FACULTAD TECNOLÓGICA

DEPARTAMENTO DE TECNOLOGÍAS DE ADMINISTRACIÓN Y GESTIÓN

PROPUESTA DE MEJORA PARA EL FORTALECIMIENTO DE LA CULTURA DE CIBERSEGURIDAD EN FOSIS ATACAMA, EN EL MARCO DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023–2028.

Valeria Fabiana Galleguillos Cerezo

Copiapó, Chile 2025

FACULTAD TECNOLÓGICA

DEPARTAMENTO DE TECNOLOGÍAS DE ADMINISTRACIÓN Y GESTIÓN

PROPUESTA DE MEJORA PARA EL FORTALECIMIENTO DE LA CULTURA DE CIBERSEGURIDAD EN FOSIS ATACAMA, EN EL MARCO DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023–2028.

Trabajo de titulación presentado en conformidad a los requisitos para obtener el título de Ingeniería de Ejecución en Administración de Empresas

Profesor Guía: Mg. Mónica Padilla Romero

Valeria Fabiana Galleguillos Cerezo

Copiapó, Chile 2025

AGRADECIMIENTOS

A mi familia, en especial a mi mamá Adriana Cerezo, por siempre estar preocupada de mí, de mis avances y por muchas veces entender el hecho de vernos poco por estar ocupada, pero siempre atenta enviándome mucho ánimo y palabras bonitas para continuar este camino.

A mi papá, Luis Galleguillos (Q.E.P.D.), por acompañarme espiritualmente en cada paso, en mis pensamientos e incluso en mis sueños. Gracias por darme señales de que estás ahí. Donde sea que estés papá, te recuerdo siempre, y sé que estás orgulloso y feliz por mis logros.

A mi hermanita, Fernanda Galleguillos, por estar conmigo en las buenas y en las malas. Gracias por esas conversaciones profundas, que han fortalecido nuestro vínculo como hermanas y han hecho cada momento compartido especial.

A mi compañero de vida Sebastián Flores, por ser el impulso en esta importante etapa, por ayudarme y guiarme para lograr mis objetivos de la mejor manera posible, brindándome apoyo y contención cuando realmente sentía que no podía más, gracias a ti pude lograr esto, así que este logro es de ambos, y espero con ansias más objetivos y planes juntos, porque mientras vayamos de la mano, todo estará bien.

A mis gatos (Carey, Rubio, Pollito e Ivy) gracias por su dulce compañía, a pesar de los eternos pelos que cubren mi ropa y cama, los seguiría eligiendo mil veces. Al nuevo integrante que se unió hace unos meses; Choco, mi perrito negro, que a pesar de que no lo buscábamos, nos eligió y nos vino a enseñar la paciencia y a entregar mucho amor.

Los amo. ♡

A Dios y mis ángeles por darme la fortaleza, por escucharme y siempre atender a mis peticiones, increíblemente todo se me ha dado perfecto y es gracias a ustedes.

Y por último a la Universidad de Atacama que me entregó la oportunidad de poder crecer y ampliar mis conocimientos para un mejor futuro, y a mi profesora guía Mónica Padilla por orientarme en este proceso.

¡Muchas gracias!

TABLA DE CONTENIDOS

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

RESUMEN

El avance tecnológico y la creciente digitalización del Estado han incrementado la dependencia de los sistemas de información, junto con la exposición a amenazas cibernéticas que afectan directamente la continuidad y seguridad de los servicios públicos. En este contexto, FOSIS Atacama enfrenta el desafío de fortalecer su cultura de ciberseguridad, considerando que gestiona datos sensibles de personas vulnerables. A través de un diagnóstico aplicado a todos sus funcionarios, se identificaron prácticas inseguras, baja percepción del riesgo digital y una limitada articulación institucional respecto de las exigencias de la Ley Marco de Ciberseguridad y la Política Nacional de Ciberseguridad 2023–2028. A partir de estos hallazgos, se elaboró una propuesta de mejora orientada a consolidar una cultura organizacional más consciente, mediante acciones de capacitación, gobernanza, comunicación interna y ciberhigiene operativa, contribuyendo a una gestión pública más segura y alineada con los estándares nacionales.

Palabras claves: Ciberseguridad, sector público, cultura organizacional, resiliencia digital.

ABSTRACT

The advancement of technology and the increasing digitalization of the State have intensified dependence on information systems, while also heightening exposure to cyber threats that directly affect the continuity and security of public services. In this context, FOSIS Atacama faces the challenge of strengthening its cybersecurity culture, considering that it manages sensitive data belonging to vulnerable individuals. Through a diagnostic assessment applied to all its staff, insecure practices, low awareness of digital risk, and limited institutional alignment with the requirements of the Cybersecurity Framework Law and the National Cybersecurity Policy 2023–2028 were identified. Based on these findings, an improvement proposal was developed aimed at consolidating a more aware organizational culture through actions focused on training, governance, internal communication, and operational cyber hygiene, contributing to a safer public management aligned with national standards.

Keywords: Cybersecurity, public sector, organizational culture, digital resilience.

CAPITULO I

MARCO INTRODUCTORIO

1.1. INTRODUCCIÓN

La sociedad contemporánea atraviesa una profunda transformación digital que ha redefinido el funcionamiento de las organizaciones a nivel global. En Chile, este proceso se ha visto acelerado e institucionalizado, especialmente en el sector público, a través de mandatos como la Ley N° 21.180 de Transformación Digital del Estado. Esta modernización, si bien optimiza la eficiencia y la entrega de servicios a la ciudadanía, introduce simultáneamente una importante dependencia a los sistemas de información y expone a las instituciones a riesgos digitales en constante evolución.

El ciberespacio se ha convertido en un lugar donde las amenazas han incrementado en sofisticación y frecuencia. Los ciberataques ya no son eventualidades, sino acciones constantes que han afectado a diversos organismos públicos en Chile, comprometiendo la continuidad operacional, la fe pública y datos sensible de los ciudadanos. En este contexto, la ciberseguridad abandona el ámbito puramente técnico y se convierte en un pilar estratégico para la estabilidad y confianza en la gestión del Estado.

Reconociendo esta realidad, el Estado de Chile ha realizado una respuesta institucional robusta. La promulgación de la Ley Marco de Ciberseguridad N° 21.663 y la creación de la Agencia Nacional de Ciberseguridad (ANCI) establecen un marco regulatorio para la protección de la infraestructura crítica y los servicios esenciales. Complementariamente, la Política Nacional de Ciberseguridad 2023–2028 define la hoja de ruta estratégica del país, estableciendo cinco objetivos fundamentales para alcanzar un ciberespacio resiliente.

Dentro de este marco estratégico, la Política Nacional destaca un objetivo crucial: el desarrollo de una Cultura de Ciberseguridad. Diversos estudios y análisis de incidentes, tanto a nivel nacional como internacional, demuestran que la tecnología por sí sola es insuficiente. El factor humano es frecuentemente identificado como el eslabón más débil, donde errores no intencionados, el desconocimiento o el caer en tácticas de ingeniería social, como el phishing, son la causa principal de las brechas de seguridad.

El Fondo de Solidaridad e Inversión Social (FOSIS), como servicio público dependiente del Ministerio de Desarrollo Social y Familia es una entidad que maneja datos personales y sensibles de la población vulnerable del país. Como parte de la Administración del Estado, FOSIS es considerado un prestador de "Servicios Esenciales" y, por ende, está directamente mandatado a alinear su operación con las nuevas exigencias normativas. La Dirección Regional de FOSIS Atacama no es ajena a este desafío, enfrentando la necesidad de asegurar que sus procesos digitales sean robustos no solo tecnológicamente, sino también culturalmente.

El presente trabajo de titulación aborda la brecha existente entre los mandatos nacionales de ciberseguridad y la cultura organizacional en el FOSIS Atacama. A través de un diagnóstico de la situación actual, este trabajo de titulación busca identificar las debilidades en las prácticas, percepciones y conocimientos de los funcionarios, para así, diseñar una propuesta de mejora orientada a fortalecer la cultura de ciberseguridad.

1.2. PLANTEMIENTO DEL PROBLEMA

En la dirección regional del FOSIS Atacama, se observa una débil cultura de ciberseguridad, manifestada en prácticas inadecuadas, falta de capacitación y un escaso liderazgo estratégico que impide la correcta alineación con la Política Nacional de Ciberseguridad 2023–2028. Este problema se enmarca en el proceso de modernización del Estado de Chile, impulsado por la Ley N° 21.180 de Transformación Digital, que ha incrementado significativamente la digitalización de los procesos en la gestión pública. Si bien este avance mejora la eficiencia, también eleva la importancia de la protección de la información, haciendo fundamental el cumplimiento de normativas como la Ley de Protección de Datos Personales y la Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información (N° 21.643). En este escenario, FOSIS Atacama enfrenta el desafío de fortalecer su cultura organizacional para que sus funcionarios comprendan, valoren y apliquen prácticas seguras en su quehacer diario, un objetivo central de la política nacional.

Los funcionarios del FOSIS Atacama son un componente clave en la gestión operativa del servicio, utilizando sistemas informáticos y plataformas digitales para manejar información institucional y comunicarse con usuarios. Por ello, su comportamiento, percepción y conocimiento en ciberseguridad adquieren una importancia estratégica. El Gobierno de Chile ha avanzado en la creación de un marco institucional robusto a través de la Ley Marco de Ciberseguridad N° 21.663 y la Agencia Nacional de Ciberseguridad (ANCI). La Política Nacional de Ciberseguridad 2023–2028, a su vez, define la cultura de ciberseguridad como el conjunto de valores, actitudes y comportamientos que permiten prevenir y responder responsablemente ante los riesgos digitales. Sin embargo, en FOSIS Atacama existe una notoria brecha entre estos lineamientos y las prácticas cotidianas, lo que se manifiesta en el uso inadecuado de contraseñas, la falta de actualización de sistemas, el escaso reporte de incidentes y una limitada percepción del riesgo. Estas conductas reflejan una falta de apropiación institucional de la seguridad de la información, un fenómeno también presente en otros servicios públicos del país.

Las causas de esta baja cultura de ciberseguridad en la oficina regional son identificables y responden a tres dimensiones principales. En primer lugar, la falta de una capacitación sistemática y pertinente dirigida a los funcionarios reduce su nivel de conocimiento y su capacidad para reconocer y responder a amenazas digitales. En segundo lugar, una comunicación interna deficiente respecto a protocolos y políticas institucionales genera desconocimiento sobre las responsabilidades de cada individuo en la protección de la información. Finalmente, la ausencia de un liderazgo estratégico en torno al tema impide consolidar una visión compartida sobre la relevancia de la ciberseguridad como un elemento transversal e indispensable de la gestión pública. La misión del FOSIS, centrada en contribuir a la superación de la pobreza, implica el manejo constante de datos personales sensibles, lo que convierte a la ciberseguridad en un pilar fundamental para su quehacer y para la protección de la confianza pública.

Las consecuencias de esta situación pueden ser críticas tanto para la institución como para sus beneficiarios. Una cultura de ciberseguridad débil aumenta el riesgo de pérdida o filtración de datos sensibles de personas en situación de vulnerabilidad, afectando su privacidad y la credibilidad del servicio. Además, eventuales incidentes informáticos

podrían interrumpir la continuidad operativa de programas sociales clave, generando impactos reputacionales y económicos significativos. Esta urgencia es reforzada por datos del Observatorio Nacional de Ciberseguridad, que señalan que más del 60% de los incidentes en organismos públicos se originan por errores humanos o prácticas inseguras del personal, lo que evidencia la necesidad de fortalecer la educación digital y la gestión preventiva.

Frente a este escenario, el presente trabajo busca evaluar el estado de la cultura de ciberseguridad en el FOSIS Atacama, identificando los factores críticos y las brechas existentes respecto a la Política Nacional de Ciberseguridad. El principal aporte será proponer recomendaciones estratégicas y contextualizadas, orientadas a fortalecer las competencias del personal y mejorar la gestión de la seguridad digital. Con ello, se pretende mejorar la resiliencia digital del FOSIS Atacama a través de sugerencias pertinentes a su realidad local, enriqueciendo la comprensión de la cultura organizacional de la institución frente a los desafíos tecnológicos actuales.

1.3. OBJETIVOS

1.3.1. Objetivo General.

Elaborar una propuesta de mejora para el fortalecimiento de la cultura de ciberseguridad en FOSIS atacama en el marco de la política nacional de ciberseguridad 2023–2028.

1.3.2. Objetivos Específicos.

- Realizar un diagnóstico de la cultura de ciberseguridad actual en los funcionarios del FOSIS Atacama, mediante la aplicación de una encuesta estructurada.
- Analizar el grado de alineación entre las prácticas actuales de ciberseguridad en FOSIS Atacama y los lineamientos establecidos en la Política Nacional de Ciberseguridad 2023–2028, determinando las brechas.

- Proponer recomendaciones estratégicas orientadas a fortalecer la cultura de ciberseguridad en FOSIS Atacama, considerando los hallazgos del análisis y el marco de la política nacional.

1.4. Justificación

La transformación digital que experimenta el Estado en los últimos años ha generado una creciente dependencia de los sistemas tecnológicos, la gestión de datos y las plataformas digitales en la administración pública. En este contexto, la ciberseguridad se ha convertido en un componente esencial para garantizar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad operativa de los servicios públicos (Ministerio de Hacienda, 2023). Sin embargo, junto con los avances tecnológicos, también han aumentado las amenazas informáticas, lo que obliga a las instituciones del sector público a fortalecer su cultura organizacional y su capacidad preventiva frente a riesgos digitales (Contraloría General de la República, 2023).

En Chile, la promulgación de la Ley Marco de Ciberseguridad N° 21.663 y la creación de la Agencia Nacional de Ciberseguridad (ANCI) marcan un hito en materia de protección de datos y de la infraestructura tecnológica crítica nacional. En este sentido, la Política Nacional de Ciberseguridad 2023–2028 establece como uno de sus pilares la necesidad de desarrollar una cultura de ciberseguridad sólida en los organismos públicos, promoviendo la formación y sensibilización de los funcionarios, la gestión del riesgo y la adopción de buenas prácticas institucionales (Gobierno de Chile, 2023). De esta forma, el Fondo de Solidaridad e Inversión Social (FOSIS) de Atacama, como servicio público que maneja información sensible de programas sociales y beneficiarios, enfrenta el desafío de alinear su cultura interna con dichos lineamientos nacionales.

La importancia de este trabajo de título radica en que aborda una dimensión humana y organizacional de la ciberseguridad, la cual suele ser menos visible frente a las soluciones tecnológicas, pero igual o más determinante en la gestión del riesgo.

Según el Observatorio Nacional de Ciberseguridad (2023), más del 60% de los incidentes digitales en el sector público se originan por errores humanos o desconocimiento de protocolos, lo que demuestra que el factor cultural es crítico para la sostenibilidad de la seguridad digital. En este contexto, elaborar una propuesta de mejoras, a partir de la evaluación de la cultura de ciberseguridad del FOSIS Atacama permitirá comprender las percepciones, actitudes y prácticas de sus funcionarios, así como identificar brechas respecto de la Política Nacional vigente.

Desde el punto de vista institucional, el resultado del trabajo busca generar recomendaciones estratégicas y operativas que orienten al FOSIS Atacama hacia una mejor gestión interna de la ciberseguridad. Estas recomendaciones estarán enfocadas en mejorar la capacitación del personal, fortalecer los canales de comunicación interna y fomentar la responsabilidad compartida en la protección de la información. Con ello, se pretende contribuir a la creación de una cultura organizacional resiliente, que integre la seguridad digital como un valor institucional transversal, en coherencia con las directrices de la ANCI y los objetivos de modernización del Estado.

La meta principal de este trabajo es proponer acciones concretas que fortalezcan la gestión institucional de ciberseguridad del FOSIS Atacama, promoviendo un entorno laboral más consciente, seguro y alineado con los estándares nacionales.

