia.

Una vez realizada la exploración de las necesidades de las mujeres emprendedoras mediante la realización del taller de 'Modelamiento de amenazas' en dos grupos distintos, lo siguiente fue pasar a la etapa de vinculación.

3.2. VINCULACIÓN

En esta etapa se buscó en una primera instancia hacer un análisis de lo obtenido en la etapa anterior, para luego hacer comparativas frente a lo que plantean los *frameworks* de ciberseguridad tradicionales.

3.2.1. ANÁLISIS DEL RESULTADO DEL TALLER

Mediante el uso de *affinity diagram* sobre los *post-it*, se realizó un análisis sobre la información recopilada durante el taller. Para ello se determinaron las siguientes categorías: (1) Problemática, (2) Datos, (3) Beneficio, (4) Solución, (6) Sentimientos y (7) Hechos. La Figura 24 identifica los colores asignados a cada categoría.

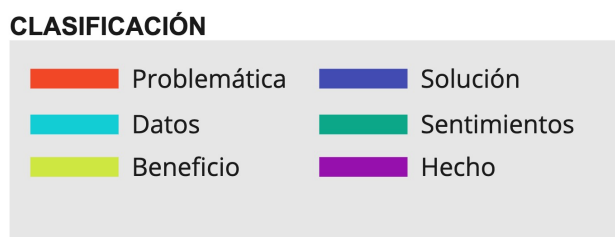


Figura 24: Propuesta de clasificación para los *post-it*.
Fuente: Elaboración propia.

Luego los *post-it* fueron agrupados por la afinidad que tenían entre ellos, dando como resultado la creación de 5 grandes *clusters*: (1) Datos financieros, (2) Datos personales, (3) Datos de emprendimientos, (4) Seguridad Digital y (5) Otros temas.

Ahora bien, el límite entre los *clusters* asociados al término 'dato' no estaba completamente delimitado, puesto que habían ciertos *post-it* que podían caer en incluso las 3 categorías. Dicho esto, la estructura de los *clusters* quedó delimitada como lo evidencia la Figura 25, donde hay una intersección entre los datos personales, financieros y de emprendimientos, mientras que vida digital y otros temas son conjuntos disyuntos.

Al realizar el análisis en la macro-categoría de 'Datos' (Ver Figura 26), se pudo dar cuenta de que las participantes hacía constantemente referencia a sus datos financieros, datos personales, y en menor medida, los datos referente a sus emprendimientos. En más detalles se pudo observar que:

- Cuando las participantes se referían a los datos financieros, mencionaban el tipo de información relacionado al número de cuentas corrientes, saldos contables o si recibiste

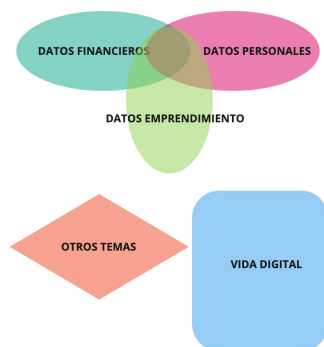


Figura 25: *Clustering* de los *post-it*.
Fuente: Elaboración propia.

el 10 %. ³⁶ Además, al hablar de problemáticas se mencionaba la clonación de cuentas, la venta de bases de datos y estafas. Pero también, algunas de ellas comentaron acciones que pueden ser consideradas para mitigar estos problemas, por ejemplo el uso de intermediarios para pagos, la separación de cuentas personales con la de emprendimientos y la importancia de compartir en internet lo estrictamente necesario.

- Por otra parte, cuando las participantes comentaban sobre datos personales hacían referencia principalmente al tipo de información que era recopilada sobre ellas, como lo son el rut, dirección, información de familiares; y problemáticas que han vivido como la clonación de cuentas y estafas. Así fue como se mencionó en reiteradas ocasiones como nuestra información personal está muy expuesta en las redes sociales, siendo Facebook y Whatsapp las más nombradas. Otro punto necesario de rescatar es la preocupación de las participantes por el cómo las organizaciones se comparten estos datos, y cómo incluso existe la venta de bases de datos con información que era recopilada de ellas.
- Finalmente, cuando se mencionaron los emprendimientos, se pudieron encontrar opiniones divididas; puesto que por una parte algunas participantes valoraban tremendamente el poder de la internet para poder visibilizar sus emprendimientos, mientras otras tenían el temor de que estos pudieran ser plagiados.

También las participantes hablaron de temas relacionados a la 'Vida Digital' y otras temáticas. En la Figura 27 se pueden evidenciar estos resultados. Fueron destacados con color rosa mosqueta aquellos *post-it* que tienen el potencial de transformarse en precursores para puntos importantes dentro de las políticas y mecanismos de ciberseguridad. Si analizamos en más detalles, se puede observar que:

³⁶La crisis económica provocada por la pandemia del COVID-19, llevó al 24 de Julio del 2020 al estado de Chile a promulgar la reforma constitucional que permitió el retiro excepcional del 10 % de los fondos de capitalización individual.

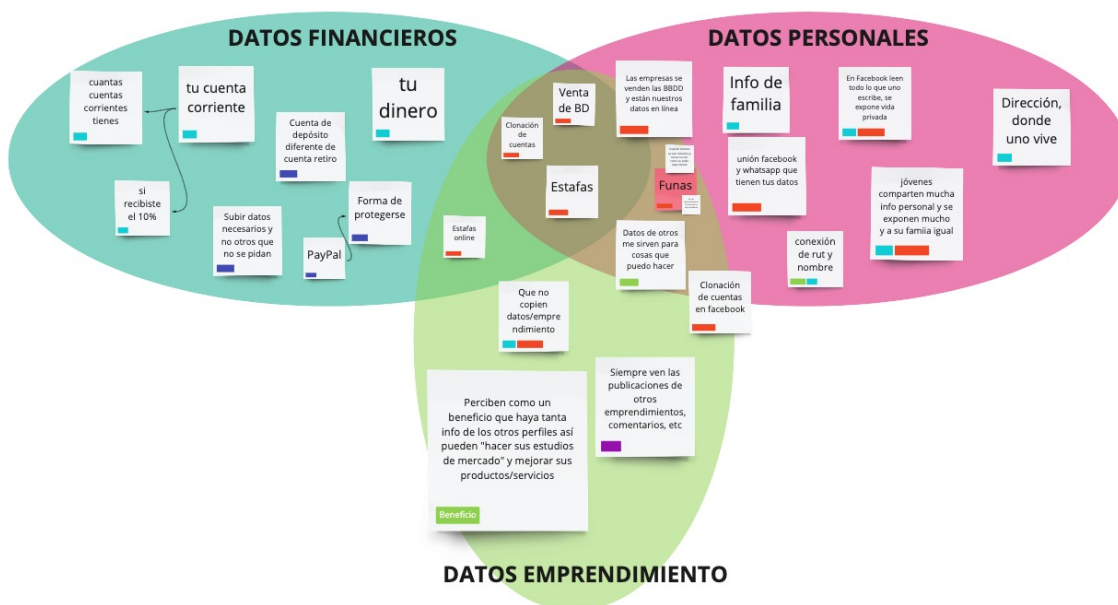


Figura 26: Resultados del *clustering* de 'Datos' y etiquetado de ellos.

Fuente: Elaboración propia.

- En cuanto a las contraseñas, las participantes sentían una dificultad para elaborar contraseñas puesto que las limitaciones dentro de un sitio a otro variaban. Además, estaba conscientes de que no era adecuado poner datos o información personal en sus contraseñas, lo cual dificultaba la labor de memorizarlas. Sumado a lo anterior, también las participantes relataron que muchas veces recurren a llevar sus contraseñas escritas o sacarles fotos con su dispositivo móvil para poder acceder a ellas.
- Existe un temor de las participantes frente a llamadas fraudulentas o correos provenientes de otros países. Fue mencionado que constantemente su casilla de correo se 'llena' de correos no deseados. Algunas durante la actividad mencionaron que no se sienten seguras en identificar la legitimidad de un correo.
- Sumado a lo anterior, las participantes fueron enfáticas en mencionar más de una vez que existe un desconocimiento en lo que respecta a 'seguridad en la vida digital'. Dentro de los sentimientos asociados a esto, se encontró la frustración, puesto que era de su conocimiento que el no protegerse trae como consecuencia quedar 'expuesta'.
- Otro punto mencionado fue la *validación* de las usuarias. Para las participantes, era importante saber que la persona detrás del compromiso de compra efectivamente existe.
- Finalmente, fueron mencionados aspectos muy relacionados a la ciberseguridad como contar con información encriptada, conocer los datos personales que posee una

aplicación, e incluso se mencionó la utilidad de los indicadores del grado de seguridad de una contraseña.

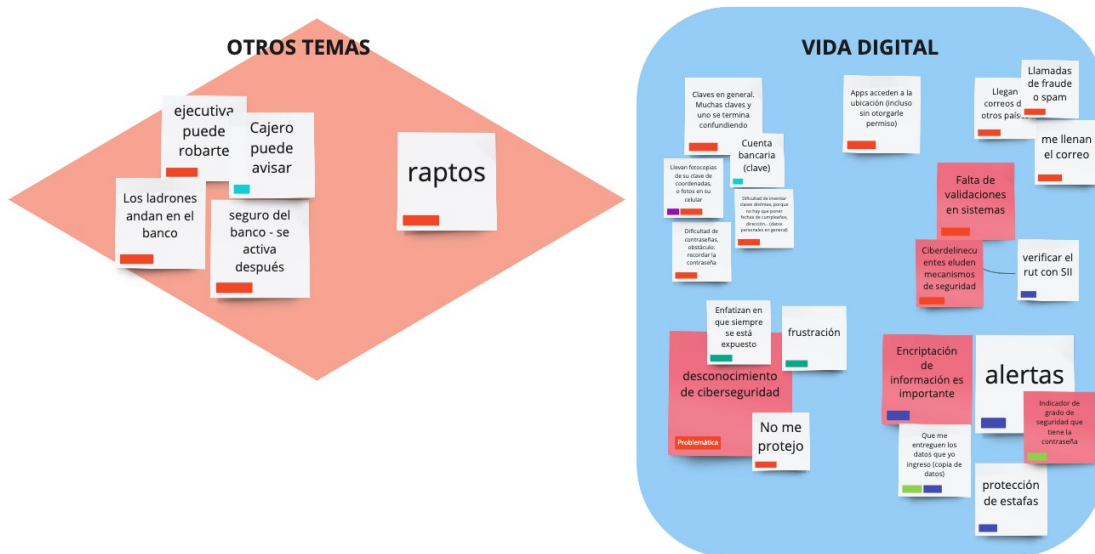


Figura 27: Resultados del *clustering* de 'Vida Digital' y 'Otros temas', y etiquetado de ellos.
Fuente: Elaboración propia.

Luego de haber realizado este análisis, inspirándose en los tres pilares planteados por los controles de CIS, se determinaron tres ejes centrales: (1) Información, (2) Mecanismos y (3) Concientización. Se construyó una *creative matrix* que consideró como eje horizontal estos pilares y como eje vertical los distintos segmentos de usuarias dentro de la organización: (1) Usuarias de la plataforma y (2) equipo de Aliadas. El objetivo de esta actividad era poder gatillar nuevas ideas o aspectos que surgieran al cruzar los ejes y considerar los *post-it* de los *clusters* que fueron clasificados como problemáticas o soluciones (Ver Figura 28).

Dentro de los resultados se obtuvo:

■ Información

- La transparencia en cuanto al uso de la información es un aspecto relevante para las usuarias. En ese sentido tener el poder de visualizar esta información y poder eliminarla es algo que debe ser considerado.
- Debe existir un acceso controlado a la información por parte del equipo de Aliadas, y toda información referente a la aplicación en sí, debe ser compartida por canales seguros.

■ Mecanismos

- Un sistema de alertas, como por ejemplo de ingresos desde un nuevo dispositivo, y validaciones a las usuarias, fueron aspectos que surgieron en este ejercicio.
- En cuanto al equipo de Aliadas, quedan las responsabilidades de implementar mecanismos que puedan proteger la infraestructura. La idea de un WAF se planteó como una potencial solución.

■ Concientización

- Las usuarias de la plataforma desean aumentar sus conocimientos sobre identidad digital y financiera. Una forma de hacerlo es mediante una campaña de educación en las redes sociales de la aplicación y/o la realización de talleres.
- Es importante que dentro del equipo de Aliadas los y las desarrolladoras manejen conceptos de desarrollo seguro, y que todo el equipo tenga conocimientos sobre qué y por qué es importante la ciberseguridad.



Figura 28: *Creative matrix* realizado una vez concluido el análisis de los resultados del taller.
Fuente: Elaboración propia.

Un punto que se repitió constantemente en el taller con las participantes fue el temor de qué y cómo iba a ser utilizada la información que era recopilada de ellas. Varias de las participantes se refirieron a temas como el robo de base de datos, la compartición de información entre terceros y lo expuesta que pueden llegar a quedar. Esto impulsó a desarrollar una actividad enfocada en la transparencia de la información.