1.5. Estructura del trabajo

El Capítulo II, Marco Teórico, profundiza en los fundamentos conceptuales y el contexto normativo del trabajo. Se describe la estructura y misión del Ministerio de Desarrollo Social y Familia y del FOSIS. Adicionalmente, se desarrolla el marco conceptual de la ciberseguridad y se analiza en detalle el marco normativo chileno, incluyendo la Política Nacional de Ciberseguridad y la Ley Marco N° 21.663, finalizando con la definición de cultura organizacional y de ciberseguridad.

El Capítulo III, Metodología, detalla la hoja de ruta para el desarrollo del trabajo. Se expone el tipo el detalle de la metodología aplicada bajo un enfoque cualitativo, junto con

un diseño no experimental. Se define la población de estudio, correspondiente al censo de los funcionarios de FOSIS Atacama, y se describen las técnicas de recolección de datos, que combinan la revisión documental con la aplicación de una encuesta de diagnóstico.

El Capítulo IV, Desarrollo y Resultados, presenta la ejecución del diagnóstico. En esta sección se procesan y analizan los datos recopilados mediante la encuesta aplicada, identificando patrones, percepciones y comportamientos. El capítulo culmina con una síntesis de hallazgos que identifica las brechas específicas entre la cultura actual y los requerimientos normativos.

El Capítulo V, Propuesta de Mejora, constituye el aporte central de este trabajo. Basándose en los hallazgos del capítulo anterior, se formulan ejes estratégicos de intervención y acciones específicas. Se detalla un plan de implementación diseñado para fortalecer de manera práctica la cultura de ciberseguridad en FOSIS Atacama.

El último capítulo VI, presenta las Conclusiones y Recomendaciones, donde se sintetizan los resultados del trabajo, se evalúa el cumplimiento de los objetivos planteados y se entregan las reflexiones finales.

Finalmente, se incluye un reporte ejecutivo (Ver Anexo 2), respecto a la síntesis más relevante del Capítulo IV y Capítulo V, para ser entregado a la jefatura del FOSIS Atacama con el propósito de entregar una evidencia objetiva, simple y visual del trabajo realizado en dicho servicio público

CAPÍTULO II

MARCO TEÓRICO

Los servicios públicos son órganos administrativos encargados de satisfacer necesidades colectivas, de manera regular y continua (Ley 18.575, artículo 25, 2025). Sin perjuicio de la realización de las actividades necesarias para el cumplimiento de sus funciones propias, les corresponde según la ley, aplicar las políticas, planes y programas que apruebe el Presidente de la República a través de los respectivos ministerios, pues aún cuando fuesen creados para actuar en todo o parte de una región, siempre quedarán sujetos a las políticas nacionales y a las normas técnicas del respectivo sector. (SII, 2025)

2.1. Marco institucional del FOSIS

2.1.1. Ministerio de Desarrollo Social y Familia

Durante el gobierno del Presidente de la República, Eduardo Frei Montalva (1964-1970), nace la necesidad de desarrollar un organismo técnico, que guíe a la planificación de estrategias sociales enfocadas al desarrollo y fortalecimiento del capital humano presente en la Nación.

Por lo tanto, en el año 1965 se instaura en el país la Oficina de Planificación (ODEPLAN), cuya administración y dependencia está al mando de la Presidencia de la República de Chile.

Transcurridos dos años desde su formación, adquiere la calidad de servicio público descentralizado y con asignación de patrimonio propio. A consecuencia de este cambio se determina y facilita la creación de las Oficinas Regionales de Planificación, las cuales al transcurrir el tiempo pasan a denominarse Secretarías Regionales de Planificación y Coordinación (SERPLAC).

Posteriormente en el año 1990 y mediante el Decreto de Ley N° 18.899 del 19 de Julio, se transforma en el Ministerio de Planificación y Cooperación (MIDEPLAN).

En el marco de su nueva misión, MIDEPLAN amplía sus facultades y roles de manera progresiva a fin de realizar evaluaciones de políticas y programas públicos, en un trabajo coordinado con los Ministerios de Hacienda y Secretaría General de la Presidencia.

Ante este escenario, se potencia el Sistema Nacional de Inversiones, a fin de abarcar no sólo la evaluación previa de los proyectos que optan al financiamiento público, sino que también la evaluación posterior y el seguimiento de todos aquellos proyectos a los cuales el Estado asigna recursos.

Siguiendo lo anterior, y con la finalidad de producir mejoras en las atribuciones y facultades del Ministerio de Planificación y Cooperación, el ex Presidente de la República Sebastián Piñera Echeñique, en su primer gobierno, reemplaza a MIDEPLAN por el Ministerio de Desarrollo Social, posicionándose éste, como ente coordinador de todas las políticas sociales del país, articulando iniciativas interministeriales y fiscalizando su funcionamiento. Por tanto, el establecimiento del Ministerio de Desarrollo Social, posee como misión: "Contribuir en el diseño y aplicación de políticas, planes y programas en materia de desarrollo social, especialmente aquellas destinadas a erradicar la pobreza y brindar protección social a las personas o grupos vulnerables, promoviendo la movilidad e integración social. Asimismo, deberá velar por la coordinación, consistencia y coherencia de las políticas, planes y programas en materia de desarrollo social, a nivel nacional y regional y evaluar los estudios de pre inversión de los proyectos de inversión que solicitan financiamiento del Estado para determinar su rentabilidad social de manera que respondan a las estrategias y políticas de crecimiento y desarrollo económico y social que se determinen para el país" (Ministerio de Desarrollo Social y Familia, 2025).

El ex Presidente de la República Sebastián Piñera Echenique, en su segundo periodo en la presidencia y en conjunto con sus colaboradores y a través de la modificación del Decreto Ley Nº 20.530, el 16 de abril de 2019, crea el Ministerio de Desarrollo Social y Familia, con el objetivo de cambiar de forma radical las políticas sociales, colocando de esta forma a la familia como eje principal de intervención social.

La Ilustración 1: Cap. 2 Modificación de la Ley N° 20.530 muestra la modificación que amplía el sistema de protección del Ministerio de Desarrollo Social.

Ilustración 1: Cap. 2 Modificación de la Ley N° 20.530.


Biblioteca del Congreso Nacional de Chile Legislación chilena

Tipo Norma	:Ley 21150
Fecha Publicación	:16-04-2019
Fecha Promulgación	:02-04-2019
Organismo	:MINISTERIO DE DESARROLLO SOCIAL
Título	:MODIFICA LA LEY N° 20.530 Y CREA EL MINISTERIO DE DESARROLLO SOCIAL Y FAMILIA
Tipo Versión	:Única De : 16-04-2019
Inicio Vigencia	:16-04-2019
Id Norma	:1130640
URL	:https://www.leychile.cl/N?i=1130640&f=2019-04-16&p=

LEY NÚM. 21.150

MODIFICA LA LEY N° 20.530 Y CREA EL MINISTERIO DE DESARROLLO SOCIAL Y FAMILIA

Fuente: Biblioteca del Congreso Nacional de Chile.

Sumado a lo anterior, esta cartera ministerial cuenta con tres subsecretarías en el sector público, las cuales son:

- Subsecretaría de Evaluación Social.
- Subsecretaría de Servicios Sociales.
- Subsecretaría de la Niñez.

A continuación, en la Ilustración 2: Cap. 2 Nuevo logo del Ministerio de Desarrollo Social y Familia., se observan los logos modificados del Ministerio de Desarrollo Social y Familia.

Ilustración 2: Cap. 2 Nuevo logo del Ministerio de Desarrollo Social y Familia.

Fuente: www.fosis.cl

2.1.2. Fuentes de financiamiento para el desarrollo de emprendimientos

En la actualidad existe una amplia variedad de instituciones públicas y/o privadas, preocupados por apoyar las iniciativas y fortalecimientos de ideas de negocio, motivo por

el cual gestionan recursos y/o programas de capacitaciones, que permiten que los emprendedores, puedan contar con fácil acceso a estos beneficios y mejorar su situación socioeconómica mediante el desarrollo de trabajos por cuenta propia.

A continuación, se detallan algunas de las instituciones que apoyan a emprendedores/as en las áreas de financiamiento, capacitación y regularización: (Portal PYME, s.f.)

- FOSIS (Fondo de Solidaridad e Inversión Social): es un servicio dependiente del Ministerio del Desarrollo Social y Familia, que apoya a las personas en situación de pobreza o vulnerabilidad que buscan mejorar su calidad de vida. Según las necesidades, implementa programas en tres ejes de acción: expansión de capacidades, bienestar comunitario e inversión para las oportunidades.

- SERCOTEC (Servicio de Corporación Técnica): esta es una de las instituciones que promueven y apoyan iniciativas para las micro y pequeñas empresas, especialmente para fortalecer los procesos de gestión, asimismo entrega apoyo a emprendedores y emprendedoras para plasmar sus ideas de negocio. Cuenta con seminarios, talleres y plataformas de financiamiento, dentro de sus principales requisitos está la formalización de sus beneficiarios.

- CORFO (Servicio de Fomento y la Producción): Es un servicio del gobierno, dependiente del Ministerio de Economía, Fomento y Turismo, con la responsabilidad de apoyar el emprendimiento, la innovación y competitividad en el país, además de fortalecer el capital humano y las capacidades tecnológicas.

- SENCE (Servicio Nacional de Capacitación y Empleo): es un organismo técnico del Estado, funcionalmente descentralizado, con personalidad jurídica de derecho público, que se relaciona con el Gobierno a través del Ministerio del Trabajo y Previsión Social, esta entidad contribuye a la generación de empleo, permitiendo un dinamismo en el mercado laboral. Además, está enfocado en el desarrollo de capital humano mediante la aplicación de políticas públicas de fomento e intermediación laboral y de capacitación.

- CONADI (Corporación Nacional de Desarrollo Indígena): esta organización no está enfocada exclusivamente al emprendimiento, pero promueve, gestiona y ejecuta proyectos que favorezcan el desarrollo integral de las personas y comunidades indígenas dentro del país, especialmente en lo económico, social y cultural y de impulsar su participación en la vida nacional, a través de la coordinación intersectorial, el financiamiento de iniciativas de inversión y la prestación de servicios a usuarios y usuarias.

- ANID (Agencia Nacional De Investigación Y Desarrollo) anteriormente CONICYT (Comisión Nacional de Investigación Científica y Tecnológica): es una corporación que busca, promueve y fortalece la investigación científica y tecnológica en Chile, con la finalidad de colaborar con el desarrollo económico, social y cultural. Es por ello que impulsa el desarrollo de capital humano en base a temas científicos y tecnológicos, mediante becas y concursos.

- SUBDERE (Subsecretaría de Desarrollo Regional y Administrativo): esta entidad, por medio del Fondo Nacional de Desarrollo Regional (FNDR), busca fomentar el emprendimiento en todas las regiones de Chile.

- INDAP (Instituto de Desarrollo Agropecuario): es el principal servicio del Estado de Chile en apoyo de la agricultura familiar campesina. Su objetivo es el fomento productivo, lo que significa, asignar recursos para el fortalecimiento del capital humano y financiero a través de la entrega de herramientas que permiten superar la pobreza, promover la sostenibilidad y competitividad en la agricultura nacional de esta manera convertir la agricultura familiar en unidades productivas autosustentables.

Ilustración 3: Cap. 2 Logos de instituciones que apoyan a emprendedores.

Fuente: Elaboración propia.

2.1.3. Fondo de Solidaridad e Inversión Social (FOSIS)

El Fondo de Solidaridad e Inversión Social, FOSIS, es un servicio del Gobierno de Chile, creado el 26 de octubre de 1990. Cuenta con 16 direcciones regionales y 20 oficinas provinciales; y se relaciona con la Presidencia de la República a través del Ministerio de Desarrollo Social y Familia.

Según lo dispuesto en la Ley Orgánica del FOSIS, la dirección de la institución corresponde a un Consejo que será la autoridad superior del Servicio. Este Consejo delega sus funciones y atribuciones en el director Ejecutivo del FOSIS. (Sitio oficial de FOSIS, 2025)

La Ilustración 4: Cap. 2 Logo de FOSIS. , muestra el logo institucional del Fondo de Solidaridad e Inversión Social, FOSIS.

Ilustración 4: Cap. 2 Logo de FOSIS.

Fuente: www.fosis.gob.cl.

A continuación, en la Ilustración 5 Cap. 2 Organigrama del FOSIS., se presenta el organigrama del Fondo de Solidaridad e Inversión Social.

Ilustración 5 Cap. 2 Organigrama del FOSIS.

Fuente: www.fosis.gob.cl.

2.1.4. FOSIS Atacama

El Fondo de Solidaridad e Inversión Social, FOSIS, en la región de Atacama cuenta con oficinas en la comuna de Copiapó, estas se encuentran ubicadas en calle Maipú N° 580 y en Vallenar en Fáez N° 1343. La actual directora es la señora Paloma Fernández Valdés, de profesión psicóloga, trabajó entre el 2008 y el 2015 en el Servicio de Salud de Atacama y fue jefa de la carrera de Psicología en la Universidad Santo Tomás, además de ser docente de esa casa de estudios y de la Universidad de Atacama. Entre el 2016 y el 2021, fue concejala de Copiapó. La siguiente ilustración muestra la oficina donde opera FOSIS ubicada en la calle Maipú N° 580.

Ilustración 6 Cap. 2 Oficina de FOSIS en Copiapó.

Fuente: www.fosis.gob.cl

2.1.5. Tipos de programas

El Fondo de Solidaridad e Inversión Social, en el marco de su misión y bajo la dependencia del Ministerio de Desarrollo Social y Familia, gestiona y planifica recursos a través de un conjunto de programas, para brindar beneficios a personas y familias que requieran apoyo para mejorar sus condiciones de vida. (FOSIS, 2022) A continuación, se presentan algunos de los diferentes y principales tipos de programas sociales:

Programas para la autonomía económica:

- Emprendamos Semilla: dirigido a quienes quieren desarrollar un negocio o fortalecer un pequeño emprendimiento en funcionamiento. Se obtienen los siguientes beneficios
- Capacitaciones
- Financiamiento para tu idea de negocio o negocio.
- Acompañamiento para mejorar tu emprendimiento.
- Servicio de cuidado infantil durante las actividades grupales.
- Material didáctico y educativo.

Los requisitos principales para postular son:

- Ser mayor de 18 años.
- Estar en los tramos de mayor vulnerabilidad según el Registro Social de Hogares
- Estar sin trabajo o tener un empleo precario.
- Tener una idea de negocio o un pequeño negocio en funcionamiento.
- Tener cédula de identidad y clave única.

- Emprendamos: potencia el emprendimiento, aprovechando las oportunidades del mercado y el contacto con otras instituciones que puedan ayudar a crecer, también se enseña a usar herramientas para gestionar mejor el negocio del beneficiado para que aumente los ingresos que generan. Dicho programa cuenta con una versión básica y otra avanzada, las que se diferencian según el nivel desarrollo del negocio, asociado a las ventas, antigüedad y formalización, entre otras variables. Se obtienen los siguientes beneficios:
- Capacitación en temas como comercialización, marketing digital, formalización, innovación, entre otros.
- Sesiones de asesoría personalizadas y acompañamiento.
- Financiamiento para tu emprendimiento.
- Material didáctico y educativo.
- Servicio de cuidado infantil durante las actividades grupales.

Los requisitos principales para postular son:

- Ser mayor de 18 años.
- Estar en los tramos de mayor vulnerabilidad según el Registro Social de Hogares
- Tener un negocio en funcionamiento.
- Tener cédula de identidad y clave única.

- Emprendamos Grupal: apoya a organizaciones o grupos productivas a fortalecer su actividad económica a través de capacitación, asesoría y financiamiento de sus propios proyectos. Se obtienen los siguientes beneficios:

- Capacitaciones y asesorías.
- Financiamiento para la compra de materiales, insumos o herramientas de un plan de financiamiento.

Los requisitos principales para postular son:

- Ser mayor de 18 años.
- Estar en los tramos de mayor vulnerabilidad según el Registro Social de Hogares.
- Tener un negocio en funcionamiento.
- Tener cédula de identidad y clave única.

- Emprendamos Ferias: dirigido a personas que tienen un negocio o emprendimiento en funcionamiento y requieren espacios de comercialización. Se obtienen los siguientes beneficios:
- Capacitación en temas como comercialización presencial y digital.
- Sesiones de asesoría personalizadas y acompañamiento.
- Financiamiento para tu emprendimiento.
- Participación en ferias de emprendimiento.

Los requisitos principales para postular son:

- Ser mayor de 18 años.
- Tener formalización.
- Estar participando o haber participado en un programa de emprendimiento del FOSIS.
- Tener stock para instalarse en un espacio de comercialización.

- Acceso al microcrédito: el FOSIS, mediante convenios con instituciones de microfinanzas, facilita la obtención de créditos para personas microemprendedoras. Este programa está dirigido a personas emprendedoras que tienen dificultades de financiamiento para sus pequeños negocios. Se obtiene el siguiente beneficio:

- Acceso a créditos por montos de hasta $500.000.

Los requisitos principales para postular son:

- Ser mayor de 18 años.
- Estar en los tramos de mayor vulnerabilidad según el Registro Social de Hogares.
- Tener un negocio en funcionamiento.
- Manifestar el consentimiento de ser contactados por personal de una institución de microfinanzas.

Programas de Cohesión Social

- Acción local: este programa busca aumentar las capacidades de las comunidades para que mejoren su bienestar, a través de la participación y el trabajo conjunto. Está dirigido a las comunidades que habitan en barrios vulnerables. Se obtienen los siguientes beneficios:

- Tener una comunidad organizada, capaz de sacar sus proyectos adelante.
- Financiamiento para una iniciativa local.
- Concretar alianzas público-privadas para que la comunidad se beneficie.

Puede ser seleccionado un barrio donde el 60% o más de los hogares se encuentra en el 40% más vulnerable según el Registro Social de Hogares. A este programa no se

postula. Los hogares son invitados a participar por una institución ejecutora, según una evaluación previa del FOSIS.

- EcoMercados solidarios: los EcoMercados Solidarios recuperan, almacenan y distribuyen alimentos que no serán comercializados por supermercados o ferias libres, entre otros, y entrega a familias vulnerables alimentos gratuitos, para aportar a la seguridad alimentaria y paliar el encarecimiento de la canasta básica de alimentos. La gestión de cada EcoMercados Solidario cuenta con el protagonismo de las comunidades organizadas, que se coordinan con la municipalidad y otros actores público-privados del territorio. Los EcoMercados solidarios apoyan a hogares con jefatura de hogar de mujeres que viven en situación de pobreza o pobreza extrema y que no tienen acceso adecuado a alimentos en calidad y cantidad. Además, se priorizan los hogares que tienen personas que requieren de cuidados.

  A este programa no se postula. Los hogares que cumplen con estos requisitos son invitados a participar por el municipio. Y se implementan en varias comunas del país.

- Juntos más barato: es una iniciativa del FOSIS que busca fortalecer la cohesión social y mejorar la economía familiar mediante un modelo de educación financiera y compras colectivas. A través de este programa, familias y organizaciones comunitarias se organizan para adquirir alimentos, implementos de higiene y otros productos de primera necesidad a precios más bajos, aprovechando la compra al por mayor y generando ahorros significativos en el presupuesto del hogar. Está dirigido a jefas y jefes de hogar, organizaciones comunitarias y comunidades en general, que deseen sumarse a un modelo de consumo más justo y solidario. Se obtienen los siguientes beneficios:

- Acceso a productos básicos a precios más convenientes.
- Ahorro promedio de hasta un 30% en la canasta familiar.
- Formación en educación financiera y optimización de presupuestos.
- Fortalecimiento de la organización comunitaria y redes locales.
- Participación en un modelo solidario que favorece el bienestar colectivo.

Programas de Cohesión Social

- Programa habitabilidad: este programa mejora las condiciones en que habitan familias del subsistema Seguridades y Oportunidades. Es ejecutado principalmente por municipios, con recursos del Ministerio de Desarrollo Social y Familia y con la asistencia técnica del FOSIS para asegurar buenos resultados. Está dirigido a familias que pertenecen al subsistema Seguridades y Oportunidades. Se obtienen los siguientes beneficios:

- Soluciones constructivas para mejorar servicios básicos, infraestructura de la vivienda, entorno residencial o equipamiento doméstico.
- Asesorías para el uso, cuidado y mantención de la vivienda.
- Sesiones de asesorías familiares o grupales en hábitos de vida saludable y de uso y autocuidado de la vivienda.

Los requisitos principales son:

- Formar parte del subsistema Seguridades y Oportunidades.
- Tener problemas en la dimensión de habitabilidad.

A este programa no se postula.

Programa apoyo a seguridad alimentaria: este programa apoya a que las familias o comunidades accedan a alimentos saludables a través de la implementación de tecnologías que faciliten la obtención de alimentos para consumo propio. Para ello, entrega técnicas de cultivo, crianza, pesca, recolección, elaboración, purificación de agua o preparación y conservación de alimentos y capacitaciones en alimentación y nutrición.

- Se obtienen los siguientes beneficios:

- Taller de implementación de tecnologías.
- Tecnologías para la autoprovisión de alimentos.
- Capacitación en alimentación y nutrición.
- Talleres comunales para grupos de familias.
- Sesiones familiares de asesoría y seguimiento.
- Apoyo para producir o conservar alimentos.
- Desarrollo de espacios comunitarios de autoproducción.

- Material didáctico y educativo.

Los requisitos principales son:

- Formar parte del subsistema Seguridades y Oportunidades.
- Tener problemas de disponibilidad de alimentos saludables.

2.2. Marco Conceptual de Ciberseguridad

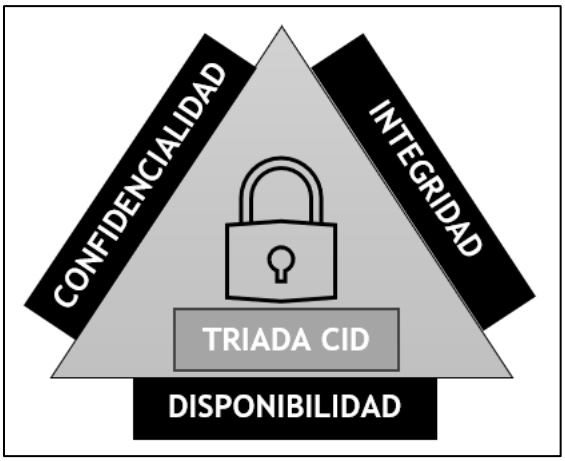
Para el correcto entendimiento de este trabajo, es necesario familiarizarse con cada uno de los conceptos, siglas e identidades que se verán mencionadas a continuación.

2.2.1. Ciberseguridad

El concepto de ciberseguridad es el eje central de este trabajo. El Comité de Sistemas de Seguridad Nacional (CNSS) de Estados Unidos lo define como la "prevención de daños, protección y restauración de computadoras, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para asegurar su disponibilidad, integridad, autenticidad, confidencialidad y no repudio". También se entiende por ciberseguridad como la "habilidad de proteger o defender el uso del ciberespacio de ataques cibernéticos", definición más corta dada por el propio NIST (National Institute of Standards and Technology. Information Security ., 2023). Entiéndase ciberespacio como "dominio global dentro del entorno de la información que consiste en la red independiente de infraestructuras de sistemas de información que incluyen Internet, redes de telecomunicaciones, sistemas computacionales y procesadores y controladores integrados".

La ciberseguridad tiene tres pilares fundamentales: Confidencialidad, Integridad y Disponibilidad. Estos tres conceptos forman lo que se conoce como la "triada CID" ´ o CIA, en inglés (Fortinet. Tríada CIA: confidencialidad, integridad y disponibilidad. Ed. por, 2025).

Ilustración 7 Cap. 2 La triada CID.



Fuente: Elaboración propia

- Confidencialidad: los datos de un usuario no se filtran a entidades no autorizadas.
- Integridad: los datos deben ser confiables y libres de alteraciones.
- Disponibilidad: garantizar que el usuario autorizado podrá acceder a la información cuando sea necesario.

Un buen sistema que contemple la seguridad debe satisfacer estos tres elementos. Si un sistema de seguridad de información carece de sólo uno de estos elementos, entonces se considera un sistema insuficiente.

2.2.2. Conceptos claves de ciberseguridad

1. Ataque

Uno de los conceptos que más se repiten dentro del mundo de la ciberseguridad es el ataque, el cual se define como "cualquier tipo de actividad maliciosa que intente recopilar, interrumpir, negar, degradar o destruir los recursos del sistema de información o la información en sí".

2. Hacker malicioso

El término Hacker a menudo se asocia hacia una persona con grandes capacidades y conocimientos computacionales que utiliza ese conocimiento para realizar actos ilícitos.

Sin embargo, esto no es correcto, ya que la definición de hacker, según la RAE, es un "experto en informática, capaz de acceder a un sistema sin autorización, normalmente para detectar sus fallos de seguridad y desarrollar mejoras". Por otro lado, hacker malicioso o cibercriminal es un término utilizado para describir a un "individuo o grupo que usa el entendimiento de sistemas, redes y programación para acceder a sistemas de forma ilegal, causar daños o robar información".

3. Vulnerabilidad

Según la Real Academia Española (RAE), se define que algo es vulnerable como algo que puede ser "herido o recibir lesión física o moralmente". Esta definición encaja bien con el concepto de vulnerabilidad en el mundo de la ciberseguridad, ya que esta se define formalmente como "debilidad en un sistema de información, procedimientos de sistemas de seguridad o implementación que podría ser explotada o desencadenada por una fuente de amenaza"

4. Encriptación y desencriptación

La encriptación se define como "transformación criptográfica de datos para producir un texto cifrado". Esta acción transforma data inteligible (texto plano) a una forma ininteligible (texto cifrado). Esto puede ser revertido a través del proceso de desencriptación.

5. Phishing

En esencia, el phishing es una técnica de ingeniería social utilizada por ciberdelincuentes con la finalidad de obtener datos relevantes y confidenciales de sus víctimas (por ejemplo, credenciales de acceso a cuentas o datos bancarios) (Cano Teruel, 2021).

El ataque se lleva a cabo mediante la suplantación de identidad de una entidad de confianza (como un banco, una red social o una empresa conocida) para enviar mensajes fraudulentos generalmente por correo electrónico, SMS o llamadas telefónicas que instan a la víctima a realizar una acción urgente, como hacer clic en un enlace malicioso o ingresar información personal en un sitio web falso.

2.3. Marco Normativo

2.3.1. **Política Nacional de Ciberseguridad** (Ciberseguridad, 2017)

En el año 2017, se oficializó en Chile la primera Política Nacional de Ciberseguridad 2017-2022, la cual presentó dos políticas sobre la implementación de objetivos de largo plazo para lograr un ciberespacio más seguro, cuyos objetivos específicos incluyeron el desarrollo de una infraestructura de información robusta para resistir y recuperarse de incidentes cibernéticos, desarrollar una industria nacional de ciberseguridad y participar en foros internacionales.

Luego esta política se actualiza, dando lugar a la Política Nacional de Ciberseguridad 2023-2028, la cual entró en vigor el 4 de diciembre del 2023 y trae consigo 5 objetivos (ANCI - "PNSC 2023-2028", 2025):

1. Infraestructura resiliente: El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos. Esto será a través del fortalecimiento de los elementos técnicos físicos y lógicos del ciberespacio, incluida la creciente red de dispositivos conectados a Internet.

2. Derecho de las personas: El Estado resguardará y promoverá la protección de los derechos de las personas en Internet, a través del fortalecimiento de la institucionalidad pública en materia de ciberseguridad; y de la generación, adopción, y promoción de los mecanismos y las herramientas tecnológicas suficientes para que cada persona pueda integrarse a la sociedad, desarrollarse y expresarse plenamente, otorgando especial protección a mujeres, niñas, niños, adolescentes, adultos mayores y disidencias sexogenéricas. Todas las personas deberían poder hacer uso de Internet para comunicarse, trabajar, estudiar, y desarrollarse en lo personal, familiar y social en un entorno de equidad, inclusión, justicia y protección a la diversidad. En este objetivo se busca proteger los datos personales, generar instancias de capacitación sobre hábitos y medidas básicas de seguridad digital, prevenir la comisión de delitos

informáticos, e identificar y corregir inequidades en el acceso y uso del ciberespacio producidas por falta de conocimiento de seguridad digital.

3. Cultura de Ciberseguridad: Desarrollar una cultura de la ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas. La protección de la sociedad va en directa relación con la capacidad que tenga cada persona de protegerse. Se requiere generar nociones y prácticas de ciberhigiene (adquirir una serie de buenos hábitos en torno a la ciberseguridad y, así, estar un paso por delante de las ciberamenazas y los problemas de seguridad online en la población, de forma que cada uno sea capaz de cuidar por sí mismo su identidad digital y su información.

4. Coordinación nacional e internacional: Es indispensable la acción coordinada e intencionada hacia la consecución de los objetivos de la política pública. Los organismos públicos y privados promoverán instancias de cooperación con el resto del sector público y de la industria, y con la futura autoridad nacional de ciberseguridad, con especial énfasis en la comunicación y difusión de los esfuerzos que se realicen en ciberseguridad, a fin de evitar la duplicación de trabajo y pérdida de recursos.

5. Fomento de la industria y la investigación científica: Se promoverá el desarrollo de una industria de la ciberseguridad, que proteja a las personas y las organizaciones y que sirva a sus objetivos estratégicos. Este fomento se implementará a través de estímulos y fondos dirigidos a la oferta de servicios y productos en ciberseguridad, pero también a través de la generación de una demanda más sofisticada en ciberseguridad, de forma que la industria nacional pueda proteger de mejor forma a las personas y organizaciones, y servir mejor a los intereses del país.

Esta nueva versión de la PNC fomentó la aprobación de la Ley Marco de Ciberseguridad.

2.3.2. **Ley Marco de Ciberseguridad** (Ciberseguridad, 2017)

Esta ley, consecuencia de la PNC 2023-2028, establece el marco regulatorio legal que regula a instituciones públicas y privadas que sean calificadas como esenciales y/u operadores de importancia vital.

- Servicios esenciales: Aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional; los prestados bajo concesión de servicio público, y los proveídos por instituciones privadas que realicen las siguientes actividades: generación, transmisión o distribución eléctrica; transporte, almacenamiento o distribución de combustibles; suministro de agua potable o saneamiento; telecomunicaciones; infraestructura digital; servicios digitales y servicios de tecnología de la información gestionados por terceros; transporte terrestre, aéreo, ferroviario o marítimo, así como la operación de su infraestructura respectiva; banca, servicios financieros y medios de pago; administración de prestaciones de seguridad social; servicios postales y de mensajería; prestación institucional de salud por entidades tales como hospitales, clínicas, consultorios y centros médicos, y la producción y/o investigación de productos farmacéuticos.
- Operadores de importancia vital: Aquellos que la provisión de dicho servicio dependa de las redes y sistemas informáticos, y que la afectación, interceptación, interrupción o destrucción de sus servicios tenga un impacto significativo en la seguridad y el orden público, en la provisión continua y regular de servicios esenciales, en el efectivo cumplimiento de las funciones del Estado o, en general, de los servicios que este debe proveer o garantizar.

Las instituciones anteriormente mencionadas deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas instituciones serán reguladas por la Agencia Nacional de Ciberseguridad (ANCI), la cual, además de regular, también fiscaliza y sanciona, en caso necesario, a los organismos descritos.

Esta ley también impulsa la creación de un Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT Nacional) dentro de la ANCI.

2.3.3. CSIRT Nacional

El Equipo Nacional de Respuesta a Incidentes de Seguridad Informática o CSIRT Nacional (*Computer Security Incident Response Team*, por sus siglas en inglés) se define en la Ley Marco de Ciberseguridad como:

“Centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos”.

En el 2019, el Departamento del Interior y Seguridad Pública proclamó una resolución que establecía una subdivisión llamada Unidad de Coordinación de Ciberseguridad. Luego, este departamento se amplió y actualizó en el 2023, creando el CSIRT Nacional.