3.2.2. TRANSPARENCIA EN LA INFORMACIÓN

Fue necesario vincular las necesidades de las usuarias en cuanto a la protección de sus datos y aquello que era exigido por las plataformas de distribución digital de aplicaciones en donde es distribuida Aliadas (Google Play y App Store) y las plataformas que permiten la vinculación de cuentas para el login (Facebook y Google).

La exigencia principal en la transparencia de datos, de estas cuatro entidades, es contar con una política de privacidad. Por su parte, Facebook tiene ciertas exigencias más críticas que deben ser cumplidas para poder habilitar este tipo de login mediante sus sistemas. Por tanto, fue necesario evidenciar las exigencias solicitadas por Facebook a terceros por el uso de la API proporcionada para el “Inicio de sesión con Facebook”.³⁷

Esto se realizó mediante el análisis del documento titulado ‘Condiciones de la plataforma de Facebook para desarrolladores’,³⁸ en donde se incluyen apartados referente a la protección de datos. Y en la medida de poder ordenar la información obtenida, fue necesario tener en cuenta las siguientes consideraciones respecto al uso de la API:

- **Casos de uso:** El caso de uso evaluado fue el uso de la API para la creación de cuentas.
- **Base de las exigencias:** Como base fundamental, Facebook utiliza el RGPD (Ver en sección 2.4.3) para la elaboración de sus exigencias. Si bien este reglamento opera en la UE y aquellas aplicaciones donde los usuarios sean ciudadanos de la UE, el equipo de Aliadas concluyó que es una buena práctica cubrir los puntos planteados por este reglamento; y en particular aquellos que explícitamente se encuentran en las exigencias de Facebook.
- **Revisión de la aplicación:** Todas las aplicaciones que hagan uso de la API tienen derecho a consultar sin necesidad de ser llamadas a una revisión el perfil público del usuario y/o correo del usuario. Si la aplicación llegara a solicitar otro tipo de permisos, Facebook puede optar por la revisión de la aplicación, la cual para ser aprobada debe adherirse a las condiciones de la plataforma de Facebook y las políticas de desarrolladores.

El análisis de estas exigencias más lo obtenido en la etapa de exploración, derivó en una serie de condiciones que deben fundamentar la política de privacidad de Aliadas. En estas condiciones encontramos:

- Provenientes de la RGDP y participantes del taller
 - Contar con una política de privacidad pública y de fácil acceso

³⁷Recuperado en <https://developers.facebook.com/docs/facebook-login/overview>

³⁸Más información en <https://developers.facebook.com/terms>

- Contar con una política de privacidad transparente en el uso de los datos
- Provenientes de la RGDP
 - Incluir la protección de menores de edad
 - Adoptar la privacidad desde el diseño y la privacidad por defecto
 - Transparentar el tiempo de almacenamiento de los datos

De forma paralela, y considerando los pilares *qué*, *cómo* y *quiénes* (Ver sección 2.4.3), fue posible determinar las tres preguntas en la que posteriormente se fundamentó la política de privacidad de Aliadas. Además, sobre cada una de estas preguntas se desarrolló una lluvia de ideas para encontrar los puntos claves de la política (Ver Figura 29). En cada una de las preguntas se observó:

- **¿Qué información es recolectada por Aliadas?:** Hay dos grandes categorías para la información que es recolectada. Por una parte, los datos que proporcionan las usuarias para la creación de sus cuentas y, por otra parte, la información generada por el uso de la aplicación. En lo último se incluye información relacionada a las interacciones con la plataforma, información sobre tiendas y productos, y la información referente a la vinculación de cuentas.
- **¿Cómo es utilizada la información recolectada?:** Se identificaron procesos del funcionamiento de Aliadas tales como lo son la creación de cuenta/perfil, la creación de tiendas (incluyendo productos), el sistema recomendador y el sistema de colaboración de la aplicación. Estos dos últimos recolectan información para la recomendación de tiendas y productos, y para armar una red de colaboración, respectivamente.
- **¿Con quién se comparte la información recolectada?:** Bajo esta pregunta fue posible identificar tres entidades claves. La misma aplicación de Aliadas, las aplicaciones de terceros con las que eventualmente se podría hacer login y la ANID. Esta última es quien financia la aplicación y quien solicitará datos obtenidos.

Todo lo realizado en las etapas de exploración y vinculación permitieron poder pasar a una etapa de diseño más robusta en dónde se pudo redactar el documento de la primera versión de políticas de ciberseguridad de Aliadas. A la vez, se determinaron aquellos mecanismos de ciberseguridad a implementar.

POLÍTICAS DE PRIVACIDAD



Figura 29: Lluvia de ideas sobre los tres pilares en las 'Políticas de privacidad'.

Fuente: Elaboración propia.

Con toda la información recopilada ya más trabajada y vinculada a las necesidades detectadas, fue posible pasar a la etapa de diseño.

3.3. DISEÑO

Para el diseño de las políticas de ciberseguridad, el primer paso fue recopilar todas aquellas recomendaciones de los *frameworks* de ciberseguridad mencionados en la sección 2.2.3, y que pueden ser aplicados en las circunstancias actuales de Aliadas. De esta recopilación se obtuvo el siguiente listado de recomendaciones:

- **R1 Control de accesos:** Contempla los lineamientos para el control y la gestión de accesos (Obtenido de la ISO 27001 y los Controles de CIS).

- **R2 Aspectos administrativos:** Contempla las asignaciones de responsabilidades relativas a la seguridad de la información (Obtenido de la ISO 27001).
- **R3 Desarrollo seguro:** Contempla las principales directrices para enfocar el desarrollo con una visión de ciberseguridad (Obtenido de ISO 27001).
- **R4 Configuraciones seguras:** Contempla las principales configuraciones de ciberseguridad del hardware y software de equipos y servidores (Obtenido de los Controles de CIS).
- **R5 Postura de ciberseguridad:** Describe la postura y objetivos de la ciberseguridad en la organización (Obtenido de NIST).
- **R6 Política de contraseñas:** Contempla los lineamientos para la construcción y gestión de contraseñas (Obtenido de Controles de CIS).
- **R7 Política de vulnerabilidades:** Contempla la forma en que deben ser gestionadas las vulnerabilidades de código e infraestructura (Obtenida de la ISO 27001).

Paralelamente a la obtención de las recomendaciones, se evaluaron ciertos aspectos claves relacionados al cómo estaba operando el equipo de desarrollo frente a distintas situaciones incluyendo la conexión a los servidores, autenticación en otras plataformas y compartición de documentos. Esto permitió alinear el listado de recomendaciones con las necesidades de las personas pertenecientes al proyecto de Aliadas.

Toda esta investigación permitió determinar la manera en que fue estructurada y que aspectos consideró la política de ciberseguridad de Aliadas.

3.3.1. PROPUESTA DE POLÍTICAS DE CIBERSEGURIDAD

La documentación de la política de ciberseguridad fue organizada en cuatro niveles que van desde lo más general -nivel 1- a lo más específico -nivel 4- (Ver Figura 30), y consideró los siguientes puntos:

- Políticas de ciberseguridad
 - Políticas generales
 - Políticas de control de acceso
 - ◇ Políticas de accesos con privilegios
 - Políticas de acceso remoto
 - Políticas de gestión de credenciales y contraseñas
 - Políticas de uso aceptable de recursos

- Políticas de gestión de vulnerabilidades y parches
- Políticas de desarrollo seguro
- Política de privacidad

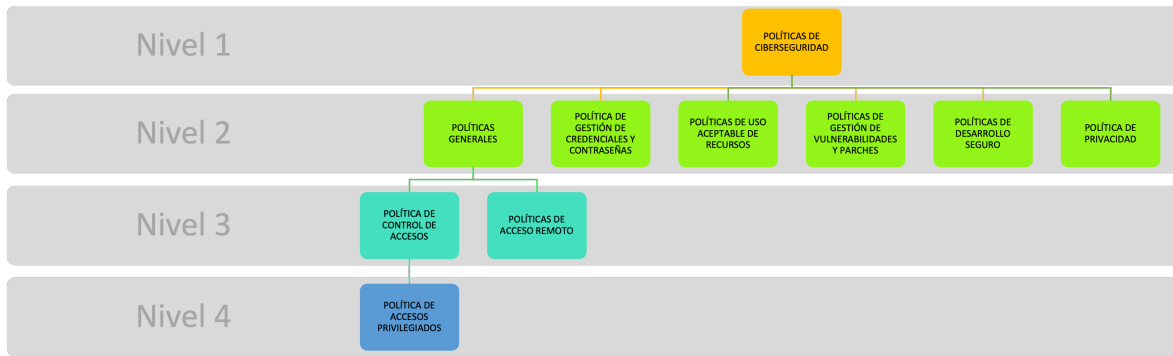


Figura 30: Diagrama de la organización de las "Políticas de ciberseguridad de Aliadas".
Fuente: Elaboración propia.

En la Tabla 3 se puede encontrar a que recomendación, del listado definido al inicio de esta etapa, está asociada la respectiva políticas. Se destaca que la política de privacidad proviene del trabajo previamente realizado en la Sección 3.2.2.

Tabla 3: Políticas de ciberseguridad de Aliadas.
Fuente: Elaboración propia.

Política	Recomendación asociada
Políticas generales	R2 y R5
Política de control de accesos	R1
Política de accesos con privilegios	R1
Política de gestión de credenciales y contraseñas	R6
Políticas de uso aceptable de recursos	R4
Política de gestión de vulnerabilidades y parches	R7
Política de desarrollo seguro	R3
Política de privacidad	-

Para cada política se determinaron los aspectos generales. Varios de estos aspectos también se encuentran definidos en las sub-políticas derivadas del documento principal. Estos aspectos son:

- **Objetivo:** Indica de forma clara la finalidad que tiene el documento dentro de Aliadas.

- **Terminología:** Define palabras que se repiten constantemente en cada política y de las cuáles es necesario alinear las definiciones para que todos y todas entiendan lo mismo.
- **Definiciones:** Son definiciones que deben ser conocidas por las personas consideradas en el alcance de la política.
- **Alcance:** Especifica el alcance que tendrá la política, es decir, aquellas personas a las que estará dirigido.
- **Cumplimiento:** Señala las acciones que serán tomadas si la política es incumplida.
- **Excepciones:** Determinan la manera en que serán agregadas excepciones a la política y bajo que condiciones.
- **Cambios y revisión:** Señalan que es lo que se debe realizar al momento de efectuar cambios en la política y, a su vez, determinan los tiempos en que esta deba ser revisada.

Cabe finalmente destacar que hay ciertas definiciones que deben ser tratadas a nivel organizacional, como los medios de publicación o roles a cargo de esta política. En los casos en dónde no se ha definido de manera formal dichas definiciones, el documento utiliza la etiqueta <> para indicar estas entidades.

3.3.2. POLÍTICA DE CIBERSEGURIDAD

La política de ciberseguridad de Aliadas será descrita por medio de todas las políticas que la componen. En cuanto a los aspectos generales se destaca:

- **Terminología**
 - Debe: El requerimiento al que se refiere es Obligatorio
 - Debería: El requerimiento al que se refiere es Recomendado
 - Puede: El requerimiento al que se refiere es Opcional
- **Definiciones**
 - Confidencialidad: Propiedad de la información de no ser revelada o expuesta a usuarios, procesos o terceros que no han sido autorizados.
 - Integridad: Propiedad de la información en relación a su exactitud y no haber sido modificada, ni alterada por terceros.
 - Disponibilidad: Propiedad de la información de ser accesible y usable bajo demanda por un usuario o proceso autorizado.

- **Activos de Información:** Todos aquellos medios físicos o digitales donde se reciba, almacene, transfiera o se pueda visualizar la información.

■ **Roles y responsabilidades**

- Eventualmente se debería gestionar la creación de un Equipo de Ciberseguridad, cuya función principal debe ser velar por el cumplimiento de esta política, así como asesorar y apoyar a todos los equipos internos de Aliadas.
- Entre algunas de las funciones principales que debería tener este equipo podemos encontrar:
 - Establecer políticas y cumplimientos en conjunto con cada una de las áreas de Aliadas.
 - Implementar medidas y controles de seguridad para proteger la información de usuarios y activos de información de la organización.
 - Liderar, coordinar y ejecutar la respuesta frente a incidentes de seguridad, en conjunto con los procesos de recuperación.
 - Implementar mecanismos de seguridad en concordancia con los lineamientos expuestos en esta política.