Las funciones definidas por la Ley Marco de Ciberseguridad que el CSIRT debe realizar son las siguientes:

1. Responder ante ciberataques o incidentes de ciberseguridad, cuando estos sean de efecto significativo.
2. Coordinar a los CSIRT que pertenezcan a organismos de la Administración del Estado frente a ciberataques o incidentes de ciberseguridad de efecto significativo. La misma coordinación deberá establecer con el CSIRT de la Defensa Nacional. En el ejercicio de esta función, el CSIRT Nacional podrá realizar todas las acciones necesarias para asegurar una respuesta rápida, incluida la supervisión de las medidas adoptadas por estos.
3. Servir de punto de enlace con Equipos de Respuesta a Incidentes de Seguridad Informática extranjeros o sus equivalentes para el intercambio de información de ciberseguridad, siempre dentro del marco de sus competencias.
4. Prestar colaboración o asesoría técnica a los CSIRT que pertenezcan a organismos de la Administración del Estado en la implementación de políticas y acciones relativas a ciberseguridad.
5. Supervisar incidentes a escala nacional.
6. Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.
7. Realizar entrenamiento, educación y capacitación en materia de ciberseguridad.

8. Requerir a las instituciones afectadas o a los CSIRT correspondientes, información anonimizada de incidentes de ciberseguridad y vulnerabilidades encontradas y los planes de acción respectivos para mitigarlos.
9. Difundir alertas tempranas, avisos e información sobre riesgos e incidentes para la comunidad.
10. Elaborar un informe con los criterios técnicos para la determinación de las categorías de incidentes o vulnerabilidades de ciberseguridad que estarán eximidas de notificación.

Actualmente, el CSIRT forma parte de la Agencia Nacional de Ciberseguridad, la cual entró en funcionamiento el 1 de enero del 2025.

2.3.4. Agencia Nacional de Ciberseguridad (ANCI)

La ANCI se creó en la Ley Marco de Ciberseguridad. Esta agencia es un servicio público de carácter técnico y especializado, funcionalmente descentralizado y dotado de personalidad jurídica y patrimonio propio que se relaciona con el Presidente de la República por intermedio del ministerio encargado de la Seguridad Pública.

Las principales funciones de esta entidad son:

- Asesorar al Presidente de la República en la elaboración y aprobación de la Política Nacional de Ciberseguridad.
- Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de ciberseguridad.
- Coordinar y supervisar al CSIRT Nacional.
- Establecer una coordinación con el CSIRT de la Defensa Nacional en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades, y respecto a las materias que serán objeto de intercambio de información.
- Calificar a los servicios esenciales y operadores de importancia vital.

- Diseñar e implementar planes y acciones de formación ciudadana, capacitación, fortalecimiento, difusión y promoción de la cultura en ciberseguridad.
- Cooperar con organismos públicos e instituciones privadas, en materias propias de su competencia, sin perjuicio de las atribuciones de otros organismos del Estado.
- Otorgar y revocar acreditaciones correspondientes a los centros de certificación, en los casos y bajo las condiciones que establezca la ley y el reglamento respectivo.
- Fomentar la investigación, innovación, capacitación y entrenamiento frente a amenazas, vulnerabilidades e incidentes de ciberseguridad y, en conjunto con los Ministerios de Economía, Fomento y Turismo, y de Ciencia, Tecnología, Conocimiento e Innovación, diseñar planes y acciones que fomenten el desarrollo o fortalecimiento de la industria de ciberseguridad local.
- Certificar el cumplimiento de los estándares de ciberseguridad correspondientes por parte de los organismos de la Administración del Estado.
- Establecer los estándares que deberán cumplir las instituciones que provean bienes o servicios al Estado, y las normas de seguridad para el desarrollo de los sistemas y programas informáticos que serán utilizados por los organismos del Estado.
- Establecer estándares de ciberseguridad y deberes de información al público sobre riesgos de ciberseguridad de dispositivos digitales disponibles a consumidores finales.
- Administrar la Red de Conectividad Segura del Estado.

Este servicio entró en funcionamiento el 1 de enero del 2025, haciendo que el CSIRT Nacional, que ya estaba en funcionamiento, pasara a ser parte integral de la ANCI, siendo supervisado por esta misma.

2.3.5. Las Leyes 21.719 y 19.628

El 18 de agosto de 1999 se promulgó la ley N° 19.628 sobre protección de la vida privada, la cual fue publicada el 28 de agosto del mismo año. Esta normativa regula cómo las empresas y el Estado pueden tratar los datos personales de las personas. Recientemente, el 13 de diciembre del 2024, dicha ley fue modificada por la ley N° 21.719, que regula la

protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Esta actualización incorporó y reformuló diversos artículos de la ley N° 19.628, destacando la introducción de principios y la inclusión de multas y sanciones.

Entre las diversas modificaciones, destaca la realizada al artículo 3°, el cual incorporó 8 principios que se deben regir para el tratamiento de los datos personales. Entre ellos, el Principio de seguridad es especialmente relevante para este trabajo, ya que establece que el responsable del tratamiento de los datos personales debe: "garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos." (Artículo 3°, literal f).

Adicionalmente, a la Ley N° 19.628 se incorporaron multas, las cuales se aplican en caso de que, durante operaciones de tratamiento de datos personales, se vulneren los principios señalados en el artículo 3°, así como los derechos y las obligaciones establecidos en normativa. Para ello, se definieron 3 categorías de infracciones: leves, graves y gravísimas, cuyas multas, estipuladas en el artículo 5°, alcanzan hasta 5.000, 10.000 y 20.000 Unidades Tributarias Mensuales (UTM), respectivamente.

Cabe señalar que todas las modificaciones introducidas por la Ley 21.719 aún no entran en vigencia. Según lo dispuesto en el artículo 1° de esta normativa, estas modificaciones entrarán en vigor 24 meses después de la publicación de la ley en el Diario Oficial, es decir, el 1 de diciembre del 2026.

2.3.6. Ley de Transformación Digital del Estado

La Ley n°21.180 impulsa que el ciclo completo de los procedimientos administrativos de todos los órganos de la Administración del Estado sujetos a Ley de Bases de Procedimiento Administrativo (19.880), se realice en formato electrónico. Esto permitirá otorgar mayor certeza, seguridad y velocidad en la entrega de servicios a las personas, junto con una mayor transparencia de los procesos y actuaciones del Estado en su relación con los ciudadanos. La ley aplica a Ministerios, intendencias, gobernaciones y los servicios públicos creados para el cumplimiento de la función administrativa, Contraloría

General de la República, a las Fuerzas Armadas y a las Fuerzas de Orden y Seguridad Pública, a los gobiernos regionales y a las municipalidades, según lo dispuesto en el artículo 2° de la Ley N° 19.880, que establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.

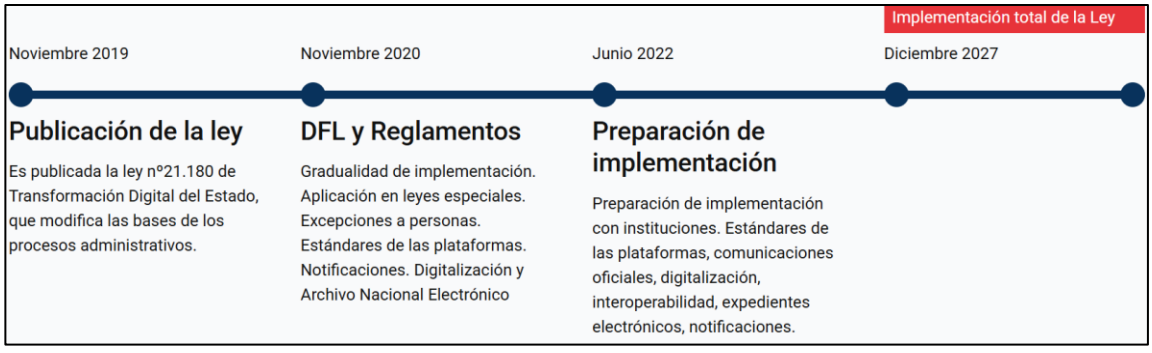
Ejes de la ley de Transformación Digital del Estado

Ilustración 8 Cap. 2 Ejes de la ley de transformación digital

Fuente: www.digital.gob.cl

Etapas de la ley

Ilustración 9 Cap. 2 Etapas de la ley.



Fuente: www.digital.gob.cl

2.4. Cultura Organizacional y de Ciberseguridad

2.4.1. Cultura Organizacional

La cultura organizacional es un pilar fundamental para entender el comportamiento dentro de una institución. Idalberto Chiavenato (2009) la define como “el conjunto de hábitos, creencias, valores y tradiciones, interacciones y relaciones sociales típicos de cada organización”. Por su parte, Edgar Schein (2010), uno de los principales teóricos en la materia, la define como "un patrón de supuestos básicos compartidos que el grupo aprendió a medida que resolvía sus problemas de adaptación externa e integración interna". Schein propone tres niveles de análisis: artefactos (visible), valores adoptados (declarado) y supuestos básicos subyacentes (inconsciente), siendo este último el más profundo y determinante del comportamiento real.

2.4.2. Cultura de Ciberseguridad

Este concepto se refiere a una subcultura dentro de la organización. Information Systems Audit and Control Association (ISACA) la define como “los conocimientos, creencias, percepciones, actitudes, supuestos, normas y valores de las personas en relación con la ciberseguridad y cómo se manifiestan en su comportamiento con los sistemas de información” (ISACA, 2018). En esencia, es la suma de comportamientos individuales que contribuyen a la seguridad global de la organización. Una cultura sólida transforma la ciberseguridad de una simple función técnica a una responsabilidad compartida por todos.

2.4.3. Importancia de la Cultura Organizacional

La cultura es un factor determinante en el éxito o fracaso de una organización. Autores como Deal y Kennedy (1982) argumentan que una cultura fuerte, donde los valores son compartidos intensamente por sus miembros, se correlaciona directamente con un mayor rendimiento. La cultura guía el comportamiento de los empleados en ausencia de reglas formales, influye en la moral, el compromiso y la capacidad de adaptación al cambio, convirtiéndose en un activo estratégico intangible, pero de gran valor.

2.4.4. Importancia de la Cultura de Ciberseguridad en el Sector Público

En el sector público, esta importancia se magnifica. Las instituciones manejan datos sensibles de los ciudadanos y la continuidad de sus servicios es crítica. Un ciberataque puede paralizar la entrega de beneficios sociales, afectando a la población más vulnerable. Dado que el "factor humano" es la causa principal de la mayoría de los incidentes (Observatorio Nacional de Ciberseguridad, 2023), fortalecer la cultura transforma a cada funcionario en una primera línea de defensa activa.

2.5. Antecedentes de Ciberataques en el Sector Público

La relevancia de una cultura de ciberseguridad se evidencia al analizar incidentes reales que han afectado al Estado de Chile, demostrando que ninguna entidad es inmune.

- **Caso Estado Mayor Conjunto (EMCO):** En septiembre de 2022, el grupo hacktivista "Guacamaya" filtró más de 400.000 correos electrónicos de las Fuerzas Armadas de Chile. El análisis posterior reveló que el punto de entrada fue una vulnerabilidad en el servidor de correo electrónico de la institución, exponiendo información sensible sobre seguridad nacional y operaciones estratégicas (Ciper Chile, 2022). Este incidente subrayó las debilidades en la gestión de vulnerabilidades y la falta de protocolos robustos.
- **Caso Poder Judicial:** En agosto de 2023, un ataque de ransomware afectó los sistemas informáticos del Poder Judicial, encriptando información y alterando el funcionamiento de tribunales a lo largo del país. El ataque se propagó a través de un archivo malicioso abierto por un funcionario, lo que evidencia la efectividad de las tácticas de ingeniería social y la necesidad crítica de capacitación continua al personal (CSIRT de Gobierno, 2023).

- **Ataques a Municipios:** Diversas municipalidades han sido víctimas de ataques de ransomware, como fue el caso de la Municipalidad de La Florida en 2024, donde los atacantes exigieron un rescate para liberar los datos secuestrados. Estos eventos no solo interrumpen servicios básicos para los ciudadanos, como el pago de permisos de

circulación, sino que también exponen datos personales de los vecinos, generando una crisis de confianza (Meganoticias, 2024).

- **Caso FOSIS (Suplantación de Identidad):** En septiembre de 2025, se registró un caso de ingeniería social dirigido a una funcionaria de FOSIS de la región de Antofagasta. Un atacante, haciéndose pasar por un director regional, contactó a la víctima vía teléfono de la institución y la convenció de continuar la comunicación por WhatsApp bajo un pretexto técnico. A continuación, el atacante envió un código de verificación de 6 dígitos al teléfono de la funcionaria y la persuadió para que lo compartiera. Con este código, los ciberdelincuentes tomaron control de su cuenta de WhatsApp, usándola para estafar a sus contactos solicitando dinero. Este incidente resalta cómo la manipulación psicológica puede eludir las defensas técnicas, convirtiendo a los funcionarios en la puerta de entrada para los atacantes. (Sitio oficial de FOSIS, 2025)

Estos casos demuestran un patrón claro: las vulnerabilidades técnicas a menudo se combinan con fallos humanos, desde la falta de actualización de sistemas hasta la caída en trampas de phishing. Esto refuerza la idea de que la tecnología por sí sola es insuficiente, y que fortalecer la cultura de ciberseguridad es una necesidad estratégica e impostergable para el sector público.

CAPÍTULO III

METODOLOGIA

Para construir una propuesta de mejora que fuera útil para la realidad de FOSIS Atacama, era necesario definir una ruta clara y definida. Este capítulo presentó precisamente esa hoja de ruta, es decir, la metodología que guiaría cada paso del trabajo, explicando cómo se abordaría, a quiénes involucraría y qué se utilizaría para entender de buena manera la cultura de ciberseguridad actual y así poder proponer recomendaciones efectivas.

A continuación, se detalla el enfoque metodológico que se siguió para la elaboración de la propuesta de mejora de la cultura de ciberseguridad en FOSIS Atacama, donde se describe el enfoque, el diseño del marco investigativo, la población y muestra, las técnicas de recolección de datos y el procedimiento para realizar el diagnóstico de la situación actual, y, finalmente la elaboración de la propuesta de mejora.

3.1. Tipo de investigación, enfoque y diseño metodológico

Este trabajo nació con un propósito eminentemente práctico: proponer recomendaciones y soluciones concretas ante un desafío institucional. Por ello, la investigación fue de tipo aplicada, ya que no se limitó a la teoría, sino que buscó generar un impacto real.

Para lograrlo, fue necesario trascender los aspectos puramente técnicos para enfocarse en la dimensión humana de la ciberseguridad, motivo por el cual se optó por un enfoque mixto (cualitativo-cuantitativo). Esta metodología permitió recopilar, interpretar y comprender las percepciones, conocimientos y motivaciones que guiaban el comportamiento diario de los funcionarios, buscando comprender los factores que guían su comportamiento, para lograr un diagnóstico efectivo.

Para examinar esta cultura en su contexto cotidiano, se eligió un diseño no experimental. Esto significó que no se alteró ni intervino el entorno de trabajo; por el contrario, se observó la realidad en su estado natural, tal como se presentaba en ese momento. El alcance fue descriptivo, orientado a detallar y caracterizar con la mayor fidelidad posible

la vivencia de la ciberseguridad en FOSIS Atacama, con el objetivo de identificar sus particularidades, debilidades y por tanto oportunidades de mejora.

3.2. Población y muestra

El trasfondo del marco investigativo fueron las personas que trabajan en FOSIS Atacama. Por ello, la población de estudio la componían todos y cada uno de los funcionarios de la dirección regional. Dado que el equipo estaba formado por 30 personas, incluyendo jefaturas, profesionales y administrativos, se incluye como muestra a la totalidad mediante un censo. Escuchar todas las voces era lo mejor para que el diagnóstico fuera preciso y la propuesta de mejora, verdaderamente representativa.

3.3. Técnicas e instrumentos de recolección de datos

Para recolectar la información, se utilizó un enfoque dual, se utilizaron dos técnicas principales:

1. **Revisión documental y contextualización:** Se analizaron documentos clave como la Política Nacional de Ciberseguridad 2023-2028, la Ley Marco de Ciberseguridad, y cualquier política o protocolo interno existente en la institución. Esta técnica permitió establecer el marco de referencia y los estándares con los cuales se compararon las prácticas actuales.