En cuanto a cada una de las políticas que componen toda esta documentación, encontramos:

a) Políticas generales

La política general plantea los siguientes aspectos:

- Toda persona perteneciente a la organización interna de Aliadas que identifique alguna vulnerabilidad, brecha de datos o debilidad que ponga en riesgo la seguridad de la organización debe reportarla inmediatamente mediante el canal de #seguridad en el servidor Discord de la organización.
- Se debe proteger la confidencialidad de la información de los usuarios, asignando a cada grupo de usuarios los permisos mínimos necesarios para el correcto funcionamiento de la aplicación.
- El acceso a la información de los usuarios debe estar restringido únicamente a aquellos empleados y colaboradores de Aliadas que necesiten acceder a tales datos para el desempeño de sus funciones y/o para el desarrollo o mejoramiento de la aplicación.
- Se debe impedir el acceso, modificación o divulgación de la información por cualquier entidad no autorizada por Aliadas.

a.1) Políticas de control de accesos

La política de control de accesos plantea los siguientes aspectos:

- **Gestión de accesos:** Los propietarios de los sistemas determinarán el nivel de control de acceso para el sistema y su servicio. Respecto a los diferentes sistemas y servicios:
 - Redes: Se debe controlar el acceso a los servicios de red, tanto internos como externos.
 - Aplicaciones e información: El acceso lógico a las aplicaciones e información debe estar restringido a los usuarios autorizados en función de las necesidades del usuario y siguiendo el principio del mínimo privilegio.
- **Accesos con privilegios:** Toda asignación de accesos privilegiados, que permitan a los usuarios anular los controles del sistema, debe estar debidamente controlados, aprobados por el propietario del sistema y alineados con la política de accesos con privilegios.

a.1.1) Políticas de control de accesos con privilegios

La política de control de accesos con privilegios plantea los siguientes aspectos:

- Todas las cuentas administradas deberían ser inventariadas y sus propietarios validados para ser autorizados.
- Los derechos de acceso con privilegios deben revisarse a intervalos más frecuentes, se recomienda cada 6 meses.
- Los derechos de accesos con privilegios deben ser supervisados para asegurar que no se han concedido privilegios no autorizados.
- Antes de desplegar cualquier dispositivo nuevo, todas las contraseñas por defecto de las aplicaciones, sistemas operativos, routers, firewalls, y otros sistemas, deben cambiarse por una contraseña que cumpla con la Política de gestión de credenciales y contraseñas.
- Las cuentas con accesos privilegiados sólo deben utilizarse para actividades de administración de sistemas.
- Los propietarios de cuentas con accesos privilegiados deben establecer contraseñas únicas y diferentes para sus cuentas con accesos privilegiados y no privilegiados.
- El acceso a las herramientas de scripting (como bash, python, etc) debe limitarse solo a los usuarios administradores o desarrolladores que tengan la real necesidad de acceder a estas capacidades.
- Los sistemas deberían estar configurados de tal manera que permita llevar un registro de cuando una cuenta se añade/elimina, así como también cuando se crean/eliminan nuevos grupos con privilegios administrativos. Además deberían registrar los intentos de inicio de sesión de cuentas administrativas.

a.2) Política de acceso remoto

Esta política contempla que toda persona perteneciente a la organización interna de Aliadas deba evitar conectarse a los servidores de Aliadas por medio de una red de internet pública, poco frecuente o desconocida.

b) Política de gestión de credenciales y contraseñas

La política de gestión de credenciales y contraseñas plantea los siguientes aspectos:

■ Generalidades:

- Todos los usuarios deben proteger las credenciales que les fueron asignadas, y deben garantizar la complejidad de sus contraseñas. Además, los usuarios deben estar conscientes de que todas las credenciales son personales e intransferibles.
- No se debe utilizar los valores predeterminados del proveedor de algún sistema para las contraseñas y/o otros parámetros de seguridad. Lo anterior implica que antes de desplegar cualquier activo nuevo, se deben cambiar las contraseñas que vienen por defecto.
- Todas las contraseñas a nivel de usuario (correo electrónico, computador, aplicaciones, etc), deben ser cambiadas en caso de existir pruebas que confirmen la vulnerabilidad de éstas. Este compromiso debería ser llevado a cabo por el equipo de seguridad.

- **Credenciales de GitHub y Google Drive:** Todos los usuarios que tengan acceso al repositorio Github de Aliadas y/o a los archivos en el Google Drive general del proyecto, deben tener habilitado el doble factor de autenticación siempre y cuando esté disponible la opción.

■ Recomendaciones

- Siguiendo las recomendaciones del NIST, las contraseñas deben seguir lo siguiente:
 - Longitud mínima de ocho caracteres en todos los sistemas
 - Siempre cambiar la contraseña por defecto
 - Cambiar la contraseña si hay evidencia de que hay peligro
 - Omitir sugerencia de contraseñas y preguntas de seguridad basadas en aspectos personales
 - Siempre limitar el número de intentos de autenticación fallidos
 - Al asignar una nueva contraseña, se sugiere comparar esta con un listado de contraseñas conocidas que hayan sido comprometidas.
- Además, debería:
 - Permitirse la función de copiar y pegar en los campos de contraseñas para facilitar el uso de gestores de contraseñas.

- Promover el uso de un gestor de contraseñas o brindar la licencia para la utilización de uno.
- En caso de que un sistema del tipo root, administrador o de servicio, no permita el uso de doble factor de autenticación (u otro método similar), la contraseña utilizada deberá ser de uso exclusivo para ese sistema.

c) Política de uso aceptable de recursos

La política de uso aceptable de recursos plantea los siguientes aspectos:

- Toda persona perteneciente a la organización interna de Aliadas debe dar buen uso a todos los recursos tecnológicos y herramientas que le sean asignados para el desarrollo de sus funciones.
- Toda persona perteneciente a la organización interna de Aliadas debe utilizar su correo electrónico organizacional sólo con fines laborales.

d) Políticas de gestión de vulnerabilidades y parches

Esta política a la fecha se encuentra en estado de borrador pero plantea los siguientes aspectos:

- Se deben realizar escaneos de vulnerabilidad al código al menos trimestralmente o después de cualquier cambio significativo. Dentro de estos resultados, aquellos escaneos que sean calificados como críticos o altos deben ser corregidos, y al terminar se debe volver a realizar un escaneo con el fin de resolver todos los riesgos críticos y altos.
- Se puede definir un protocolo de parcheo para todas las vulnerabilidades o bugs.

e) Políticas de desarrollo seguro

A la fecha, la política de desarrollo seguro se encuentra solo en etapa de investigación puesto que es un documento que debe ser trabajado junto a un desarrollador con experiencia en desarrollo seguro. Lo que si se realizó fue prestar apoyo al equipo de desarrollo, con la elaboración de reportes técnicos cortos referentes a las consultas de seguridad que realizaban los y las desarrolladoras.

f) Políticas de privacidad

Dado que la política de privacidad es un documento que está destinado a ser leído y aceptado por las usuarias de la plataforma, se propuso trabajarlo de manera separada al resto de las políticas. Se optó por tener una primera parte del documento que abarque las políticas de una manera simple y precisa; mientras que una segunda parte que contenga la política de privacidad de forma convencional.

A lo anterior se sumó el hecho de que no fue utilizado un lenguaje formal como el usado en la política de ciberseguridad, sino más bien un lenguaje coloquial que acerque a el o la lectora al documento. También, si bien por una parte se evitó el uso de tecnicismos, se trató de no obviar términos realmente necesarios, con el fin de no caer en indefiniciones.

La primera parte del documento de políticas de privacidad menciona lo siguiente:

■ **¿Qué información es recolectada por Aliadas?**

- La información de registro, para la creación de tu cuenta, es decir, correo electrónico o redes sociales vinculadas.
- La información personal y privada que proveas, como nombre, apellidos, número de teléfono, rut, fecha de nacimiento y/o género.
- (Si eres emprendedora) La información relacionada a tu tienda y productos, como el nombre de la tienda, listado de productos y precio/descripción de ellos.
- Información sobre las interacciones con la aplicación y dispositivo utilizado, incluyendo la información referente a “likes” y opiniones sobre tiendas y/o productos, y comentarios realizados en la aplicación.

■ **¿Cómo es utilizada tu información recolectada?**

- Elaboración de perfiles, para realizar un análisis con los datos vinculados a ti.
- Realizar recomendación de productos, en base a un análisis sobre tus tiendas favoritas y productos adquiridos.
- (Si eres emprendedora) Contribuir al sistema de colaboración entre emprendedoras.
- (Si eres emprendedora) Creación de Tiendas Virtuales, con la información que nos entregues de tu(s) emprendimiento(s).

- **¿Con quién se comparte tu información?** Toda tu información personal, de contacto y de tiendas será utilizada exclusivamente por Aliadas para el funcionamiento de la aplicación. Tendrás control sobre aquellos datos que desees hacer públicos. Toda información utilizada para realizar análisis y estadísticas sobre la plataforma será compartida con ANID (Agencia Nacional de Investigación y Desarrollo de Chile), enfatizando que en este tipo de información no se incluyen tus datos personales y/o privados.

Además de contar con un documento escrito de la política de privacidad, se trabajó un diseño apto para la aplicación junto al diseñador gráfico y una de las desarrolladoras *front-end* de Aliadas. Esto se hizo con el objetivo de quedar alineado y adaptado al diseño de la aplicación. Como resultado se obtuvo el diseño mostrado en la Figura 31.

Finalmente la política de ciberseguridad de Aliadas cuenta con la siguiente documentación:

- Política de ciberseguridad de Aliadas, segunda versión (Anexo A - Sección 5.1)
- Política de control de accesos de Aliadas, primera versión (Anexo B - Sección 5.2)
- Política de accesos con privilegios de Aliadas, primera versión (Anexo C - Sección 5.3)
- Política de gestión de credenciales y contraseñas de Aliadas, primera edición (Anexo D - Sección 5.4)
- Política de gestión de vulnerabilidades y parches, borrador (Anexo E - Sección 5.5)
- Política de privacidad de Aliadas, segunda versión (Anexo F - Sección 5.6)

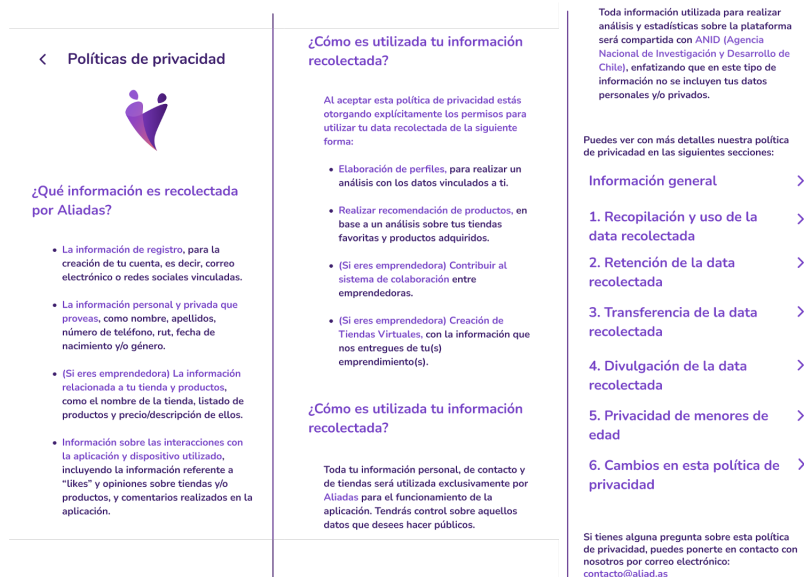


Figura 31: Aspecto en la aplicación de las políticas de privacidad en la aplicación Aliadas.
Fuente: Equipo de Aliadas.

La política de desarrollo seguro no cuenta con documentación oficial pues solo llegó a una etapa de investigación.

3.4. VALIDACIÓN

El siguiente paso involucraba validar con las usuarias las decisiones tomadas en todos los aspectos que las involucraban: la política de privacidad y la creación de contraseñas. Tanto el diseño de la política de privacidad como las interacciones que se pueden realizar con ella en la aplicación y la forma en que esta expresa sus contenidos, fueron validados en una

actividad de *think aloud* con alguna de las participantes que estuvieron en el taller de 'Modelamiento de amenazas'. Las participantes mostraron una actitud positiva frente al resumen de las políticas de privacidad, puesto que al enfrentarse a un texto más reducido no se sentían abrumadas por la lectura y procedían a hacerla. Además agradecieron que el lenguaje no utilizara palabras técnicas de las no tienen conocimiento.

Con todas estas políticas definidas y los aspectos relacionadas a las usuarias validados, se procedió a buscar aquellos mecanismos de ciberseguridad que permitiera la implementación de todos los aspectos que éstas plantean.

3.5. IMPLEMENTACIÓN

Primero se realizó la presentación de ésta al equipo de Aliadas. Esto permitió discutir con los distintos equipos dentro del proyecto de Aliadas, las diferentes alternativas de mecanismos a implementar. Si bien por administrativos es necesario contar con esta documentación escrita tal y cómo se ha presentado en la Sección 3.3.1, se buscó la mejor manera de presentarla al equipo, en vías de seguir con el espíritu de esta memoria que es centrarse en los y las usuarias, siendo las personas pertenecientes a la organización de Aliadas, parte de los y las usuarias de estas políticas de ciberseguridad.

Dicho lo anterior, se utilizó una presentación más dinámica ³⁹ (Ver Figura 32) que abarcó los principales puntos de la política, dejando una invitación a leer la documentación completa. Esto puede ser mejorado con la creación de un vídeo explicativo que permita abordar las políticas de Aliadas.



Figura 32: Capturas de la presentación de las políticas de ciberseguridad de Aliadas realizada en Mayo 2021.