2. **Diseño y aplicación de encuesta:** Esto buscó recolectar datos directamente de la fuente para obtener una "fotografía" de la cultura actual. Se diseñó y aplicó una encuesta censal a todos los funcionarios utilizando Microsoft Forms. El cuestionario midió 4 dimensiones fundamentales: i) Percepción general sobre la ciberseguridad; ii) Prácticas y comportamientos diarios; iii) Identificación de amenazas y respuesta a incidentes; iv) Formación y capacitación.

3.4. Procedimiento del diagnóstico

El objetivo de esta etapa fue comprender en detalle el estado actual de la cultura de ciberseguridad en la institución, identificando fortalezas, debilidades, brechas y percepciones claves. Este proceso se inició con la organización y el procesamiento de toda la información recopilada, para así realizar el análisis de los resultados, buscando patrones, ideas recurrentes y brechas entre el quehacer diario y lo que dictaban las buenas prácticas.

En otras palabras, el diagnóstico se construyó a partir del análisis e interpretación de los datos recolectados, para lo cual, el procedimiento fue el siguiente:

1. **Procesamiento de datos y análisis de resultados:** Se tabuló y organizó las respuestas obtenidas de la encuesta, para de esta forma identificar patrones, tendencias, puntos críticos y las brechas más significativas entre las prácticas reportadas por los funcionarios y los lineamientos establecidos en la Política Nacional de Ciberseguridad.
2. **Síntesis de hallazgos:** Los resultados del análisis se consolidaron en un diagnóstico claro y fundamentado, que sirvió como base directa para la formulación de los ejes estratégicos y las recomendaciones de la propuesta de mejora.

3.5. Procedimiento de la Propuesta de Mejora

Con base en los hallazgos del diagnóstico, esta fase se centra en estructurar una propuesta con acciones concretas. La propuesta se organiza de manera lógica, para esto, se agruparon los problemas identificados en el diagnóstico en áreas de acción. Estas áreas y su finalidad fueron:

i) Liderazgo y gobernanza: Para fortalecer el rol de las jefaturas.
ii) Formación y sensibilización: Para desarrollar conciencia en los funcionarios e idealmente competencias en el área.

iii) Comunicación y protocolos: Para mejorar la claridad y difusión de las normativas y/o acciones.

iv) Gestión y reporte de incidentes: Esto para optimizar los canales para informar y reaccionar ante amenazas, aunque esto puede ser considerado inicialmente de manera opcional, debido a que es un eje de acción mayoritariamente técnico.

El diseño de la propuesta de mejora fue organizado en dos partes, que son:

- **Formulación de recomendaciones y acciones específicas**: Acá, se traduce el diagnóstico en un plan de acción tangible. Para cada área de acción, se elaboró un conjunto de recomendaciones y acciones específicas y realizables. Por ejemplo, para el área de formación y sensibilización: "Implementar un programa de capacitación anual obligatorio" y "Realizar simulacros de phishing trimestrales con fines educativos". El objetivo de este capítulo es tener una propuesta coherente que sirva como una herramienta de apoyo para cualquier funcionario del FOSIS Atacama.

- **Elaboración de un plan de implementación:** Tiene como propósito asegurar que la propuesta sea práctica y factible de implementar. Se propuso una hoja de ruta de cómo se podrían llevar a cabo las acciones propuestas. Este plan incluye: i) Cronograma: plazos sugeridos para cada acción. (ii) Responsables: roles o departamentos encargados de liderar cada iniciativa. iii) Recursos necesarios: estimación de recursos humanos, tecnológicos o de capacitación requeridos.

Con el fin de realizar una transferencia de información fluida y simple de comprender respecto al diagnóstico realizado, así como también, para las recomendaciones/acciones y plan de implementación, se elaboró un reporte ejecutivo para entrega a la jefatura del servicio. (ver Anexo 2).

CAPÍTULO IV

DIAGNÓSTICO

En base a la metodología, la recolección de datos se realizó a partir de dos fuentes de información, las cuales fueron: *i*) Revisión documental y contextualización; *ii*) Diseño y aplicación de instrumento de diagnóstico. La estructura del capítulo siguió la siguiente la secuencia según la metodología: Comenzó con la descripción de la logística y los detalles técnicos del Diseño y aplicación de la encuesta (4.2). Posteriormente, se procede a la etapa de Diagnóstico de la situación actual (4.3), la cual incluye el Procesamiento de datos y el respectivo Análisis de resultados (4.3.1) obtenidos según la encuesta. Finalmente, el capítulo concluye con una Síntesis de hallazgos (4.4), cuyo propósito es consolidar la información analizada para identificar las fortalezas y las principales brechas que definen el estado actual de la cultura de ciberseguridad.

A continuación, se detallan cada una de estas fuentes:

4.1. Revisión Documental y Contextualización

El FOSIS, como organismo de la Administración del Estado, se encuentra directamente sujeto a las disposiciones de la Ley N° 21.663 y los objetivos de la Política Nacional de Ciberseguridad 2023-2028. Este marco normativo establece un mandato ineludible de transformación cultural y operativa en materia de seguridad digital.

Por otra parte, este servicio público no cuenta actualmente con documentación propia, ya sean, políticas, mecanismos o protocolos, por lo cual, el análisis documental se reduce a estos dos grandes marcos normativos.

- **Ley Marco de Ciberseguridad (Ley N° 21.663)**

Como se mencionó en el Capítulo Marco Teórico, La Ley Marco establece la institucionalidad, los principios y la normativa general de ciberseguridad. Su aplicación al FOSIS Atacama se fundamenta en su rol como organismo de la Administración del Estado que provee Servicios Esenciales.

Aplicación como Servicio Esencial: FOSIS, al ser un organismo de la Administración del Estado, es un prestador de servicios esenciales. Aunque la Ley N° 21.663 no lo califica como Operador de Importancia Vital de forma automática (dicha calificación debe ser realizada por la ANCI), al ser parte de la Administración del Estado y manejar datos sensibles de beneficiarios vulnerables, está sujeto a los deberes generales de ciberseguridad.

Deberes Regulatorios Clave (Art. 7° y 9°): Deberes Generales: El FOSIS debe aplicar permanentemente medidas tecnológicas, organizacionales, físicas o informativas para prevenir, reportar y resolver incidentes de ciberseguridad. Esto exige la implementación de protocolos y estándares establecidos por la Agencia Nacional de Ciberseguridad (ANCI). Por ejemplo: Deber de Reportar: El FOSIS tiene la obligación de reportar al CSIRT Nacional los ciberataques e incidentes que puedan tener efectos significativos, con un plazo máximo de tres horas para la alerta temprana y 72 horas para la actualización inicial de la información.

- **Política Nacional de Ciberseguridad (PNC) 2023-2028**

La PNC 2023-2028, impulsada por el Comité Interministerial sobre Ciberseguridad, establece cinco objetivos estratégicos, siendo el más relevante para el FOSIS Atacama el de **Cultura de Ciberseguridad**, ya que:

- Busca desarrollar una cultura en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales.

- La meta es generar nociones y prácticas de ciberhigien**e** en la población (incluidos los funcionarios públicos), para que cada persona sea capaz de proteger su identidad digital y su información.

De esta forma la PNC exige: Generar instancias de capacitación para todos los funcionarios públicos en hábitos y medidas básicas de seguridad digital. El objetivo es que el funcionario proteja la información de ciudadanos que le es confiada y que administra. Además, llama a fomentar una cultura de evaluación y gestión del riesgo en organizaciones públicas.

4.2. Diseño y aplicación de encuesta

A continuación, se muestra la encuesta desarrollada y utilizada para identificar la cultura de ciberseguridad en los funcionarios del FOSIS Atacama. Esta encuesta fue elaborada considerando las siguientes dimensiones: i) Percepción General sobre la Ciberseguridad; ii) Prácticas y Comportamientos Diarios; iii) Identificación de Amenazas y Respuesta a Incidentes; y iv) Formación y Capacitación.

Cabe señalar que esta herramienta se implementó en la herramienta Forms de Microsoft 365, lo que permitió poder capturar la información en cualquier dispositivo ya que no requiere el uso de ningún tipo de cuenta de usuario.

- Título de la encuesta.

Encuesta de Cultura de Ciberseguridad en FOSIS Atacama.

- Texto introductorio.

Estimado/a funcionario/a de FOSIS Atacama:

Junto con saludar, le invito a participar en esta encuesta, la cual se enmarca en el desarrollo de un trabajo de título de la Universidad de Atacama.

El objetivo principal de este instrumento es conocer la cultura de ciberseguridad en nuestra institución. Su participación es fundamental, completamente anónima y la información recopilada será tratada con fines académicos y con absoluta confidencialidad.

Le solicitamos responder con la mayor sinceridad posible, ya que sus percepciones y experiencias son clave para este estudio.

¡Muchas gracias por tu colaboración!

- Cuerpo de encuesta.

Parte 1: Percepción General sobre la Ciberseguridad:

1. La ciberseguridad es una prioridad importante en mi trabajo diario.

	1	2	3	4	5
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)	○	○	○	○	○

2. Conozco y entiendo la Política de Seguridad de la Información de nuestra organización.

	1	2	3	4	5
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)	○	○	○	○	○

3. En tu opinión, ¿quién es el principal responsable de proteger la información en FOSIS?

- ○ El equipo de Informática/TI.
- ○ Cada uno de los funcionarios/as
- ○ Solo las jefaturas y directivos.
- ○ No estoy seguro/a.

Parte 2: Prácticas y Comportamientos Diarios:

4. Utilizo una contraseña única y robusta para cada una de mis cuentas de trabajo.

	1	2	3	4	5
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)	○	○	○	○	○

5. Siempre bloqueo mi equipo cuando me ausento de mi puesto.

	1	2	3	4	5
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)	○	○	○	○	○

6. Comparto información confidencial solo por canales autorizados y seguros.

	1	2	3	4	5
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)	◯	◯	◯	◯	◯

7. Me aseguro de que los dispositivos personales que uso para el trabajo estén actualizados y protegidos.

	1	2	3	4	5
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)	◯	◯	◯	◯	◯

Parte 3: Identificación de Amenazas y Respuesta a Incidentes:

8. ¿Te consideras capaz de identificar un correo electrónico o mensaje falso?

- ◯ Sí, totalmente
- ◯ Creo que sí, en la mayoría de los casos
- ◯ No estoy muy seguro/a
- ◯ No, me resulta difícil

9. Recibes un mensaje de WhatsApp de un número desconocido, pero la persona dice ser tu jefatura (o un colega) y te pide con urgencia que le envíes un dato "sensible" o un código que te llegó por SMS. ¿Qué haces? ¿Cómo reaccionarías?

- ◯ Hago lo que me pide
- ◯ Le respondo para pedir más detalles
- ◯ Intento contactar por otro medio para confirmar
- ◯ No hago nada y lo ignoro

10. Si detectas algo "raro" en tu computador ahora mismo (ej. un mensaje extraño), ¿sabes exactamente a quién y cómo debes reportarlo?

- ◯ Sí, tengo claro el procedimiento y a quién contactar.
- ◯ Tengo una idea, pero no estoy 100% seguro/a.
- ◯ No, no sabría qué hacer o a quién llamar.

Parte 4: Formación y Capacitación:

11. ¿Has recibido alguna charla, capacitación o instructivo claro sobre ciberseguridad en el último año?

- ◯ Si
- ◯ No
- ◯ No recuerdo

12. ¿Con qué frecuencia lees los correos informativos en materia de ciberseguridad del Nivel Central? (tips, posteos, consejos, charlas, etc.).

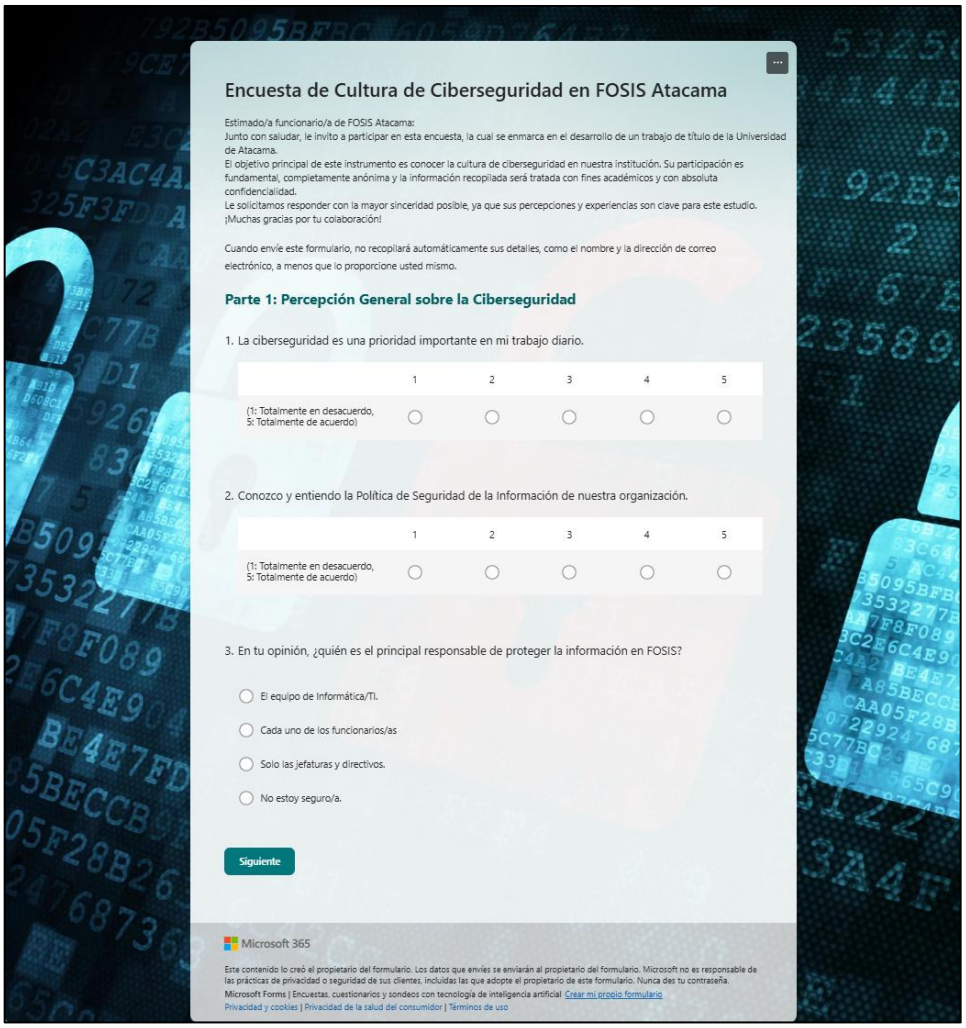
	Siempre	A veces	Casi nunca	Nunca
Seleccione:	◯	◯	◯	◯

13. ¿Considero que mi formación en ciberseguridad se realiza con la frecuencia adecuada?

☆ ☆ ☆ ☆ ☆

14. ¿Qué tipo de ayuda, capacitación o información te gustaría recibir para sentirte más seguro/a al usar las herramientas digitales en tu trabajo? *

Ilustración 10 Cap. 4 Captura de encuesta.



Fuente: cuenta personal Microsoft 365.

4.3. Diagnóstico de la situación actual

A continuación, se muestra el análisis realizado de la situación actual del FOSIS Atacama con relación a la cultura de ciberseguridad. Se debe destacar que esto fue realizado hasta el mes de octubre de 2025, por tanto, cualquier cambio posterior a esta fecha no fue considerado.

La presente sección, está dividida en dos partes, que son:

1) Procesamiento de datos y análisis de resultados: Se entrega un análisis tanto cuantitativo como cualitativo por cada sección. Además, se analiza de manera individual el resultado de las preguntas.

2) Análisis de resultados: Acá se vincula la naturaleza de este servicio público con el Marco regulatorio y conformidad legal, así como las brechas de la cultura de ciberseguridad detectadas en los funcionarios de FOSIS Atacama con relación a las obligaciones legales que como parte del servicio público que se están eventualmente incumpliendo.