Fuente: Elaboración propia.

³⁹Revisar en https://docs.google.com/presentation/d/14IfLyEhxxUilii6_FYzP_GR_c4gbM8HvOHCI33BwOnY

3.5.1. MECANISMOS DE CIBERSEGURIDAD EN ALIADAS

La elección de los mecanismos de ciberseguridad implementados en Aliadas fue un trabajo realizado junto al equipo de desarrollo de Aliadas y consideró los resultados del análisis del taller de 'Modelamiento de amenazas' (Ver Sección 3.2.1).

Dado que las políticas generales contemplan e incluyen las políticas referente a controles de acceso, acceso remoto y accesos privilegiados, es que se tomará como un conjunto y se hablará de los mecanismos para el **control de accesos**. Estos mecanismos incluyen:

- Sólo los puertos realmente necesarios para el funcionamiento de Aliadas han sido habilitados.
- El acceso a los servidores es mediante el protocolo SSH con la utilización de llaves SSH. Esta llave consisten en un par de claves RSA que son protegidas mediante una contraseña.
- El acceso acceso vía SSH al usuario *root* ha sido restringido solo a las personas que realmente necesitan de este.

Otro de los mecanismos seleccionados para **proteger la infraestructura de Aliadas** fue la implementación de un *Web Application Firewall* (WAF). Este tipo de *firewall* supervisa, filtra y/o bloquea todo el tráfico HTTP hacia y desde una aplicación web. Al poder inspeccionar el tráfico HTTP, el WAF es capaz de proteger a la aplicación de ataques como los de inyecciones SQL, XSS, CSRF, etc. Junto al encargado de infraestructura de Aliadas, luego de una investigación de distintas alternativas, se seleccionó e implementó el proyecto *open-source* ModSecurity⁴⁰ debido a que:

- Es compatible con nginx, teniendo una implementación relativamente sencilla de realizar.
- Es de código abierto y mantenido por una comunidad muy activa.
- La fundación OWASP proporciona un set de reglas específico para ModSecurity que busca la detección de los ataques más comunes.⁴¹

Al momento de la implementación del WAF la aplicación de Aliadas se encontraba en desarrollo. Para no interrumpir este desarrollo, el WAF quedó en modo de simulación. Esto quiere decir no bloquea el tráfico, pero si deja logs en un archivo, registrando el bloqueo simulado, su motivo y todos los datos relacionado. Esto ha permitido ir ajustando las distintas configuraciones del WAF en la medida de que su implementación no afecte el funcionamiento de la aplicación.

⁴⁰Más información en <https://modsecurity.org>

⁴¹Más información en <https://owasp.org/www-project-modsecurity-core-rule-set/>

En cuanto al **manejo de vulnerabilidades** que puedan existir en el código de la aplicación (aspectos contemplados en la política de gestión de vulnerabilidades), se ha determinado como mecanismo de escaneo para la detección de vulnerabilidades, en base a las necesidades de los y las desarrolladoras, la plataforma *snyk*.⁴² Al ser una plataforma *open-source*, esta puede ser adoptada sin mayores problemas.

La herramienta permite realizar un escaneo del código que se encuentra en un repositorio. Además de proporcionar la severidad de las vulnerabilidades encontradas, entrega información suficiente para determinar si ésta aplica para Aliadas, y así tomar la mejor medida para mitigarla. Dado que *snyk* se puede integrar a Github,⁴³ la herramienta da la sugerencia del PR⁴⁴ que puede mitigar la vulnerabilidad.

Para adaptar a los y las desarrolladoras de Aliadas a *snyk*, se elaboró una guía en Miro. Esta guía fue elaborada de manera tal que no sea percibida como una documentación formal de la herramienta, sino más bien un paso a paso de aquellas acciones que son realmente necesarias para los y las desarrolladoras.⁴⁵

En cuanto a la **gestión de contraseñas**, se utilizaron los siguientes mecanismos dentro de la aplicación:

- La creación de contraseñas tiene la condición de un mínimo de 10 caracteres, un número y una mayúscula. Además, la interfaz indica si estas condiciones no se cumplen.
- Al solicitar la recuperación de contraseñas, se ha anonimizado el correo de la usuaria.

Además quedó desarrollada una propuesta para poder evaluar si las contraseñas que son definidas por las usuarias, al momento de registrarse en la aplicación, por medio de la API de *Have i been pwned?*.⁴⁶ Esta API permite consultar si una contraseña ha sido previamente expuesta en alguna brecha de datos. Para realizar la consulta se debe enviar el hash SHA-1 de la contraseña.

3.5.2. ESTRATEGIA DE CONCIENTIZACIÓN

De las etapas anteriores también se identificó la necesidad de las usuarias de poder aprender más sobre seguridad en su vida digital. Frente a ello, y sumándose a la campaña de redes sociales realizada por el equipo de marketing de Aliadas, es que se diseñaron una serie de publicaciones junto al equipo de diseño de Aliadas.

⁴²Más información en <https://snyk.io>

⁴³Más información en <https://github.com>

⁴⁴En Github, un PR o *pull-request* es la acción de validar un código que se va a *mergear* de una rama a otra.

⁴⁵Link a la guía: https://miro.com/app/board/o9J_INgu4Po=/ Password: 7C270iHpZS* &

⁴⁶Más información en <https://haveibeenpwned.com/API/v2>

Estas publicaciones se elaboraron en base a los puntos de interés de las participantes del taller de "Modelamiento de amenazas", y el cómo reaccionaron frente a los prototipos presentados en dicha actividad.

En las Figuras 33 y 34 se pueden encontrar aquellas publicaciones que ya fueron aprobadas por el equipo de diseño y marketing, y están próximas o ya fueron publicadas en las redes sociales de Aliadas.



Figura 33: Capturas de las publicaciones de la estrategia de concientización (Parte I)
Fuente: Equipo de Aliadas.



Figura 34: Capturas de las publicaciones de la estrategia de concientización (Parte II).
Fuente: Equipo de Aliadas.

CAPÍTULO 4

VALIDACIÓN DE LA SOLUCIÓN

Dado que lo que se quiere evaluar es si las políticas y mecanismos de ciberseguridad de Aliadas fueron efectivamente creadas considerando las necesidades de las usuarias y no basándose en su totalidad en los *frameworks* de ciberseguridad estudiados, es que se ha propuesto como forma de validación el realizar una comparativa entre las políticas establecidas, el mecanismo implementado y si estos provienen de las necesidades de las usuarias.

4.1. VALIDACIÓN DE POLÍTICAS Y MECANISMOS DE CIBERSEGURIDAD

La primera etapa de esta validación consistió en listar los puntos principales de las políticas y los mecanismos establecidos para aplicarla. En ese sentido, la política de privacidad se continuará trabajando de forma separada puesto que involucra otro tipo de validación.

El listado de los principales puntos de políticas y mecanismos queda de la siguiente manera:

- 1 La identificación de vulnerabilidades, brechas de datos o debilidad debe ser reportada (política). Para ello se implementó el canal de #security en Discord como canal de comunicación directo (mecanismo).
- 2 Se debe proteger la confidencialidad y disponibilidad de la información (política). Para ello se implementó ModSecurity como WAF (mecanismo).
- 3 El acceso a la información debe estar restringido a aquellos que necesitan acceder a tales datos para el desempeño de sus funciones (política). Para ello se verificaron las configuraciones de seguridad de las distintas plataformas que contienen información de Aliadas (mecanismo).
- 4 Se debe impedir el acceso no autorizado a la infraestructura de Aliadas (política). Para ello en los servidores de Aliadas se habilitaron sólo los puertos necesarios para su funcionamiento (mecanismo).
- 5 La asignación de accesos privilegiados debe estar debidamente controlado (política). Para ello se deshabilitó el acceso al usuario root por defecto, siendo este asignado solo a quienes necesiten (mecanismo).
- 6 Las personas pertenecientes a Aliadas deben proteger las credenciales que le fueron asignadas (política). No hay un mecanismo como tal para ello, más que la concientización de hacerlo al momento de presentar las políticas.

- 7 Los usuarios con acceso al repositorio Github y/o los archivos en el Google Drive de Aliadas deben tener habilitado el 2FA (política). No hay un mecanismo como tal para ello, más que la concientización de hacerlo al momento de presentar las políticas.
- 8 Las personas pertenecientes a Aliadas deben dar buen uso de los recursos (política). Para ello se realizó la verificación de las configuraciones de seguridad de los recursos (mecanismo).
- 9 Las personas pertenecientes a Aliadas deberán evitar conectarse a los servidores de Aliadas desde redes públicas y/o desconocidas. No hay un mecanismo como tal para ello, más que la concientización de hacerlo al momento de presentar las políticas.
- 10 Se deben realizar escaneos de vulnerabilidades al código fuente de la aplicación (política). Se fomentó el uso de snyk por parte de los y las desarrolladoras (mecanismo).

Al analizar estos puntos se determinó que:

- La política y mecanismo del punto 1 surge desde la necesidad del equipo de Aliadas de tener un canal abierto desde donde poder plantear consultas sobre ciberseguridad.
- La política del punto 2 proviene de las recomendaciones de los *frameworks* estudiados, pero el método aplicado surgió trabajando junto al equipo de infraestructura de Aliadas.
- Las políticas del punto 3 y 8 proviene de las recomendaciones de los *frameworks* estudiados, pero el método aplicado surgió al conversar con miembros del equipo de Aliadas y ayudarlos a configurar permisos en estas plataformas.
- Las políticas y mecanismos del punto 4 y 5 surge de la necesidad del equipo de infraestructura de Aliadas.
- Las políticas de los puntos 6, 7 y 9 provienen de los *frameworks* estudiados.
- La política del punto 10 proviene de las recomendaciones de los *frameworks* estudiados, pero el método aplicado surgió trabajando junto al equipo de Aliadas.

Lo que pudo ser resumido en que el 60 % de las políticas de ciberseguridad, sin considerar la de privacidad, provienen de los *frameworks* estudiados, en contraste con un 40 % que pudo ser determinado a partir de las necesidades del equipo (Ver Figura 35.a). Por otra parte la totalidad de los mecanismos seleccionados fue gracias al trabajo en conjunto con los distintos equipos de Aliadas (Ver Figura 35.b).

Otro punto interesante que pudo ser abordado, pero que quedó fuera del alcance de esta memoria, por temas de cantidad de esfuerzo requerido, es la implementación de un sistema que permitiera comprobar el cumplimiento de las políticas de ciberseguridad de Aliadas.

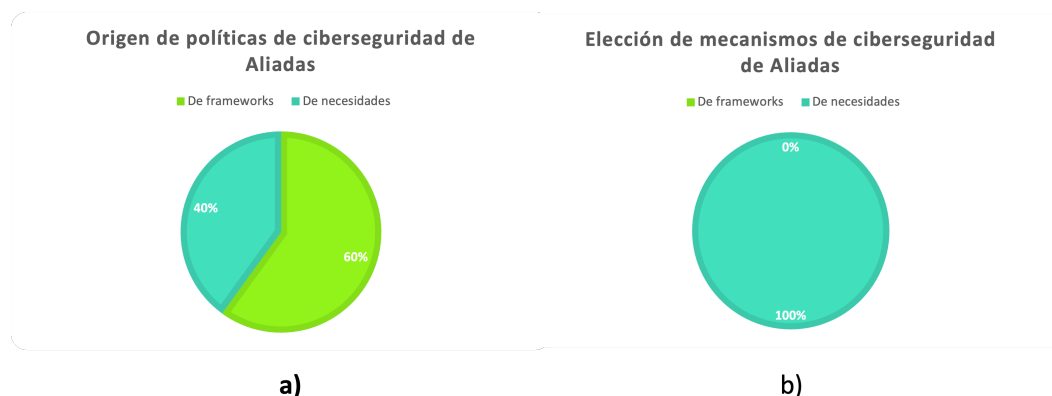


Figura 35: (a) Origen de políticas de ciberseguridad de Aliadas y (b) elección de mecanismo de ciberseguridad

Fuente: Elaboración propia.

Al poder evaluar el nivel de cumplimiento de una política, puede determinar si el método utilizado para crearla fue acertado o no. Para esto sería necesario tener un equipo 100 % dedicado a esta tarea, lo que no siempre es fácil de lograr.

Finalmente, la política de privacidad de Aliadas se trabajó de forma separada a las otras políticas de ciberseguridad y, por tanto, su validación difiere a la de estas, y tal como se mencionó en la Sección 3.4 esta validación se trabajó junto a las mismas usuarias. Las reacciones a esta política frente a aspectos como su visualización y entendimiento resultaron ser bastantes positivas, dando cuenta que el enfoque utilizado fue acertado.

Se podría evaluar el nivel de implementación de esta política en comparación a lo que plantea la RGDP y así validar que tan efectiva es, pero dado que fue este mismo reglamento el que fue utilizado junto a los resultados del taller, los puntos para elaborar la política de privacidad, que no tendría sentido hacerlo de esta manera.