4.3.1. Procesamiento de datos y Análisis de resultados

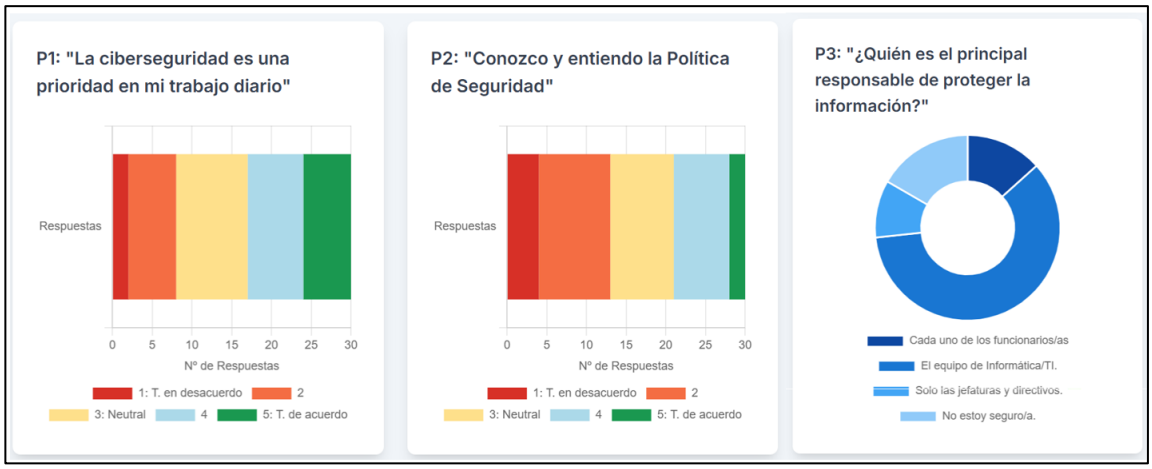
La sección 1 abarca desde la pregunta 1 a la 3.

Los resultados de estas tres preguntas evidencian una cultura organizacional débil en ciberseguridad, caracterizada por:

- Baja percepción de prioridad.
- Escaso conocimiento de políticas institucionales.
- Visión errónea sobre quién es responsable.

Para un servicio público como FOSIS que maneja información sensible de personas en situación de vulnerabilidad, esto representa un riesgo institucional alto.

Análisis por preguntas de la Sección 1:



- **Pregunta 1. "La ciberseguridad es una prioridad importante en mi trabajo diario"**

(Escala 1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)

Análisis Cuantitativo:

- De acuerdo (4-5): 13 de 30 funcionarios (43.3%)
- Neutral (3): 9 de 30 funcionarios (30.0%)
- En desacuerdo (1-2): 8 de 30 funcionarios (26.7%)

Análisis Cualitativo: La percepción de la ciberseguridad como una prioridad laboral está peligrosamente fragmentada. Menos de la mitad del personal (43.3%) la integra activamente en sus tareas, mientras que un 56.7% la considera neutral o irrelevante. Desde una perspectiva de administración, esto indica una cultura de seguridad débil y una falta de alineación estratégica. Si los funcionarios no perciben la seguridad como parte integral de sus responsabilidades, es poco probable que sigan los protocolos, viendo la seguridad como un obstáculo y no como un facilitador. Esto expone a la organización a riesgos operativos significativos derivados de errores humanos.

- **Pregunta 2. "Conozco y entiendo la Política de Seguridad de la Información de nuestra organización"**

(Escala 1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)

Análisis Cuantitativo:

- En desacuerdo (1-2): 14 de 30 funcionarios (46.7%)
- Neutral (3): 7 de 30 funcionarios (23.3%)
- De acuerdo (4-5): 9 de 30 funcionarios (30.0%)

Análisis Cualitativo: Este es un hallazgo crítico. Casi la mitad del personal (46.7%) admite activamente no conocer o no entender la política que rige la seguridad de la información. Una política que no se comunica, no se internaliza y no se comprende es administrativamente inútil. Esto representa una grave brecha de gobernanza. La organización no puede exigir el cumplimiento de normativas que no han sido eficazmente diseminadas. Esta falta de conocimiento anula la capacidad de la administración para hacer cumplir los estándares y expone a FOSIS a riesgos de cumplimiento y operacionales.

- **Pregunta 3. "En tu opinión, ¿quién es el principal responsable de proteger la información en FOSIS?"**

Análisis Cuantitativo:

- El equipo de Informática/TI: 18 de 30 funcionarios (60.0%)
- No estoy seguro/a: 5 de 30 funcionarios (16.7%)
- Cada uno de los funcionarios/as: 4 de 30 funcionarios (13.3%)
- Solo las jefaturas y directivos: 3 de 30 funcionarios (10.0%)

Análisis Cualitativo: Los resultados revelan una cultura de "responsabilidad delegada" en lugar de una "responsabilidad compartida". Una abrumadora mayoría (60%) cree que la seguridad es un problema exclusivo del departamento de TI. Esto es un concepto obsoleto y peligroso que socava el principio del "cortafuegos humano". Solo el 13.3% entiende el concepto moderno de que la seguridad es responsabilidad de todos. Desde la gestión administrativa, esta mentalidad crea un factor limitante: el equipo de TI no puede prevenir brechas si los otros 28 funcionarios no actúan como la primera línea de defensa.

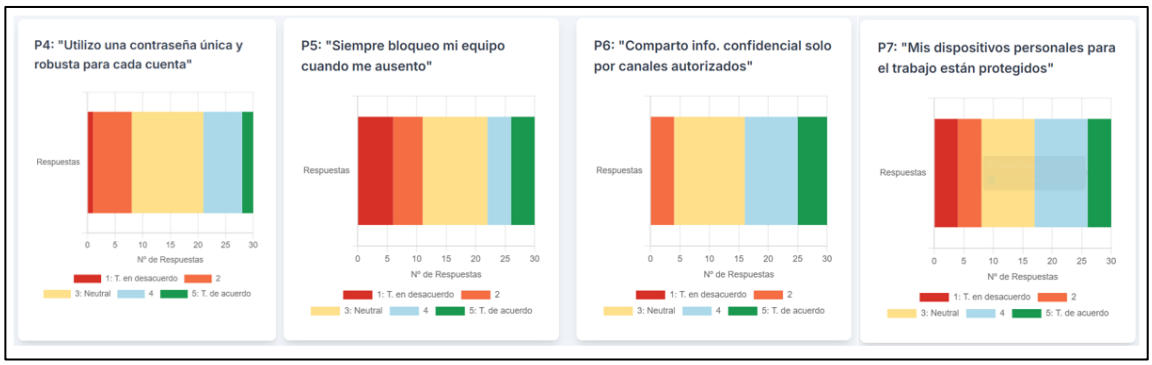
La sección 2 abarca desde la pregunta 4 a la 7.

Los resultados de esta sección indican que existe una brecha crítica entre la percepción de responsabilidad y la adopción de buenas prácticas técnicas básicas. Las conductas de seguridad más elementales, como gestionar contraseñas, bloquear equipos o proteger dispositivos no están suficientemente internalizadas. Esto evidencia una falta de hábitos

operativos seguros, lo que incrementa la exposición a riesgos como accesos no autorizados, robo de credenciales o filtraciones accidentales.

En un entorno donde FOSIS maneja datos sensibles de personas en situación de vulnerabilidad, estas prácticas deficientes contradicen los principios seguridad de la información del estado y exponen a la institución a sanciones legales y pérdida de legitimidad.

Análisis por pregunta de la Sección 2.



- **Pregunta 4. "Utilizo una contraseña única y robusta para cada una de mis cuentas de trabajo"**

(Escala 1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)

Análisis Cuantitativo:

- Neutral (3): 13 de 30 funcionarios (43.3%)
- De acuerdo (4-5): 9 de 30 funcionarios (30.0%)
- En desacuerdo (1-2): 8 de 30 funcionarios (26.7%)

Análisis Cualitativo: La higiene de contraseñas es deficiente. Solo el 30% afirma seguir buenas prácticas. El grupo más grande (43.3%) es "Neutral", lo que en encuestas de seguridad a menudo se interpreta como una admisión pasiva de incumplimiento. Sumado al 26.7% que lo niega, se puede inferir que más del 70% del personal probablemente reutiliza contraseñas o utiliza contraseñas débiles. Esto representa un riesgo técnico elevado de posible riesgo de vulnerabilidad de credenciales. Es un área de bajo costo y alto impacto que la administración puede mejorar mediante controles técnicos (por ejemplo: políticas de contraseña obligatorias) y formación.

- **Pregunta 5. "Siempre bloqueo mi equipo cuando me ausento de mi puesto"**

(Escala 1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)

Análisis Cuantitativo:

- Neutral (3): 12 de 30 funcionarios (40.0%)
- En desacuerdo (1-2): 10 de 30 funcionarios (33.3%)
- De acuerdo (4-5): 8 de 30 funcionarios (26.7%)

Análisis Cualitativo: Las prácticas de seguridad física básicas son extremadamente débiles. Un tercio del personal (33.3%) admite abiertamente que deja sus equipos desbloqueados, y un 40% adicional es neutral (lo que implica un cumplimiento esporádico). Esto significa que, en algún momento, es probable que la mayoría de los equipos estén desbloqueados. Esto expone a la organización a riesgos internos significativos, como el acceso no autorizado a información sensible por parte de visitantes u otros colegas. Es un fallo de procedimiento básico que la administración debe corregir con una política de "escritorio limpio y pantalla bloqueada".

- **Pregunta 6. "Comparto información confidencial solo por canales autorizados y seguros"**

(Escala 1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)

Análisis Cuantitativo:

- De acuerdo (4-5): 14 de 30 funcionarios (46.7%)
- Neutral (3): 12 de 30 funcionarios (40.0%)
- En desacuerdo (1-2): 4 de 30 funcionarios (13.3%)

Análisis Cualitativo: El manejo de datos es ambiguo. Si bien solo el 13.3% admite usar canales inseguros, un preocupante 40% se muestra "Neutral". Esta neutralidad sugiere una falta de claridad sobre qué es un "canal autorizado". Es probable que los funcionarios utilicen herramientas no corporativas (como WhatsApp o correos personales) por conveniencia, sin ser conscientes del riesgo. La administración debe definir, comunicar y reforzar urgentemente cuáles son los canales autorizados para el manejo de información sensible, eliminando esta riesgosa ambigüedad.

- **Pregunta 7. "Me aseguro de que los dispositivos personales que uso para el trabajo estén actualizados y protegidos"**

(Escala 1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)

Análisis Cuantitativo:

- De acuerdo (4-5): 13 de 30 funcionarios (43.3%)
- Neutral (3): 9 de 30 funcionarios (30.0%)
- En desacuerdo (1-2): 8 de 30 funcionarios (26.7%)

Análisis Cualitativo: Un 43.3% afirma gestionar la seguridad de sus dispositivos personales. Sin embargo, un 56.7% combinado es neutral o admite no hacerlo. Esto crea un punto ciego significativo: los dispositivos personales no gestionados que acceden a datos corporativos eluden la mayoría de los controles de seguridad. La jefatura debe establecer una política de clara, que podría incluir soluciones de gestión de dispositivos móviles o, en su defecto, delimitar el acceso a posibles datos sensibles desde equipos personales.

La sección 3 abarca desde la pregunta 8 a la 10.

Los resultados de esta sección indican que el personal carece tanto de capacidad técnica para detectar amenazas comunes (phishing, ingeniería social) como de protocolos claros y accesibles para actuar ante ellas. Esta combinación es especialmente peligrosa en contextos de presión o urgencia, donde los atacantes suelen operar.

La incapacidad para reconocer y reportar incidentes impide una respuesta oportuna, aumentando el impacto potencial de brechas. Además, contradice el principio de “respuesta ante incidentes” exigido por estándares nacionales e internacionales de ciberseguridad.

Análisis por pregunta de la Sección 3.

- **Pregunta 8. "¿Te consideras capaz de identificar un correo electrónico o mensaje falso?"**

Análisis Cuantitativo:

- No estoy muy seguro/a: 24 de 30 funcionarios (80.0%)
- No, me resulta difícil: 3 de 30 funcionarios (10.0%)
- Creo que sí, en la mayoría de los casos: 3 de 30 funcionarios (10.0%)

Análisis Cualitativo: Este es uno de los hallazgos más alarmantes de la encuesta. El 90% del personal (27/30) no confía en su capacidad para detectar un ataque de phishing o ingeniería social, el ataque más común y exitoso. El "cortafuegos humano" de la organización es prácticamente inexistente. Esto sitúa a FOSIS en una posición de vulnerabilidad extrema. Este dato por sí solo justifica una intervención administrativa inmediata y prioritaria en forma de capacitación práctica y simulaciones de phishing.

- **Pregunta 9. "Recibes un mensaje de WhatsApp... [urgente pidiendo un dato sensible]... ¿Qué haces?"**

Análisis Cuantitativo:

- No hago nada y lo ignoro (Correcto): 14 de 30 funcionarios (46.7%)
- Le respondo para pedir más detalles (Incorrecto): 8 de 30 funcionarios (26.7%)
- Intento contactar por otro medio para confirmar (Correcto): 7 de 30 funcionarios (23.3%)
- Hago lo que me pide (Muy Incorrecto): 1 de 30 funcionarios (3.3%)

Análisis Cualitativo: A diferencia de la pregunta anterior (confianza), esta mide la *acción*. Los resultados son mixtos. El 70% (21/30) toma una acción segura (ignorar o verificar por otro medio). Sin embargo, un preocupante 30% (9/30) toma una acción de alto riesgo. "Responder para pedir detalles" (8 personas) es peligroso porque confirma al atacante que el número está activo e inicia un diálogo. El 3.3% (1 persona) que obedece representa una brecha de seguridad inmediata. Esto demuestra que la falta de confianza de la pregunta 8 se traduce en comportamientos de riesgo reales.

- **Pregunta 10. "Si detectas algo 'raro' en tu computador... ¿sabes exactamente a quién y cómo debes reportarlo?"**

Análisis Cuantitativo:

- No, no sabría qué hacer o a quién llamar: 16 de 30 funcionarios (53.3%)
- Tengo una idea, pero no estoy 100% seguro/a: 14 de 30 funcionarios (46.7%)
- Sí, sé exactamente: 0 de 30 funcionarios (0.0%)

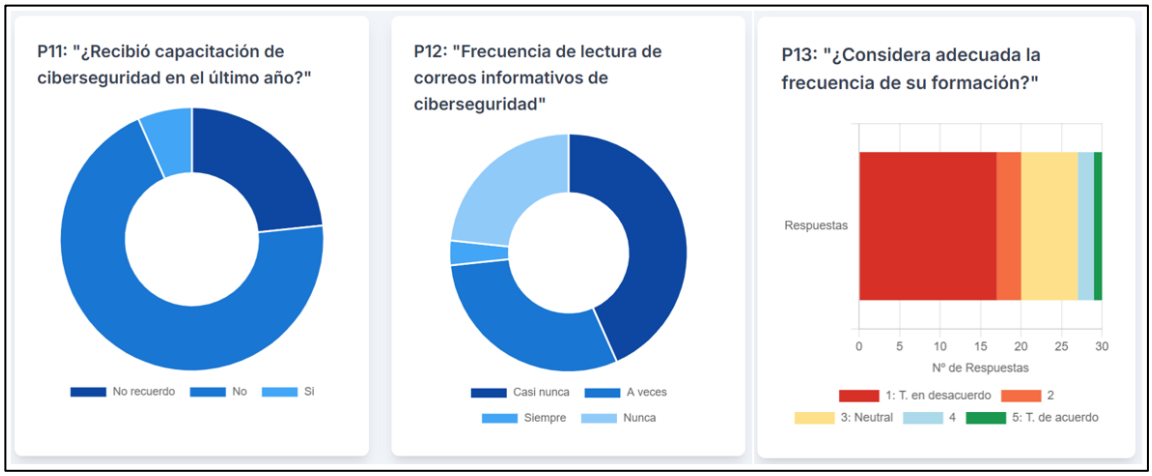
Análisis Cualitativo: Este es un fallo total en la gestión de incidentes. El 100% de los encuestados no sabe con certeza el procedimiento para reportar un incidente de seguridad. Más de la mitad (53.3%) no tiene idea alguna. Desde el punto de vista de la administración de riesgos, esto es catastrófico. Un incidente no reportado (o reportado por el canal incorrecto) no puede ser contenido, permitiendo que una infección menor se convierta en una brecha mayor (ej. ransomware). Es una prioridad administrativa urgente establecer, comunicar y capacitar un Canal Único de Reporte de Incidentes que sea claro y fácil de recordar.