4.2. VALIDACIÓN DE ESTRATEGIA DE CONCIENTIZACIÓN

La estrategia de concientización fue validada a nivel del impacto que tiene ésta sobre los y las usuarias en las redes sociales de Aliadas. Para este análisis, se puso foco en el Instagram de Aliadas, debido a que sin lugar a dudas resulta ser la red social con mayor actividad de la plataforma.

De un total de 47 publicaciones, donde solo se consideraron las del tipo "Publicación de muro" y "Reel", se pudo evidenciar cómo se han comportado los *likes* en cada una de estas publicaciones. Para efectos prácticos, las publicaciones relacionadas a esta estrategia han sido marcadas con color rojo, siendo tres en total hasta la fecha (Ver Figura 36).

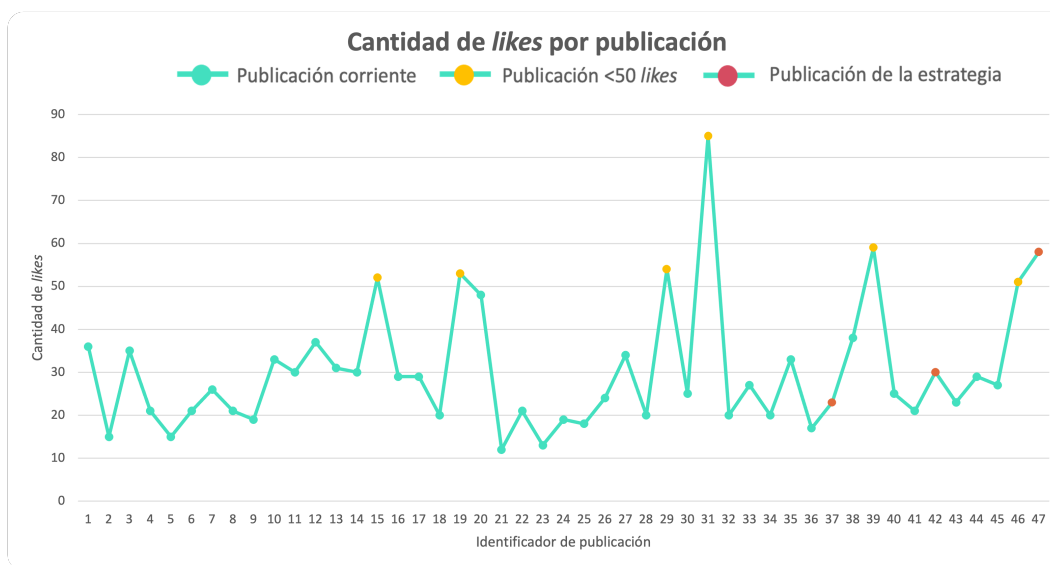


Figura 36: Gráfico de cantidad de *likes* por publicación

Fuente: Elaboración propia.

Se decidieron omitir aquellas publicaciones del tipo "Video de IGTV", ya que el tipo de interacción que se realiza con ellas es diferente a la que ocurre con las otras publicaciones. Esto se debe a que son videos de larga duración que no suelen registrar *likes*, sino más bien la cantidad de reproducciones, por ende, comparar estos ambos aspectos no tiene mucho sentido.

Dentro de los hallazgos se encontró que existe un promedio de 30 *likes* por publicación, y que los *peaks* de *likes* están asociados a hitos importantes de Aliadas, como lo son las últimas sesiones de co-diseño, el lanzamiento de la aplicación en la *App Store* y *Google Play*, el lanzamiento oficial, una nota en el periódico, etc. Por su parte, aquellas publicaciones relacionadas a la estrategia de concientización muestran cómo fueron aumentando su cantidad de *likes*, encontrando incluso que la última publicación esté dentro del *top 3* de publicaciones con más interacciones. Además, cabe señalar, que al momento de capturar estos datos, la última publicación tan solo llevaba 17 horas de ser publicada.

No ha pasado mucho tiempo para evaluar cuál es el impacto que ha tenido esta estrategia, puesto que las publicaciones sobre cuidado de la vida digital comenzaron a ser publicadas a fines de Julio, pero si se ha podido evidenciar una recepción positiva por parte de los y las usuarias, e intenciones de querer saber más.

Esta misma recepción positiva que han tenido las publicaciones llevó al equipo de marketing a solicitar la creación de un taller, sobre seguridad digital, abierto para toda la comunidad de Aliadas. Dicho taller ha quedado fuera del alcance de esta memoria ya que se llevará a cabo en un tiempo más.

CAPÍTULO 5

CONCLUSIONES

Muchos de los aspectos de nuestro diario vivir se han relacionado a las tecnologías de información con el pasar del tiempo; y junto a todos aquellos acontecimientos que han ido acelerando la transformación digital, es lógico pensar en la llegada de múltiples soluciones tecnológicas frente a los problemas sociales. Es así como Aliadas entra al mercado de las plataformas digitales, buscando fomentar los emprendimientos y microemprendimientos de mujeres y así crear una red de apoyo entre ellas.

Pero lo cierto es que cualquier plataforma que participe con el mundo digital va a estar expuesta de alguna u otra manera a ciberdelinquentes, quienes ven en la información y/o la reputación de una organización, la oportunidad de poder hacer daño y beneficiarse de distintas maneras. Frente a lo anterior, sin lugar a dudas, la ciberseguridad se planta como uno de los pilares a la hora de desarrollar soluciones digitales. Este concepto no solo se abarca desde la perspectiva del desarrollo de una plataforma, sino también en como se constituye la organización que está detrás de este desarrollo.

Ahora, si bien las regulaciones en Chile no obligan legalmente a las organizaciones a cumplir ciertos estándares, si se puede estar de acuerdo en que la implementación de políticas y mecanismos de ciberseguridad es, sin lugar a dudas, la forma más eficaz de proteger los activos de la organización, y por ende, la información en ellos. Además, actualmente se está consciente de la necesidad de estas implementaciones, aunque no exista como tal una obligación legal de hacerlo.

Cuando se habla de políticas y mecanismos de ciberseguridad debe existir un compromiso por parte de todos los involucrados en el proceso de implementación y mantenimiento de éstos. Eso implica que la ciberseguridad no debe ser tratada como algo aparte, sino más bien como un todo que involucre a toda la organización.

No cabe duda de que la existencia de distintos *frameworks*, controles y reglamentos, ayudan enormemente en la implementación de estas estrategias, pero a su vez estos resultan bastante genéricos y no siempre se adaptan a las organizaciones de la mejor manera. Además, éstas dependen en gran medida del recurso humano, por lo que están muy propensas a fracasar si no se realizan con el enfoque adecuado. Bajo las consideraciones anteriores, resulta lógico pensar entonces en un enfoque que pueda centrarse en las personas y no sólo en los sistemas.

Es así, como en el desarrollo de esta memoria se encontró una corriente de la ciberseguridad que se alinean con esta búsqueda. El enfoque feminista de la ciberseguridad busca poder comprender de mejor manera las amenazas que enfrentan las personas en el mundo digital y las barreras que les impiden acceder o actuar con un foco en la ciberseguridad.

Además, está la existencia de un enfoque de diseño que busca soluciones que puedan resolver las necesidades de los y las usuarias, consiguiendo una mayor satisfacción y una mejor experiencia de uso; lo que se conoció a lo largo de esta memoria como el DCU. Dado que este enfoque comparte lineamientos con el enfoque feminista, se utilizaron como base para la búsqueda del diseño centrado en usuarias de las políticas y mecanismos de ciberseguridad de la plataforma Aliadas.

Para ello se planteó una modalidad de trabajo que abarca cinco etapas claves: exploración de necesidades, vinculación de necesidades, diseño de la propuesta, validación de la propuesta e implementación de la propuesta. Estas etapas planteadas se alinean con el modelo cíclico de etapas que plantea el DCU. Es imposible entonces no mencionar lo favorable que podría ser el haber planteado un modelo cíclico que permita, en un futuro, ir mejorando en cada iteración que se haga sobre él. Y aunque si bien este ciclo es mucho más largo (en tiempo), si se compara por ejemplo con los ciclos típicos de desarrollo de software, si permite ir manteniendo políticas y mecanismos actualizadas.

En cuanto a la etapa de exploración, el poder elaborar una dinámica colaborativa con las usuarias de la plataforma resultó en una experiencia bastante enriquecedora, y no sólo desde el punto de vista de poder buscar y sentar las bases de lo que posteriormente se transformaría en las políticas y mecanismos de ciberseguridad, sino que también en poder acercar el concepto de ciberseguridad a las usuarias. Resultó interesante comprender que existe mucho entusiasmo por aprender sobre ciberseguridad, pero resulta que son justamente los términos técnicos como "ciberseguridad" los que causan temor y terminan alejando a las personas de ello. Esto derivó en la búsqueda de nuevas palabras que pudieran sentirse más familiares por parte de las usuarias, como lo son hablar de vida digital y seguridad digital.

Bajo esa perspectiva la adaptación del lenguaje utilizado durante las actividades, a uno que pueda sentirse "cercano", provocó una mejor participación de las usuarias, quienes se mostraron entusiastas en hablar sobre temas a los que no se habían visto enfrentadas en otras ocasiones. Muchas de las participantes señalaron que no les era fácil acatar todas las normas de seguridad que usualmente encontraban en aplicaciones, puesto que estas resultaban engorrosas e incluso no entendían el por qué de muchas de ellas. En consecuencia, durante la actividad surgieron numerosas ideas que sirvieron como impulso para mejorar la seguridad de Aliadas a través del diseño.

Además, se pudo detectar entre las participantes la existencia de tres grandes categorías para el tipo de dato/información que sienten que es importante: datos bancarios, datos personales y datos de emprendimientos, siendo el primero el que consideran como más relevante, pero el que menos preparadas se sienten para defender. En ese sentido, este descubrimiento permitió determinar los lineamientos principales a tener en la estrategia de concientización sobre vida digital que se comenzó a llevar a cabo en las redes sociales de Aliadas. Un punto importante a destacar en ese sentido, es que tanto la campaña de marketing de Aliadas, como esta campaña de educación digital, se alinean en la búsqueda de un espacio social y de apoyo donde las usuarias puedan colaborar y así mejorar sobre sus prácticas digitales ya sea que se esté hablando de mejorar las prácticas sobre sus emprendimientos, o derechamente

sobre su vida digital. Este proceso colaborativo nos permite concluir que es factible hablar de ciberseguridad como práctica comunitaria, donde las personas puedan protegerse mediante la reflexión y la acción; y donde las organizaciones puedan construir estrategias de ciberseguridad centrándose en las necesidades de sus usuarios y usuarias.

En cuanto a la etapa de vinculación, los métodos de DCU que fueron utilizados permitieron un mejor análisis de los datos obtenidos, mediante la creación de *clusters* que delimitaban la información en distintos aspectos. Además de ello, la idea de categorizar los hallazgos en distintos tipos de eventos, permitió determinar de mejor manera las problemáticas, sentimientos asociados, beneficios y potenciales soluciones cuando se hablaba de seguridad digital. Esta clusterización permitió determinar los criterios de información, mecanismos y concientización, que junto con las recomendaciones, aplicables para Aliadas, de los *frameworks* de ciberseguridad estudiados, permitieron determinar los lineamientos que siguieron las políticas de ciberseguridad, y la elección de los mecanismos para implementar estas políticas.

Cabe destacar que fue importante separar el trabajo realizado en dos grandes focos: las políticas de ciberseguridad como tal, y la política de privacidad. Esta separación fue positiva dado que las políticas de ciberseguridad tienen estrecha relación con la organización y las personas que trabajan en ella, mientras que la política de privacidad es un documento que está dirigido a los y las usuarias de la plataforma.

Al hablar de políticas de privacidad, utilizar el enfoque de "etiquetado nutricional" trajo como consecuencia la creación de una política de privacidad cercana a las usuarias y también una política que no es agobiante de leer. El responder las preguntas ¿qué información es recolectada por Aliadas? ¿cómo es utilizada la información recolectada? y ¿con quién es compartida esta información recolectada? permitió definir una política precisa. Algo sumamente positivo de es que al ser validada con las usuarias, esta política se caracterizó por ser percibida por las usuarias como una política que entregaba confianza y transparencia en cuanto al uso de los datos de ellas.

La validación de la solución propuesta evidenció que es muy difícil poder estructurar el documento de una política de ciberseguridad sin la ayuda de un *framework*, pero no así ocurre con los mecanismos de ciberseguridad, en donde su elección puede estar apoyada en las necesidades del equipo. Si bien esta memoria enfocó el trabajo realizado en las usuarias de la aplicación, queda la crítica de haber puesto más énfasis en el equipo de Aliadas. Quizás el mismo taller de "Modelamiento de amenazas" se debió haber llevado a cabo con las personas pertenecientes a la organización dándole un enfoque más técnico.

En cuanto a la validación de la política de privacidad, al realizarla mediante una actividad colaborativa con las usuarias de la plataforma, se pudo validar tanto el prototipo que eventualmente pasó a la aplicación, como también la calidad del contenido de la política. Es sumamente importante validar con las usuarias aquellos aspectos que están directamente relacionadas con ellas, pues es la única manera de determinar aquellas mejoras que pueden ser incluidas en futuras versiones, y aquellos aspectos que no están funcionando, los que en

ciberseguridad, se pueden traducir a brechas que puedan ser aprovechadas por ciberdelincuentes.