La sección 4 abarca desde la pregunta 11 a la 14.

Los resultados en esta sección señalan que existe una desconexión entre la oferta centralizada de formación y la recepción real en terreno. La capacitación, cuando existe, no es percibida como relevante, ni suficientemente recurrente. Además, los canales de difusión actuales (ej.: correos) tienen baja incidencia.

Sin una estrategia de formación efectiva, contextualizada y continua, cualquier política de ciberseguridad permanecerá como un documento teórico. Esto contradice los esfuerzos del Estado por construir una cultura de ciberseguridad activa y preventiva.

Análisis por pregunta de la Sección 4.



- **Pregunta 11. "¿Has recibido alguna charla, capacitación o instructivo claro sobre ciberseguridad en el último año?"**

Análisis Cuantitativo:

- No: 21 de 30 funcionarios (70.0%)
- No recuerdo: 7 de 30 funcionarios (23.3%)
- Sí: 2 de 30 funcionarios (6.7%)

Análisis Cualitativo: Aquí se identifica la causa raíz de la mayoría de los problemas anteriores. Un 93.3% del personal no ha recibido (70%) o no recuerda (23.3%) ninguna capacitación en el último año. La falta de capacitación del capital humano es la explicación directa de la pobre cultura de seguridad, la falta de confianza ante el phishing y el desconocimiento de políticas y procedimientos. Cualquier plan de mejora administrativa debe comenzar con la implementación de un programa de formación formal y regular.

- **Pregunta 12. "¿Con qué frecuencia lees los correos informativos en materia de ciberseguridad del Nivel Central?"**

Análisis Cuantitativo:

- Casi nunca: 14 de 30 funcionarios (46.7%)
- A veces: 11 de 30 funcionarios (36.7%)
- Nunca: 4 de 30 funcionarios (13.3%)
- Siempre: 1 de 30 funcionarios (3.3%)

Análisis Cualitativo: Los canales de comunicación actuales son ineficaces. El 60% del personal (18/30) "Nunca" o "Casi nunca" lee las comunicaciones sobre ciberseguridad. Esto demuestra que la estrategia actual de enviar correos informativos (boletines, tips) es un esfuerzo fallido. La administración no puede depender de este canal pasivo para diseminar políticas críticas o formación. Se deben buscar métodos más proactivos y atractivos (charlas presenciales, cápsulas de video cortas, alertas en el intranet) para asegurar que el mensaje sea recibido.

- **Pregunta 13. "¿Considero que mi formación en ciberseguridad se realiza con la frecuencia adecuada?"**

(Escala 1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)

Análisis Cuantitativo:

- En desacuerdo (1-2): 20 de 30 funcionarios (66.7%)
- Neutral (3): 7 de 30 funcionarios (23.3%)
- De acuerdo (4-5): 3 de 30 funcionarios (10.0%)

Análisis Cualitativo: Este dato refuerza el hallazgo de la pregunta n°11. Dos tercios del personal (66.7%) sienten activamente que la frecuencia de su formación es inadecuada. Esto es importante porque demuestra que existe una demanda interna de más capacitación. No se trata solo de una brecha identificada por la administración; los propios funcionarios se sienten inseguros y solicitan más herramientas educativas. Esto proporciona un fuerte mandato interno para que la administración asigne recursos a un plan de formación.

- **Pregunta 14. "¿Qué tipo de ayuda, capacitación o información te gustaría recibir...?"**

(Pregunta abierta)

Casi la totalidad de las respuestas solicita capacitaciones prácticas, dinámicas, repetidas en el tiempo y centradas en casos reales: charlas, videos, cursos breves, conversatorios, visitas de expertos. Varias mencionan explícitamente la necesidad de aprender desde lo más básico y vincular la ciberseguridad con el autocuidado personal y profesional.

El personal no rechaza la ciberseguridad; al contrario, demanda formación útil, accesible y adaptada a su realidad laboral. Hay una clara apertura al aprendizaje, pero también una frustración por la falta de acompañamiento concreto.

Esta demanda representa una ventana de oportunidad estratégica: invertir en formación bien diseñada mejora la seguridad, fortalece el sentido de pertenencia, la competencia digital del funcionario y la calidad del servicio al ciudadano.

Análisis Cuantitativo (agrupación temática):

- Solicitud explícita de capacitación/charlas/cursos (genérico): 20 respuestas (ej. "Capacitaciones constantes", "Charlas", "Curso breve", "Más capacitaciones").
- Solicitud de temas específicos (Phishing/Estafas): 3 respuestas (ej. "identificar correos de cuentas falsas", "detección de estafas").
- Solicitud de protocolos/procedimientos: 1 respuesta (ej. "Protocolo de seguridad y qué hacer").

- Solicitud de formación sobre herramientas: 2 respuestas (ej. "Microsoft Defender", "Herramientas a utilizar").
- Nivel de conocimiento muy bajo: 3 respuestas (ej. "Todo desde encender el compu", "mi conocimiento... es nula").

Análisis Cualitativo: Las respuestas abiertas confirman la necesidad de acción. La gran mayoría (al menos 20 de 30) son peticiones directas de más capacitación, con mayor frecuencia. El personal no es resistente al cambio; está pidiendo activamente ser instruido. Las solicitudes van desde lo más básico ("Todo desde encender el compu") hasta la necesidad de controles administrativos claros ("Protocolo de seguridad"). Esto le da a la administración una hoja de ruta clara: el personal es receptivo y demanda formación práctica, frecuente y enfocada en la detección de amenazas y los procedimientos de respuesta.

4.4. Síntesis de hallazgos

A partir de la información obtenida del análisis documental y las respuestas de la encuesta realizada a los funcionarios de FOSIS Atacama se identifica la urgencia de implementar la PNC a nivel local, revelando que el factor humano es el eslabón más débil, lo cual se alinea con el hallazgo del Observatorio Nacional de Ciberseguridad (más del 60% de los incidentes en organismos públicos se originan por errores humanos o prácticas inseguras).

El FOSIS Atacama, como servicio esencial de la Administración del Estado, debe transitar de una cultura de responsabilidad delegada y cumplimiento pasivo a una de responsabilidad compartida y ciberhigiene activa. El diagnóstico valida que la brecha no es tecnológica, sino humana y administrativa, manifestada en la ausencia de capacitación recurrente y protocolos de reporte claros. Los esfuerzos por tanto deben enfocarse en proponer acciones concretas de formación y comunicación que permitan alinear el comportamiento diario de los funcionarios con los objetivos de la Política Nacional de Ciberseguridad.

A continuación, se sintetiza a modo de resumen:

- ✓ Las obligaciones que debería cumplir el FOSIS con relación al marco normativo;
- ✓ La alineación que debe tener en relación con estrategia nacional, y, finalmente
- ✓ Las brechas detectadas en los funcionarios en relación también al marco regulatorio.

- Obligaciones que debería cumplir el FOSIS con relación al marco normativo:

Tabla 1 Cap.4 Marco Normativo ley n°21.663 y ley n°19.628.

Ley N° 21.663 (Ley Marco de Ciberseguridad)	Ley N° 19.628 (Protección de Datos Personales)
Calificación Institucional: el FOSIS, como organismo de la Administración del Estado, constituye un Servicio Esencial (Art. 4°).	Principio de Seguridad: se establece la obligatoriedad de proteger los datos sensibles de los beneficiarios.
Deber de Reporte: se impone la exigencia de notificar incidentes al CSIRT Nacional, con un plazo perentorio de tres horas para la alerta temprana.	Mitigación de Riesgos: el incumplimiento legal conlleva sanciones pecuniarias y la potencial erosión de la confianza pública.
Objetivo Primordial: garantizar la capacidad de prevención, contención y respuesta efectiva ante eventualidades de CS.	Objetivo Primordial: asegurar la integridad y la estricta confidencialidad de la información gestionada.

Fuente: Elaboración propia.

- Alineación estratégica nacional:

Tabla 2 Cap. 4 Alineación estratégica nacional

Objetivo Programático de la PNC	Requisito Estratégico Derivado
Pilar 3: Cultura de Ciberseguridad	Desarrollar Ciberhigiene y fomentar la Responsabilidad Compartida entre la totalidad del personal.
Pilar 2: Protección de los Derechos	Se establece el Mandato de Formación para el personal en competencias básicas de seguridad digital, resguardando la equidad.
Meta Institucional: El propósito fundamental es configurar al funcionario como la primera línea de defensa activa en el ecosistema digital.	

Fuente: elaboración propia

- Brecha de la Cultura de Ciberseguridad en FOSIS Atacama:

Tabla 3 Cap. 4 Brechas de la cultura de ciberseguridad

La Brecha de la Cultura de Ciberseguridad en FOSIS Atacama	Vinculación con el Marco Regulatorio
Responsabilidad delegada (60% culpa a TI)	Contradice el espíritu de la Cultura de Ciberseguridad (PNC), que promueve la responsabilidad compartida. Es un concepto obsoleto y peligroso.
Fallo en gestión de incidentes (100% no sabe el procedimiento)	Incumple el Deber de Reportar (Art. 9° de la Ley N° 21.663), ya que sin saber a quién o cómo reportar, es imposible cumplir con los plazos de 3 horas para la alerta temprana.
Ausencia de capacitación (93.3% no recibió/no recuerda)	Incumple el mandato explícito de la PNC de "Generar instancias de capacitación para todos los funcionarios". Es la causa raíz de la pobre cultura de seguridad.
Vulnerabilidad a Phishing (90% no confía en su capacidad)	Aumenta el riesgo de pérdida o filtración de datos sensibles de beneficiario, lo que contradice el Principio de Seguridad de la Ley N° 19.628 (protección contra el tratamiento no autorizado).
Malas prácticas operativas (70% usa contraseñas débiles/reutilizadas; 73.3% no bloquea equipos)	Vulnera los requisitos mínimos para la prevención, contención, y respuesta a incidentes establecidos como objeto de la Ley N° 21.663, exponiendo la continuidad operativa y la confidencialidad de la información.

Fuente: elaboración propia

CAPÍTULO V

PROPUESTA DE MEJORA PARA EL FORTALECIMIENTO DE LA CULTURA DE CIBERSEGURIDAD EN FOSIS ATACAMA

Basado en el diagnóstico realizado en el anterior capítulo, donde se evidenció fallas críticas en las dimensiones de responsabilidad compartida, gestión de incidentes, y formación y capacitación, esta propuesta de mejora se estructura para alinear a FOSIS Atacama con los mandatos de la Ley N° 21.663 y el objetivo de Cultura de Ciberseguridad de la Política Nacional de Ciberseguridad 2023–2028.

Esta propuesta se centra en transformar el factor humano de una vulnerabilidad crítica en un elemento de defensa más activa en cuanto a los riegos inherentes de acciones maliciosas de ciberseguridad.

5.1. Ejes Estratégicos de Intervención

Esta propuesta se organizó en cuatro ejes que abordan las principales brechas detectadas, buscando así una intervención transversal y sistémica en la cultura organizacional.

Tabla 4 Cap.4 Ejes estratégicos de intervención.

Eje Estratégico	**Brecha Abordada**	**Objetivo Específico (OE) que Respalda**
I. Liderazgo y Gobernanza Activa	Responsabilidad delegada (60% culpa a TI)	OE3: Proponer recomendaciones estratégicas
II. Formación y Sensibilización Continua	Ausencia de Capacitación (93.3% no recibió/no recuerda)	OE3: Proponer recomendaciones estratégicas
III. Comunicación y Protocolos de Respuesta	Fallo en Gestión de Incidentes (100% no sabe el procedimiento)	OE3: Proponer recomendaciones estratégicas

IV. Ciberhigiene Operativa	Malas Prácticas Operativas (contraseñas, bloqueo de equipos)	OE3: Proponer recomendaciones estratégicas

Fuente: elaboración propia

5.2. Formulación de recomendaciones y acciones específicas

Para cada eje estratégico, se establecieron acciones concretas, medibles y orientadas a la realidad de la operación del FOSIS Atacama. A continuación, se listas las acciones en relación con los ejes:

5.2.1. Liderazgo y gobernanza activo

El objetivo es cambiar la percepción de la ciberseguridad como un problema de TI a una responsabilidad compartida.

- Acción 1.1: Compromiso de la jefatura visible y medible
  - Recomendación: Incorporar un objetivo de Gestión de la Ciberseguridad en los lineamientos anuales de la Dirección Regional.
  - Implementación: Crear el rol de acción, que de manera práctica se podría denominar "Campeón de Ciberseguridad" o "Enlace de Seguridad" y que este dentro del equipo directivo o jefaturas. Este rol tiene el propósito que actúe como intermediario con el Nivel Central, la ANCI y los funcionarios. Este rol debe participar activamente en la presentación de charlas, comunicados, boletines, difusiones en la materia, etc.

- Acción 1.2: Auditoría de Cultura (Pre y Post)
  - Recomendación: Establecer la aplicación de la Encuesta de Cultura de Ciberseguridad de este estudio de forma obligatoria y anual.
  - Implementación: Utilizar los resultados como KPI (Key Performance Indicators) de gestión de riesgo, midiendo la progresión en la percepción de prioridad y el cambio en las prácticas post-capacitación.

5.2.2. Formación y sensibilización continua

El foco está en cubrir el 93.3% de la brecha de capacitación y atender la demanda de formación práctica y frecuente.

- Acción 2.1: Programa de ciberhigiene obligatorio y práctico.
  - Recomendación: Implementar un programa de formación obligatoria, continua y contextualizada, que cambie el formato de los correos a, acciones reales como talleres o capsulas simples y dinámicas.
  - Implementación:
  - Formato de Cápsulas: Reemplazar los correos largos por "Cápsulas de 15 Minutos" de formación presencial/virtual (una vez al mes), enfocadas en un solo tema, por ejemplos: "Phishing en WhatsApp", "Gestión de Claves Únicas", "Bloqueo de Equipo", entre otros temas de relevancia.
  - Contenido de Casos Reales: Utilizar ejemplos de incidentes en el sector público chileno (EMCO, Poder Judicial, FOSIS Antofagasta) para aumentar la conciencia del riesgo local.

- Acción 2.2: Simulacros de Phishing Educativos.
  - Recomendación: Introducir simulacros controlados para evaluar la vulnerabilidad del personal ante este ataque tan común.
  - Implementación: Realizar simulacros de phishing trimestrales o semestrales. A diferencia de un castigo, el resultado debe ser anónimo y usado para retroalimentación grupal, derivando a los funcionarios que "cayeron" a una sesión de refuerzo breve, convirtiendo el error en una instancia de aprendizaje activo.

- Acción 2.3: Módulo de Inducción de Ciberseguridad.
  - Recomendación: Asegurar que todo nuevo funcionario reciba una capacitación de ciberseguridad.
  - Implementación: Crear un módulo de bienvenida obligatorio que incluya la firma de la Política de Seguridad de la Información y una guía de primeros pasos de ciberhigiene (contraseñas, bloqueo, reporte).

5.2.3. Comunicación y Protocolos de Respuesta

Se enfoca en resolver el fallo total en la Gestión de Incidentes y el incumplimiento del deber de reportar de la Ley N° 21.663.

- Acción 3.1: Canal único de reporte de incidentes (CURI)
  - Recomendación: Establecer un procedimiento de reporte unificado y de alta visibilidad para garantizar el cumplimiento de las 3 horas para alerta temprana.
  - Implementación:
    - Creación del CURI: Definir un único canal. Esto debe ser un correo electrónico con prioridad alta, tal como, alerta.ciber@fosisatacama.gob.cl o un número de anexo interno conocido.
    - Difusión Masiva: Imprimir una ficha de escritorio o sticker para el monitor que como un mensaje como "¿Incidente digital? Llama al [Anexo CURI] o escribe a [Correo CURI]". Esto pretende asegura que la información en todo momento.