Por su parte, la estrategia de concientización con las usuarias de la plataforma tiene un buen pronóstico, lo que permite concluir que el acercar los conceptos de ciberseguridad a un lenguaje entendible logra que las personas no se sientan intimidadas por él; algo incluso se evidenció en todas las actividades colaborativas que se tuvieron.

Finalmente, y aunque no fue tema central de esta memoria, recalcar que al analizar el panorama regulatorio de la ciberseguridad en Chile, se puede apreciar que urge que tanto el poder Ejecutivo como el Legislativo, tomen medidas que busquen mejorar el estándar de las obligaciones que deben tener las organizaciones frente a la seguridad de sus activos informáticos, y más importante aún, frente a la información de los y las usuarias que se ven involucradas. Si bien en la actualidad rigen ciertas leyes relacionadas a estos aspectos (la Ley 19.223 de delitos informáticos, y la Ley 19.628 de protección de datos), al leerlas se puede concluir que son leyes que se encuentran muy desactualizadas y con una gran cantidad de indefiniciones, lo que provoca que sea muy fácil caer en vacíos legales, que le permite a las organizaciones escapar de sus responsabilidades con respecto a la seguridad de sus activos informáticos. Es necesario seguir avanzando en la tramitación y promulgación de las iniciativas legales que buscan solucionar el problema que tienen las leyes actuales. Por una parte, está la nueva ley de delitos informáticos que busca adecuarse a lo que plantea el Convenio de Budapest, y por otro lado, se tiene la nueva ley de protección de datos, que se acerca mucho más al estándar RGDP, estándar reconocido mundialmente como uno de los más estrictos en cuanto a la protección de datos. Ambas iniciativas resultan entonces sumamente relevantes si se quiere alinear la ciberseguridad del país con una infraestructura que proteja adecuadamente la información de las personas.

5.1. DISCUSIÓN FINAL

Algo que se debe tener en consideración es que el trabajo realizado hasta ahora no es el trabajo final. Aún existen muchos desafíos relacionados a la ciberseguridad que pueden ser abordados por Aliadas, y es que es imposible crear una fortaleza digital 100 % efectiva. El trabajo realizado en esta memoria permitió plantear las bases para edificar un sistema de ciberseguridad que le permite incluso mutar en un futuro a un SGSI, y así posteriormente optar a certificaciones como la ISO 27001.

Relacionado a lo anterior, cabe destacar que las personas que diseñan, desarrollan y administran las plataformas digitales también son vulnerables a amenazas de seguridad. Debido a ello, es necesario que las campañas de concientización no se enfoquen netamente en los usuarios y usuarias de las plataformas, sino también en el equipo de desarrollo de éstas. Bajo esa perspectiva, el enfoque que se le dio a las políticas de ciberseguridad en Aliadas, fue justamente el de cambiar la conducta de las personas, que trabajan en Aliadas, en el ámbito de la ciberseguridad. El desafío ahora radica en buscar la manera de lograr que estas políticas

efectivamente sean adoptadas por las personas que están dentro de la organización. Esto supone en un futuro contar con un equipo dedicado a ello. Pero esta adopción no es tarea fácil puesto que supone contar con un enfoque de gestión dispuesto a los cambios (incluir a todos los agentes, hablar de ciberseguridad como una responsabilidad que pasa por todos los miembros del equipo, contar con procesos internos, etc) ¿Es entonces indispensable el apoyo de la alta gerencia de una organización como factor de éxito? Sin duda alguna, la organización como tal debe estar completamente alineada con este pensamiento para llevarlo a cabo de manera exitosa.

Finalmente, si consideramos entonces que esta memoria se ha centrado en las necesidades de las personas, ¿Debemos entonces seguir hablando de las personas como el eslabón más débil en ciberseguridad? Este es un término que constantemente se nombra en el ámbito de la ciberseguridad, pero el trabajo realizado con las usuarias de Aliadas ha evidenciado que el castigar y ridiculizar a las personas cuando se habla de ciberseguridad sólo ha hecho que los y las usuarias se sientan lejanas a estos conceptos. Por tanto, realizar esta pregunta es un cuestionamiento totalmente válido si lo que se quiere es acercar la ciberseguridad a las personas. Estar inmersos en una sociedad que convive con el mundo digital de una forma tan estrecha, implica tomar a la ciberseguridad como algo que debe ser incluido en nuestro diario vivir.

Ahí hay un tremendo desafío que puede ser adoptado por los y las estudiantes de pregrado de ingeniería civil informática; lograr crear una cultura que se base en el uso responsable de la tecnología, puesto que en la medida que ocurra esto, se irán disminuyendo las oportunidades que tienen los ciberdelincuentes de cometer delitos.

ANEXOS

5.1. ANEXO A: Política de Ciberseguridad de Aliadas

Política de Ciberseguridad de Aliadas

Última Actualización: Julio, 2021

Preámbulo

La adopción de buenas prácticas resulta un aspecto que no se puede obviar en todas las etapas de desarrollo de un software, y es que la aplicación de estos métodos y/o técnicas permiten llevar a cabo de manera óptima el conjunto de actividades que están comprendidas en el desarrollo de un sistema.

Cuando se desarrolla software se puede caer en la cuenta de que hay numerosos factores que están involucrados, donde se pueden destacar la calidad del código fuente, la comunicación del equipo de desarrollo, aspectos de QA, desarrollo y producción; y no menos importante, factores relacionados a la seguridad.

Bajo este último punto es que resulta importante desarrollar un documento que sea capaz de abordar todas las aristas relacionadas a la seguridad del proyecto y que pueda servir de guía para todos los miembros del equipo de desarrollo.

Objetivos

Este documento presenta la "Política de Ciberseguridad" utilizada en Aliadas, la cual tiene como objetivo presentar los lineamientos y responsabilidades para proteger la confidencialidad, integridad y disponibilidad de los activos de información y datos que son gestionados por Aliadas, utilizando como base el estándar ISO 27001.

Terminología

- **Debe:** El requerimiento al que se refiere es Obligatorio
- **Debería:** El requerimiento al que se refiere es Recomendado
- **Puede:** El requerimiento al que se refiere es Opcional

Definiciones

- **Confidencialidad:** Propiedad de la información de no ser revelada o expuesta a usuarios, procesos o terceros que no han sido autorizados.
- **Integridad:** Propiedad de la información en relación a su exactitud y no haber sido modificada, ni alterada por terceros.
- **Disponibilidad:** Propiedad de la información de ser accesible y usable bajo demanda por un usuario o proceso autorizado.
- **Activos de Información:** Todos aquellos medios físicos o digitales donde se reciba, almacene, transfiera o se pueda visualizar la información.

Alcance

El alcance de este documento recae en toda la organización interna de Aliadas, como también sus proveedores cuando así aplique el caso.

Políticas de Ciberseguridad

Políticas generales

1. Toda persona perteneciente a la organización interna de Aliadas que identifique alguna vulnerabilidad, brecha de datos o debilidad que ponga en riesgo la seguridad de la organización **debe** reportarla inmediatamente mediante el canal de #seguridad en el servidor Discord de la organización.
2. Se **debe** proteger la confidencialidad de la información de los usuarios, asignando a cada grupo de usuarios los permisos mínimos necesarios para el correcto funcionamiento de la aplicación.
3. El acceso a la información de los usuarios **debe** estar restringido únicamente a aquellos empleados y colaboradores de Aliadas que necesiten acceder a tales datos para el desempeño de sus funciones y/o para el desarrollo o mejoramiento de la aplicación.
4. Se **debe** impedir el acceso, modificación o divulgación de la información por cualquier entidad no autorizada por Aliadas.
5. Políticas de acceso remoto:
 - a. Toda persona perteneciente a la organización interna de Aliadas **debería** evitar conectarse a los servidores de Aliadas por medio de una red de internet pública, poco frecuente o desconocida.

*Para más detalles sobre el control de accesos, léase la **Política de control de accesos**.*

Políticas de gestión de credenciales y contraseñas

1. Toda persona, perteneciente a la organización interna de Aliadas, a la que se le otorguen credenciales de acceso, **debe** proteger y generar contraseñas robustas, como también dar buen uso a ellas, recordando que estas credenciales son personales e intransferibles.

*Para más detalles de este apartado léase la **Política de gestión de credenciales y contraseñas**.*

Políticas de uso aceptable de recursos

1. Toda persona perteneciente a la organización interna de Aliadas **debe** dar buen uso a todos los recursos tecnológicos y herramientas que le sean asignados para el desarrollo de sus funciones.
2. Toda persona perteneciente a la organización interna de Aliadas **debe** utilizar su correo electrónico organizacional sólo con fines laborales.

Políticas de desarrollo seguro

1. Todos los desarrolladores **deben** cumplir con los lineamientos expuestos en la **Guía de Desarrollo Seguro de Aliadas**.

Políticas de gestión de vulnerabilidades y parches

1. Para la gestión de vulnerabilidades se debe cumplir con los lineamientos expuestos en la **Política de gestión de vulnerabilidades y parches**.

Roles y responsabilidades

1. Eventualmente se **debería** gestionar la creación de un *Equipo de Ciberseguridad*, cuya función principal debe ser velar por el cumplimiento de esta política, así como asesorar y apoyar a todos los equipos internos de Aliadas.
2. Entre algunas de las funciones principales que **debería** tener este equipo podemos encontrar:
 - a. Establecer políticas y cumplimientos en conjunto con cada una de las áreas de Aliadas.
 - b. Implementar medidas y controles de seguridad para proteger la información de usuarios y activos de información de la organización.
 - c. Liderar, coordinar y ejecutar la respuesta frente a incidentes de seguridad, en conjunto con los procesos de recuperación.
 - d. Implementar mecanismos de seguridad en concordancia con los lineamientos expuestos en esta política.

Cumplimiento

Toda persona perteneciente a la organización interna de Aliadas y colaboradores, **deben** cumplir con los lineamientos planteados en esta política y todas aquellas políticas y guías que se desprendan de ésta.

El incumplimiento o faltas a ella estarán sujetos a procesos disciplinarios internos de la organización.

Excepciones a esta política

Cualquier excepción a esta política o aquellas políticas y guías que se desprendan de ésta, deben ser solicitadas y autorizadas formalmente por el <ENCARGADO>.

Esta solicitud debe ser realizada a través de <MEDIO> indicando el tipo de excepción, la cual será aprobada o rechazada por el <ENCARGADO>. Toda evidencia de la solicitud y su resolución debe quedar archivada bajo la etiqueta de "excepciones a la política de ciberseguridad".

Cambios y revisión a esta política

Se **debe** definir, aprobar, publicar y comunicar a todas las personas pertenecientes a la organización interna de Aliadas y colaboradores un grupo de políticas de seguridad de la información.

Esta política **debe** ser revisada una vez al año o cuando sea necesario un cambio significativo, la cual debe ser publicada en el Drive de la organización y dar aviso a toda la organización en caso de cambios y/o actualizaciones.

5.2. ANEXO B: Política de control de accesos de Aliadas

Política de Control de Accesos de Aliadas

Última Actualización: Julio, 2021

Objetivo

El objetivo principal de esta política de control de accesos es determinar los lineamientos para limitar el acceso a la información, garantizar el acceso a usuarios autorizados y evitar el acceso no autorizado a sistemas, servicios e información.

Terminología

- **Propietario:** persona física que posee un rol de administrador sobre un sistema o servicio específico.

Alcance

Esta política de control de accesos se aplica a todas las personas pertenecientes a la organización interna de Aliadas y/o colaboradores que sean responsables de una cuenta que se utilice en cualquier sistema que sea parte del funcionamiento de Aliadas.

Política de control de accesos

Gestión de accesos

Los propietarios de los sistemas determinarán el nivel de control de acceso para el sistema y su servicio.

Respecto a los diferentes sistemas y servicios:

- Redes: Se **debe** controlar el acceso a los servicios de red, tanto internos como externos.
- Aplicaciones e información: El acceso lógico a las aplicaciones e información **debe** estar restringido a los usuarios autorizados en función de las necesidades del usuario y siguiendo el principio del mínimo privilegio.

Accesos con privilegios

Toda asignación de accesos privilegiados, que permitan a los usuarios anular los controles del sistema, **debe** estar debidamente controlados, aprobados por el propietario del sistema y alineados con la política de accesos con privilegios.

*Para más detalles de esta apartado léase la **Política de accesos con privilegios***

Accesos de usuarios

El acceso de los distintos tipos de usuarios de la organización **debe** concederse de acuerdo con las funciones definidas previamente por el propietario del sistema y los jefes de equipo.

Registro de usuarios

Todas las altas y bajas de usuarios que confieran acceso a los diversos sistemas y servicios, **deberían** ser generados por el propietario del sistema.

Reglas y derechos de control de acceso

Las reglas y derechos de los controles de acceso **deberían** estar documentados para cada tipo de usuario (o grupo de usuarios), e incluir los lineamientos mínimos indicados en las **Políticas de gestión de credenciales y contraseñas**.

Revisión de las reglas y derechos de control de acceso

Tanto reglas como derechos sobre el control de acceso de esta política, **deberían** ser revisados a intervalos regulares, por ejemplo, una vez al año.

Roles y responsabilidades

Todas las personas pertenecientes a la organización de Aliadas, consultores y otros que presten servicios a la organización, **deben** asegurarse de comprender sus funciones y sus responsabilidades en lo que respecta a las directrices establecidas por esta política.

El incumplimiento de esta política puede dar lugar a medidas disciplinarias.

Cambios y revisión a esta política

Esta política **debe** ser revisada una vez al año o cuando sea necesario un cambio significativo, la cual debe ser publicada en el Drive de la organización y dar aviso a toda la organización en caso de cambios y/o actualizaciones.

Referencias

- *ISO/IEC 27001:2013 standard, Access Control A.9.*
- *NIST Special Publication 800-12 Revision 1 Information Security Handbook: A Guide for Managers*

5.3. ANEXO C: Política de control de accesos con privilegios de Aliadas

Política de accesos con privilegios de Aliadas

Última Actualización: Julio, 2021

Objetivo

El objetivo principal de esta política de accesos con privilegios es limitar el acceso a la información, garantizar el uso controlado autorizado de los permisos administrativos y evitar accesos no autorizados a los sistemas y servicios.

Terminología

- **Cuenta con privilegios administrativos:** Es una cuenta que tiene más privilegios que la de un usuario normal. En este tipo de cuenta se encuentran funciones tales como poder instalar o eliminar software, actualizar sistemas operativos, modificar configuraciones de sistemas y/o de aplicaciones.
- **Propietario de la cuenta:** Persona física autorizada y asignada por Aliadas para utilizar una cuenta.

Alcance

Esta política aplica para todos los usuarios con accesos con privilegios (accesos administrativos).

Política de accesos con privilegios

Generalidades

Se han definido los siguientes lineamientos para todos los usuarios con privilegios administrativos:

- Todas las cuentas administradas **deberían** ser inventariadas y sus propietarios validados para ser autorizados.
- Los derechos de acceso con privilegios **deben** revisarse a intervalos más frecuentes, se recomienda cada 6 meses.
- Los derechos de accesos con privilegios **deben** ser supervisados para asegurar que no se han concedido privilegios no autorizados.
- Antes de desplegar cualquier dispositivo nuevo, todas las contraseñas por defecto de las aplicaciones, sistemas operativos, routers, firewalls, y otros sistemas, **deben** cambiarse por una contraseña que cumpla con la **Política de gestión de credenciales y contraseñas**.
- Las cuentas con accesos privilegiados sólo **deben** utilizarse para actividades de administración de sistemas.

- Los propietarios de cuentas con accesos privilegiados **deben** establecer contraseñas únicas y diferentes para sus cuentas con accesos privilegiados y no privilegiados.
- El acceso a las herramientas de scripting (como bash, python, etc) **debe** limitarse solo a los usuarios administradores o desarrolladores que tengan la real necesidad de acceder a estas capacidades.
- Los sistemas **deberían** estar configurados de tal manera que permita llevar un registro de cuando una cuenta se añade/elimina, así como también cuando se crean/eliminan nuevos grupos con privilegios administrativos. Además deberían registrar los intentos de inicio de sesión de cuentas administrativas.

Roles y responsabilidades

Todas las personas pertenecientes a la organización de Aliadas, consultores y otros que presten servicios a la organización, **deben** asegurarse de comprender sus funciones y sus responsabilidades en lo que respecta a las directrices establecidas por esta política.

El incumplimiento de esta política puede dar lugar a medidas disciplinarias.

Cambios y revisión a esta política

Esta política **debe** ser revisada una vez al año o cuando sea necesario un cambio significativo, la cual debe ser publicada en el Drive de la organización y dar aviso a toda la organización en caso de cambios y/o actualizaciones.

Referencias

- **CIS Controls** - Center for Internet Security: Reference Control 4 Controlled Use of Administrative Privileges

5.4. ANEXO D: Política de gestión de credenciales y contraseñas de Aliadas

Política de gestión de credenciales y contraseñas de Aliadas

Última Actualización: Julio, 2021

Objetivo

El objetivo principal de esta política de gestión de credenciales y contraseñas es establecer los lineamientos para la creación de credenciales y contraseñas seguras, la protección de las mismas y la frecuencia de cambio.

Alcance

Esta política de gestión de credenciales y contraseñas se aplica a toda persona perteneciente a la organización interna de Aliadas que tengan o sean responsables de una cuenta (o cualquier otra forma de acceso) en cualquier sistema que se utilice en las actividades necesarias para desempeñar sus funciones.

Política de gestión de credenciales y contraseñas

Generalidades

Todos los usuarios **deben** proteger las credenciales que les fueron asignadas, y deben garantizar la complejidad de sus contraseñas. Además, los usuarios deben estar conscientes de que todas las credenciales son personales e intransferibles.

No se debe utilizar los valores predeterminados del proveedor de algún sistema para las contraseñas y/o otros parámetros de seguridad. Lo anterior implica que antes de desplegar cualquier activo nuevo, se deben cambiar las contraseñas que vienen por defecto.

Todas las contraseñas a nivel de usuario (correo electrónico, computador, aplicaciones, etc), deben ser cambiadas en caso de existir pruebas que confirmen la vulnerabilidad de éstas. Este compromiso debería ser llevado a cabo por el equipo de seguridad.

Credenciales Github y Google Drive

Todos los usuarios que tengan acceso al repositorio Github de Aliadas y/o a los archivos en el Google Drive general del proyecto, deben tener habilitado el doble factor de autenticación siempre y cuando esté disponible la opción.

Recomendación de contraseñas

Siguiendo las recomendaciones del NIST, las contraseñas **deben** seguir lo siguiente:

- Longitud mínima de ocho caracteres en todos los sistemas
- Siempre cambiar la contraseña por defecto

- Cambiar la contraseña si hay evidencia de que hay peligro
- Omitir sugerencia de contraseñas y preguntas de seguridad basadas en aspectos personales
- Siempre limitar el número de intentos de autenticación fallidos
- Al asignar una nueva contraseña, se sugiere comparar esta con un listado de contraseñas conocidas que hayan sido comprometidas.

Además, **debería**:

- Permitirse la función de copiar y pegar en los campos de contraseñas para facilitar el uso de gestores de contraseñas.
- Promover el uso de un gestor de contraseñas o brindar la licencia para la utilización de uno.
- En caso de que un sistema del tipo root, administrador o de servicio, no permita el uso de doble factor de autenticación (u otro método similar), la contraseña utilizada deberá ser de uso exclusivo para ese sistema.

Roles y responsabilidades

Todas las personas pertenecientes a la organización de Aliadas, consultores y otros que presten servicios a la organización, **deben** asegurarse de comprender sus funciones y sus responsabilidades en lo que respecta a las directrices establecidas por esta política.

El incumplimiento de esta política puede dar lugar a medidas disciplinarias.

Cambios y revisión a esta política

Esta política **debe** ser revisada una vez al año o cuando sea necesario un cambio significativo, la cual debe ser publicada en el Drive de la organización y dar aviso a toda la organización en caso de cambios y/o actualizaciones.

Referencias

- *CIS Controls - Center for Internet Security: Reference Control 4 Controlled Use of Administrative Privileges*
- *NIST Special Publication 800-63B - Digital Identity Guidelines*

5.5. ANEXO E: Borrador de Política de gestión de y parcheo de vulnerabilidades de Aliadas

BORRADOR

Política de gestión de vulnerabilidades y parches

Última Actualización: Mayo, 2021

Objetivo

El objetivo principal de esta política de gestión de vulnerabilidades es mantener todos los componentes que forman parte de la infraestructura informática de Aliadas, al día con los últimos parches y en sus versiones más seguras.

Terminología

- Vulnerabilidad: *Falta definir*
- Parche: *Falta definir*

Alcance

La política de gestión de vulnerabilidades y parches aplica a todas las personas de la organización interna de Aliadas responsables del desarrollo de la aplicación, y de adquirir, probar, priorizar, implementar y verificar los parches de seguridad.

Política de gestión de vulnerabilidades y parches

Generalidades de vulnerabilidades

Se **deben** realizar escaneos de vulnerabilidad al código al menos trimestralmente o después de cualquier cambio significativo. Dentro de estos resultados, aquellos escaneos que sean calificados como críticos o altos deben ser corregidos, y al terminar se debe volver a realizar un escaneo con el fin de resolver todos los riesgos críticos y altos.

La siguiente tabla muestra el plazo en tiempo estipulado para abordar los distintos tipos de vulnerabilidades (según su severidad, utilizando la puntuación CVSS):

Calificación	Puntuación CVSS	Tiempo de remediación
Crítica	9.0-10.0	72 hrs
Alta	7.0-8.9	7 días
Mediana	4.0-6.9	90 días
Baja	0.1-3.9	180 días

Cualquier vulnerabilidad explotable que se encuentre durante una prueba de penetración debe ser corregida y volver a ser verificada para asegurarse de que fue corregida. Se **puede** definir un protocolo de parcheo para todas las vulnerabilidades o bugs.

Generalidades de actualizaciones

Las actualizaciones de software y los cambios de configuración aplicados a los activos informáticos, deben ser previamente testeados por <ENTIDAD ENCARGADA> antes de su despliegue generalizado.

Roles y Responsabilidades

Falta definir

Cambios y revisión a esta política

Esta política **debe** ser revisada una vez al año o cuando sea necesario un cambio significativo, la cual debe ser publicada en el Drive de la organización y dar aviso a toda la organización en caso de cambios y/o actualizaciones.

Referencias

- *NIST Special Publication 800-40r3 Guide to Enterprise Patch Management Technologies.*
- *ISO/IEC 27001:2013 standard, control A.11.2.7*

5.6. ANEXO F: Política de privacidad de Aliadass

Política de Privacidad de Aliadas

Última Actualización: Junio, 2021

¿Qué información es recolectada por Aliadas?

- **La información de registro**, para la creación de tu cuenta, es decir, correo electrónico o redes sociales vinculadas.
- **La información personal y privada que proveas**, como nombre, apellidos, número de teléfono, rut, fecha de nacimiento y/o género.
- **(Si eres emprendedora) La información relacionada a tu tienda y productos**, como el nombre de la tienda, listado de productos y precio/descripción de ellos.
- **Información sobre las interacciones con la aplicación y dispositivo utilizado**, incluyendo la información referente a “likes” y opiniones sobre tiendas y/o productos, y comentarios realizados en la aplicación.

¿Cómo es utilizada tu información recolectada?

Al aceptar esta política de privacidad estás otorgando explícitamente los permisos para utilizar tus datos recolectados de la siguiente forma:

- **Elaboración de perfiles**, para realizar un análisis con los datos vinculados a ti.
- **Realizar recomendación de productos**, en base a un análisis sobre tus tiendas favoritas y productos adquiridos.
- **(Si eres emprendedora) Contribuir al sistema de colaboración** entre emprendedoras.
- **(Si eres emprendedora) Creación de Tiendas Virtuales**, con la información que nos entregues de tu(s) emprendimiento(s).

¿Con quién se comparte tu información?

Toda tu información personal, de contacto y de tiendas será utilizada exclusivamente por **Aliadas** para el funcionamiento de la aplicación. Tendrás control sobre aquellos datos que desees hacer públicos.

Toda información utilizada para realizar análisis y estadísticas sobre la plataforma será compartida con **ANID (Agencia Nacional de Investigación y Desarrollo de Chile)**, enfatizando que en este tipo de información no se incluyen tus datos personales y/o privados.

¿Quieres saber más? Revisa a continuación nuestra política de privacidad completa.

Política de Privacidad

Información general

Esta política de privacidad describe nuestras políticas y procedimientos sobre la recopilación, el uso y la divulgación de tu información cuando utilizas Aliadas, y te proporciona información sobre tus derechos de privacidad.

Utilizamos tu data para proporcionar y mejorar Aliadas. Al utilizar nuestra aplicación, aceptas la recopilación y el uso de la información de acuerdo con esta política de privacidad.

1. Recopilación y uso de la data recolectada

1.1 Tipo de data recolectada

1.1.1. Data personal

Al utilizar Aliadas, es posible que te pidamos que nos proporciones cierta información de identificación personal que será utilizada para darte acceso a distintas funcionalidades. La información personal es de carácter público y puede incluir, pero no está limitada a:

- Correo electrónico.
- Nombre y Apellido.
- Rut.
- Fecha de nacimiento.

1.1.2 Data privada

Así mismo, es posible que te pidamos que nos proporciones cierta información personal privada que será utilizada para validar tu identidad y la de tu emprendimiento (si así aplicara). La información privada puede incluir, pero no está limitada a:

- Número de teléfono.
- Dirección.
- Género.

1.1.3 Data de autenticación

Cuando te creas una cuenta en Aliadas, deberás elegir entre dos formas distintas de autenticación: ya sea mediante correo/contraseña o vinculando la cuenta de una red social de terceros. Sea cual sea el caso, no guardaremos tu contraseña o algún identificador de autenticación, sino que almacenaremos una referencia de ésta.

1.1.4 Data de emprendimientos

Al utilizar el servicio de creación de tiendas en Aliadas, se te solicitará que proporciones información referente a tu(s) emprendimiento(s). La información de emprendimientos puede incluir, pero no está limitada a:

- Nombre del emprendimiento.
- Nombre de los productos o servicios.
- Valores de los productos o servicios.
- Descripción de los productos o servicios.
- Información de contacto de la emprendedora.

1.1.5 Datos de uso

Los datos de uso se recogen automáticamente al utilizar Aliadas. Cuando accedes a través de un dispositivo móvil, podemos recopilar cierta información automáticamente, incluyendo, pero sin limitarse a: el tipo de dispositivo móvil que utilizas; la dirección IP de tu dispositivo móvil; tu sistema operativo móvil y otros datos de diagnóstico. Además se incluyen datos referente a las secciones de Aliadas que visitas y/o el tiempo que pasas en ellas.

1.1.6 Información de servicios de redes sociales de terceros

Aliadas te permite crear una cuenta e iniciar sesión para utilizar nuestra aplicación a través de los siguientes servicios de redes sociales de terceros:

- Facebook.
- Google.
- Instagram.

Si decides registrarte a través de un servicio de redes sociales de Terceros, podemos recopilar los datos personales que ya están asociados a tu cuenta del servicio de redes sociales de terceros, como, pero sin limitarse a, tu nombre, tu dirección de correo electrónico y contactos vinculados a tu cuenta.

Si decides proporcionar dicha información y datos personales, durante el registro o de otro modo, estás dando permiso a Aliadas para que esta información la utilice y almacene de forma coherente con esta política de privacidad.

1.1.7 Información recolectada mientras utiliza la aplicación

Durante el uso de nuestra aplicación, y con el fin de proporcionar distintas funcionalidades de ésta, y mejorar y personalizar la experiencia de uso, podemos recopilar, con tu permiso previo:

- Información sobre tu ubicación.
- Imágenes y otra información de la cámara y la biblioteca de fotos de tu dispositivo.

Puedes activar o desactivar estos permisos en cualquier momento, a través de la configuración de tu dispositivo.

Además, durante el uso de nuestra aplicación, recopilamos diferentes datos con respecto a las interacciones que realizas con la aplicación durante su uso. Estos datos pueden incluir, pero no se limitan a:

- Likes a productos y/o comentarios.
- Opiniones a productos y/o tiendas.

- Productos adquiridos y/o vendidos.
- Y actividad general de la aplicación móvil de Aliadas.

1.2 Uso de la data recolectada

Aliadas puede usar la data recolectada para los siguientes propósitos:

- Para proporcionar y mantener Aliadas, incluyendo la supervisión del uso de nuestros servicios.
- Para gestionar tu cuenta, incluyendo tu registro como usuario a Aliadas. Los datos personales y privados que proporcionas pueden darte acceso a diferentes funcionalidades de los servicios que están disponibles para ti como usuaria registrada en Aliadas.
- Para ponerse en contacto contigo, por correo electrónico, llamadas telefónicas, SMS u otras formas equivalentes de comunicación electrónica, como las notificaciones push de la aplicación en relación a las actualizaciones o comunicaciones informativas relacionadas con las funcionalidades de la aplicación; incluidas las actualizaciones de seguridad, cuando sea necesario o razonable para su implementación.
- Para gestionar peticiones que realice a Aliadas.
- Para otros fines. Podemos utilizar la data recolectada para otros fines, como el análisis de datos, la identificación de tendencias de uso, la determinación de la eficacia de nuestras campañas; y para evaluar y mejorar Aliadas.

También podríamos compartir la data recolectada en las siguientes situaciones:

- Con otros usuarios: cuando compartes información personal o interactúas de otro modo en las áreas públicas con otros usuarios, y dicha información puede ser vista por todos los usuarios y puede ser distribuida públicamente en el exterior. Del mismo modo, otros usuarios podrán ver las descripciones de tu(s) emprendimiento(s) (si aplica).
- Con tu consentimiento: podemos revelar información personal que tu estimes conveniente para cualquier otro propósito, siempre con tu consentimiento.

2. Retención de la data recolectada

2.1 Retención de la data recolectada

Aliadas conservará tus datos privados únicamente durante el tiempo que sea necesario para los fines establecidos en esta política de privacidad. Conservaremos y utilizaremos tus datos privados en la medida en que sea necesario para cumplir con nuestras obligaciones legales (por ejemplo, si estamos obligados a conservar tus datos para cumplir con las leyes aplicables), resolver disputas y hacer cumplir nuestros acuerdos y políticas legales.

Aliadas también conservará la data recolectada con fines de análisis interno. Estos datos se conservan generalmente durante un periodo de tiempo más corto, excepto cuando estos datos se utilizan para reforzar la seguridad o mejorar las funcionalidades de nuestros

servicios, o estamos legalmente obligados a conservar estos datos durante períodos de tiempo más largos

2.1.1 Dar de baja tus datos personales y privados

En caso de que desees dar de baja toda la información personal y/o privada que proporcionaste a Aliadas, puedes realizarlo eliminando tu cuenta desde la misma aplicación o contactándonos a través del siguiente formulario: <https://aliad.as/contacto/>

3. Transferencia de data recolectada

3.1 Transferencia de la data recolectada

Toda la información recolectada se procesa en los servidores de Aliadas y en cualquier otro lugar donde se encuentren las partes involucradas en el procesamiento. Significa que esta información puede ser transferida y mantenida en servidores ubicados fuera de tu región, provincia, país u otra jurisdicción gubernamental donde las leyes de protección de datos pueden diferir de las de tu jurisdicción.

Es importante recalcar que la data recolectada respecto a tus interacciones y uso de la aplicación, será utilizada para realizar análisis y/o estadísticas que serán compartidas con ANID. Pero de ninguna manera en esta data se incluyen tus datos personales y/o privados.

Aliadas tomará todas las medidas razonablemente necesarias para garantizar que tus datos sean tratados de forma segura y de acuerdo con esta política de privacidad y no se realizará ninguna transferencia de tus datos a ninguna otra organización o país a menos que así lo exija la ley y existan controles adecuados que incluyan la seguridad de tus datos.

Tu consentimiento a esta política de privacidad representa tu acuerdo con dicha transferencia.

4. Divulgación de la data recolectada

4.1 Aplicación de la Ley

En determinadas circunstancias, Aliadas puede verse obligada a revelar la data recolectada si así lo exige la ley o en respuesta a solicitudes válidas de las autoridades públicas (por ejemplo, un tribunal o una agencia gubernamental).

4.2 Otros requisitos legales

Aliadas puede revelar tus datos personales si cree de buena fe que dicha acción es necesaria para:

- Cumplir con una obligación legal.
- Proteger y defender los derechos o la propiedad de Aliadas.

- Prevenir o investigar infracciones en relación con el servicio proporcionado por Aliadas.
- Proteger la seguridad personal de los usuarios de Aliadas o del público.
- Proteger contra la responsabilidad legal.

5. Privacidad de menores de edad

5.1 Sobre menores de edad

Los servicios de Aliadas no se dirigen a ninguna persona menor de 18 años. No recopilamos conscientemente información de identificación personal de ninguna persona menor de 18 años. Si eres un padre o tutor y tienes conocimiento de que tu hijo/a nos ha proporcionado datos personales, ponte en contacto con nosotros. Si tenemos conocimiento de que hemos recopilado datos personales de cualquier persona menor de 18 años sin verificar el consentimiento de sus padres, tomamos medidas para eliminar esa información de nuestros servidores.

6. Cambios en esta política de privacidad

6.1 Sobre los cambios de esta política de privacidad

Podemos actualizar nuestra Política de privacidad de vez en cuando. Te notificaremos cualquier cambio publicando la nueva política de privacidad en esta página antes de que el cambio entre en vigor y actualicemos la fecha de Última actualización; en la parte superior de esta política de privacidad.

Se te aconseja que revises esta política de privacidad periódicamente para ver si hay cambios. Los cambios en esta política de privacidad son efectivos cuando se publican en esta sección.

REFERENCIAS BIBLIOGRÁFICAS

- [Almagro, 2019] Almagro, L. (2019). Marco nist: Un abordaje integral de la ciberseguridad. White Paper Series. Edición 5. Recuperado en <https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf>.
- [Barman, 2002] Barman, S. (2002). Writing information security policies. New Riders. Edición 1.
- [Bernal, 2020] Bernal, I. (2020). El 95 % de los ciberataques que logra su objetivo viene precedido de un error humano. El Correo. Sección de Economía. Recuperado en <https://www.elcorreo.com/economia/tu-economia/ciberataques-viene-precedido-20200420175047-nt.html>.
- [BID y OEA, 2020] BID y OEA (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en américa latina y el caribe. Recuperado en <http://dx.doi.org/10.18235/0002513>.
- [Craig et al., 2014] Craig, D., Diakun-Thibault, N., y Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10).
- [de Chile, 2017] de Chile, G. (2017). Política nacional de ciberseguridad de Chile. Biblioteca Nacional de Chile. Recuperado en <https://biblioteca.digital.gob.cl/handle/123456789/1158>.
- [Dhillon y Backhouse, 2001] Dhillon, G. y Backhouse, J. (2001). Current directions in is security research: Towards socioorganisational perspectives. Information Systems Journal. 11(127-153).
- [D'Antonio y Olías de Lima, 2019] D'Antonio, G. y Olías de Lima, M. (2019). Digital security en la nueva era de transformación digital. Real Instituto Elcano.
- [Giner, 2020] Giner, G. R. (2020). Emprendimiento femenino: ¿oportunidad o necesidad? Ciencias Económicas y Contables pp:86-97.
- [Harknett y Stever, 2011] Harknett, R. J. y Stever, J. A. (2011). The new policy world of cybersecurity. Public Administration Review. 71(3):455-460.
- [ITU, 2009] ITU (2009). Overview of cybersecurity. recommendation itu-t x.1205. International Telecommunication Union website. Recuperado en <http://www.itu.int/rec/T-REC-X.1205-200804-I/en>.
- [Kelley et al., 2009] Kelley, P., Bresee, J., Cranor, L., y Reeder, R. (2009). A "nutrition label" for privacy. Proceedings of the 5th Symposium on Usable Privacy and Security. 4:1-12.
- [Kemmerer, 2003] Kemmerer, R. A. (2003). Cybersecurity. 25th International Conference on Software Engineering, 2003. Proceedings. pp:705-715.

- [Korunovska *et al.*, 2020] Korunovska, J., Kamleitner, B., y Spiekermann, S. (2020). The challenges and impact of privacy policy comprehension. Systematic Bias in Notice Comprehension Twenty-Eighth European Conference on Information Systems.
- [Lewis, 2006] Lewis, J. (2006). Cybersecurity and critical infrastructure protection. CSIS website. Recuperado en <https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection>.
- [López, 2019] López, C. (2019). Métodos de diseño centrado en usuarios. Material de Clases. Departamento de Informática, UTFSM.
- [Maguire, 2001] Maguire, M. (2001). Methods to support human-centred design. *Int. J. Human-Computer Studies* 55:587-634.
- [McLaughlin, 2020] McLaughlin, J. F. (2020). Security mechanisms. IBM Course: Introduction to Cybersecurity Tools and Cyber Attacks.
- [NICCS, 2014] NICCS (2014). A glossary of common cybersecurity terminology. NICCS website. Recuperado en <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary>.
- [Nieles *et al.*, 2017] Nieles, M., Dempsey, K., y Pillitteri, V. (2017). An introduction to information security. NIST Special Publication 800-12.
- [Norman, 2013] Norman, D. A. (2013). The design of everyday things. Basic Books. Edición 2.
- [Norman y Draper, 1986] Norman, D. A. y Draper, S. W. (1986). User centered system design; new perspectives on human-computer interaction.
- [Pérez y Gardey, 2020] Pérez, J. y Gardey, A. (2020). Definición de framework. Recuperado en <https://definicion.de/framework/>.
- [Samonas y Coss, 2014] Samonas, S. y Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*. 10(3):21-45.
- [Sangchoolie *et al.*, 2020] Sangchoolie, B., Folkesson, P., Kleberger, P., y Vinter, J. (2020). Analysis of cybersecurity mechanisms with respect to dependability and security attributes. 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops. pp:94-101.
- [Slupska y Duckworth, 2021] Slupska, J. y Duckworth, S. D. (2021). Reconfigure: Feminist action research in cybersecurity. Oxford Internet Institute.
- [Sobers, 2020] Sobers, R. (2020). 110 must-know cybersecurity statistics for 2020. Recuperado en <https://www.varonis.com/blog/cybersecurity-statistics/>.
- [Technology, 2020] Technology, T. (2020). The holistic security manual. Recuperado en <https://holistic-security.tacticaltech.org>.