- Acción 3.2: Protocolo de respuesta a ingeniería social.
  - Recomendación: Estandarizar la respuesta ante la suplantación de identidad (como el caso de WhatsApp), donde el 30% del personal tomó una acción de alto riesgo.
  - Implementación: Crear una regla de tres pasos para el personal. Esto debe ser algo como: "Dudar, Colgar/Bloquear, Verificar por Otro Medio". Difundir la política que prohíbe el envío de códigos SMS/Clave Única a cualquier persona, incluso jefaturas, como procedimiento de seguridad obligatorio.

5.2.4. Ciberhigiene Operativa

El objetivo es corregir las malas prácticas que exponen a la institución a un riesgo técnico elevado.

- Acción 4.1: Política de "Escritorio limpio y pantalla bloqueada"
  - Recomendación: Implementar una política formal para abordar la baja práctica de bloqueo de equipos y la exposición a riesgos físicos.

- Implementación: Realizar "rondas de seguridad" aleatorias sin previo aviso. Esto puede ser realizado por el “Campeón de Ciberseguridad” o personal de TI, donde se verifica que los equipos estén bloqueados al ausentarse. Las rondas deben tener un carácter formativo, no punitivo.

- Acción 4.2: Gestión de dispositivos y cuentas
  - Recomendación: Fortalecer el control sobre credenciales y acceso a datos desde dispositivos personales.
  - Implementación:
    - Contraseñas: Aplicar obligatoriamente la regla de "Doble Factor de Autenticación (2FA)" en todas las cuentas críticas, como correo electrónico o el sistema FOSIS, además de fomentar el uso de gestores de contraseñas si la política lo autoriza.
    - BYOD (Bring Your Own Device): Formalizar una política de dispositivo personal clara, que regule o prohíba el acceso a información sensible desde equipos no institucionales.

5.3. Plan de Implementación de la propuesta de mejora

El Plan de Implementación que se muestra en esta sección busca llevar a la práctica de manera realista la propuesta de mejora, proyectándolo para ser ejecutada durante un periodo de un año. Este plan, para mejor implementación se organizó en trimestres, priorizando las acciones de Gobernanza y Comunicación en las fases iniciales para establecer los cimientos del cumplimiento normativo, y luego se enfoca en la Formación Continua y la medición de resultados para asegurar una internalización de una nueva cultura de ciberseguridad en el FOSIS Atacama.

5.3.1. Primer Trimestre (Meses 1-3): Cimientos y Gobernanza

El objetivo es establecer la estructura de liderazgo y los canales de comunicación básicos para el reporte, resolviendo el problema crítico del 100% de desconocimiento del procedimiento de reporte.

- Liderazgo: Designación formal del "Campeón de Ciberseguridad" dentro del personal directivo/jefaturas. Este rol debe tener tiempo asignado para impulsar la propuesta.
- Comunicación/Protocolo: Creación e implementación inmediata del CURI (Canal Único de Reporte de Incidentes). Se debe difundir el correo y anexo en cartelería y stickers en cada puesto de trabajo, indicando el plazo de tres horas para la alerta temprana (Ley N° 21.663).
- Ciberhigiene: Implementación de la política "Escritorio Limpio y Pantalla Bloqueada" mediante una circular interna. Se realiza la primera Ronda de Seguridad (formativa) para sensibilizar sobre la práctica de bloqueo (P5: 73.3% no bloquea o es neutral).
- Formación: Diseño e inicio del Módulo de Inducción de Ciberseguridad para nuevos ingresos.

5.3.2. Segundo Trimestre (Meses 4-6): Intervención Operativa y Formación Práctica

El foco es atacar las malas prácticas y la vulnerabilidad ante la Ingeniería Social (Pregunta n°8: 90% no confía en su capacidad de detección).

- Formación (Cápsulas): Inicio del Programa de Cápsulas de 15 Minutos (Acción 2.1). Temas iniciales:
  - Cápsula 1: "Phishing en el Sector Público" (usando el caso FOSIS Antofagasta).
  - Cápsula 2: "Gestión de Contraseñas y 2FA" (aborda el 70% de contraseñas débiles).
  - Cápsula 3: "El Uso de WhatsApp y la Ingeniería Social" (aborda la Pregunta n°9: 30% de alto riesgo).

- Ciberhigiene: Implementación de Doble Factor de Autenticación (2FA) obligatorio en todas las cuentas críticas de FOSIS, como control técnico a las contraseñas débiles.
- Protocolo: Difusión del Protocolo de Respuesta a Ingeniería Social y el Protocolo CURI mediante talleres prácticos.
- Medición: Aplicación del Primer Simulacro de Phishing (Acción 2.2).

5.3.3. Tercer Trimestre (Meses 7-9): Consolidación y Refuerzo

Se refuerzan las acciones y se incrementa la frecuencia para asegurar la internalización de los hábitos.

- Formación (Cápsulas): Continuidad del programa (3 Cápsulas adicionales). Temas sugeridos: "Uso de Dispositivos Personales", "Protección de datos sensibles de beneficiarios (Ley 19.628)".
- Liderazgo: Sesión de capacitación para las jefaturas sobre su rol como "línea de defensa" y la importancia de la responsabilidad compartida (Pregunta n°3: 60% culpa a TI).
- Ciberhigiene: Realización de la tercera y cuarta Ronda de Seguridad (Acción 4.1). Se comienza a hacer un seguimiento más estricto del cumplimiento.
- Comunicación: Campaña interna para promover el uso exclusivo de los canales autorizados para compartir información confidencial (aborda el 40% neutral de la Pregunta n°6).

5.3.4. Cuarto Trimestre (Meses 10-12): Evaluación y alineación estratégica

El trimestre final se enfoca en medir el impacto de las acciones y planificar el siguiente ciclo de mejora.

- Medición: Aplicación del segundo simulacro de phishing (Acción 2.2) y análisis comparativo de resultados (Tasa de clics y reportes a CURI).

- Gobernanza: Aplicación de la Auditoría de Cultura (Acción 1.2): se utiliza la misma encuesta del diagnóstico para medir el cambio en las percepciones (ej. ¿Subió el porcentaje que considera la ciberseguridad una prioridad?).
- Liderazgo: Presentación de los resultados de la auditoría y los simulacros a la jefatura y dirección. Definición de la Hoja de Ruta de Ciberseguridad para el siguiente año.
- Alineación: Documentación de las lecciones aprendidas y adaptación del Programa de Capacitación para el siguiente ciclo, asegurando que se aborden las vulnerabilidades restantes.

Finalmente, en la siguiente tabla se sintetiza la propuesta de mejora elaborada, donde se muestran las acciones específicas de cada eje, indicando un indicador de referencia (KPI) y el responsable principal.

Tabla 5 Cap.5 Síntesis de la propuesta de mejora

Eje Estratégico	Acción Específica	Indicador de Éxito (KPI)	Responsable Principal
I. Liderazgo	1.1 Compromiso directivo visible.	Nombramiento formal del Campeón de Ciberseguridad.	Dirección regional.
III. Comunicación	3.1 Canal Único de Reporte (CURI).	Canal (correo/anexo) operativo y difundido.	Jefatura.
IV. Ciberhigiene	4.1 Escritorio limpio y pantalla bloqueada.	1ª Ronda de Seguridad realizada y comunicado.	Campeón de Ciberseguridad.
III. Comunicación	3.2 Protocolo Respuesta Ingeniería Social.	Ficha de 3 pasos (Dudar, Colgar, Verificar)	Campeón de Ciberseguridad.
II. Formación	2.3 Módulo de Inducción.	Módulo para nuevos funcionarios.	Recursos Humanos (RR.HH.)

II. Formación	2.1 Programa de cápsulas (Inicio).	3 cápsulas de 15 minutos realizadas.	RR.HH. / Campeón de Ciberseguridad.
IV. Ciberhigiene	4.2 Gestión de dispositivos (2FA).	90% de cuentas críticas con doble factor de autenticación (2FA) activo.	Jefatura.
II. Formación	2.2 Simulacro de Phishing (1ª Versión)	Tasa de "clics" no superior al 20%.	Jefatura/ Campeón de Ciberseguridad.
II. Formación	2.1 Programa de Cápsulas (Continuidad).	6 cápsulas de 15 minutos adicionales realizadas.	RR.HH. / Campeón de Ciberseguridad
IV. Ciberhigiene	4.1 Rondas de Seguridad (Consolidación).	4 rondas de Seguridad realizadas en total.	Campeón de Ciberseguridad.
II. Formación	2.1 Programa de Cápsulas (Continuidad).	3 cápsulas de 15 Minutos adicionales realizadas.	RR.HH. / Campeón de Ciberseguridad.
II. Formación	2.2 Simulacro de Phishing (2ª Versión)	Reducción de la Tasa de Clics en al menos 5%.	Jefatura/ Campeón de Ciberseguridad.
I. Liderazgo	1.2 Auditoría de Cultura (Post).	Aplicación de la Encuesta de Cultura a todos los funcionarios.	Dirección Regional / Campeón de Ciberseguridad.

Fuente: elaboración propia

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

El presente capítulo expone las conclusiones derivadas del diagnóstico sobre la cultura de ciberseguridad en FOSIS Atacama, realizado en el Capítulo IV. A partir de los hallazgos identificados, se formularon recomendaciones estratégicas orientadas a fortalecer dicha cultura en coherencia a los objetivos de la Política Nacional de Ciberseguridad 2023-2028 y las obligaciones que impone la Ley Marco de Ciberseguridad.

Además, este trabajo logró dar cumplimiento a los objetivos específicos planteados, confirmando la problemática central: FOSIS Atacama presenta una cultura de ciberseguridad débil, donde el factor humano se erige como la principal vulnerabilidad, generando una brecha significativa entre las prácticas operativas diarias y las normativas vigentes.

En relación con el objetivo específico n°1:

El diagnóstico realizado mediante la encuesta (Capítulo IV, 4.3.1) arrojó hallazgos críticos que evidencian una cultura reactiva e inmadura:

- Existe una cultura de responsabilidad delegada: Se constató que el 60% de los funcionarios percibe la ciberseguridad como una tarea exclusiva de personal con conocimientos de informática o TI. Esta visión contraviene el principio de responsabilidad compartida, fundamental en la ciberseguridad moderna, y elimina el rol del funcionario como principal encargado de la defensa digital.
- Fallo total en la gestión de incidentes de ciberseguridad. El 100% de los encuestados declaró no saber con certeza el procedimiento exacto o el canal formal para reportar un incidente de seguridad. Este desconocimiento absoluto anula la capacidad de respuesta rápida de la institución.

- Vulnerabilidad extrema ante la Ingeniería Social. Un alarmante 90% del personal (sumando las respuestas "No estoy muy seguro/a" y "No, me resulta difícil") no confía en su capacidad para identificar un correo electrónico o mensaje falso (phishing).

  Este dato es especialmente grave considerando que es el tipo de ataque más común en el sector público.

- Ausencia de formación periódica. El 93.3% del personal (sumando "No" y "No recuerdo") no ha recibido o no percibe haber recibido capacitación formal en ciberseguridad en el último año. Esto, es la principal causa de los puntos anteriores.

- Prácticas de ciberhigiene deficientes. Se identificaron hábitos operativos de alto riesgo, incluyendo un 70% de personal que admite o es neutral sobre el uso de contraseñas débiles/reutilizadas y un 73.3% que no bloquea sus equipos al ausentarse, exponiendo la información a accesos físicos no autorizados.

En relación con el objetivo específico n°2:

Al contrastar los hallazgos del diagnóstico (objetivo específico n°1) con el marco normativo (Capítulo II y IV), se concluye que FOSIS Atacama presenta un incumplimiento a las normas de la materia, y no necesariamente por falta de tecnología, sino por barreras humanas y de procedimiento:

- Incumplimiento del deber de reporte (Ley N° 21.663). El hallazgo de que el 100% del personal desconoce el protocolo de reporte implica que la institución está, en la práctica, incapacitada para cumplir con la obligación legal de emitir una alerta temprana al CSIRT Nacional dentro del plazo máximo de tres horas (Art. 9°).

- Incumplimiento del pilar "Cultura de Ciberseguridad" (PNC 2023-2028). La ausencia de capacitación (93.3%) contraviene directamente el mandato explícito de la Política Nacional de "Generar instancias de capacitación para todos los funcionarios públicos".

- Riesgo de vulneración de datos sensibles (Ley N° 19.628). La alta vulnerabilidad al phishing (90%) y las malas prácticas de contraseñas (70%) elevan drásticamente el riesgo de una filtración de datos de beneficiarios. Esto contraviene el Principio de

Seguridad (Art. 3°) de la ley, que obliga al responsable a garantizar estándares adecuados de protección.

En relación con el objetivo específico n°3:

Se concluye que cualquier propuesta de mejora orientada al fortalecimiento de la cultura de ciberseguridad debe ser práctica, continua y centrada en el ser humano para lograr una implementación efectiva y sostenible en el tiempo. El diagnóstico evidenció que los funcionarios no presentan resistencia frente a las medidas de seguridad, sino que, por el contrario, manifiestan una disposición activa hacia el aprendizaje y la mejora de sus competencias en esta materia. En particular, los resultados de la pregunta N°14 del Capítulo IV reflejan una demanda explícita por instancias de formación, destacando la necesidad de capacitaciones dinámicas, periódicas y basadas en casos reales, que permitan vincular la ciberseguridad con las situaciones cotidianas del quehacer institucional.

6.2. Recomendaciones Estratégicas:

Basado en el diagnóstico, la Propuesta de Mejora se centra en cuatro ejes con acciones prioritarias:

1. Liderazgo y Gobernanza: Nombramiento de un "Campeón de Ciberseguridad" y medición anual de la cultura como KPI.
2. Comunicación y Protocolos: Implementación de un Canal Único de Reporte de Incidentes (CURI) y un protocolo de respuesta a ingeniería social ("Dudar, Colgar/Bloquear, Verificar").
3. Formación Continua: Reemplazo de correos pasivos por "Cápsulas de 15 Minutos" (mensuales) y Simulacros de Phishing Educativos (trimestrales).
4. Ciberhigiene Operativa: Aplicación obligatoria del Doble Factor de Autenticación (2FA) y refuerzo de la política de "Pantalla Bloqueada".

Finalmente, el presente trabajo ha validado que la ciberseguridad en FOSIS Atacama es un desafío eminentemente humano y de gestión, más que tecnológico, ya que la

organización posee una buena probabilidad de mejora, los funcionarios son receptivos y abiertos a una formación coherente a lo que marco normativo exige.

En este contexto, la implementación del plan de ejecución de 12 meses (Capítulo V, sección 5.3) se presenta como la estrategia recomendada para que la Dirección Regional transite desde un escenario de alta vulnerabilidad hacia una cultura de responsabilidad compartida y ciberhigiene activa, en concordancia con su rol como servicio esencial del Estado de Chile.

BIBLIOGRAFIA

- (2023). Obtenido de Subtel.
- (2025). Obtenido de Gobierno de Chile.
- ANCI - "PNSC 2023-2028". (18 de 11 de 2025). https://anci.gob.cl. Obtenido de https://anci.gob.cl/documents/4430/Pol%C3%ADtica_Nacional_de_Ciberseguridad_2023-2028.pdf
- Cano Teruel, Q. (2021). Phishing: definición, tipos y cómo protegerse.
- Carlemany, U. (17 de marzo de 2021). Técnicas de análisis de datos cualitativos. Obtenido de https://www.universitatcarlemany.com/actualidad/blog/tecnicas-de-analisis-de-datos-cualitativos/
- Ciberseguridad, M. d. (2017). Obtenido de https://cms-dgd-prod.s3-us-west-2.amazonaws.com/uploads/pdf/Politica_Nacional_de_Ciberseguridad_2017.pdf?
- Fortinet. Tríada CIA: confidencialidad, integridad y disponibilidad. Ed. por. (2025).
- FOSIS. (2022). Sitio web FOSIS. Obtenido de https://www.fosis.gob.cl/es/sobre-nosotros/
- Gambi, M. O. (2009). Efectividad en la gestión pública chilena. Convergencia.
- Grande, I. (2005).
- Ley 18.575, artículo 25. (18 de 11 de 2025). www.suceso.cl. Obtenido de https://www.suseso.cl/612/w3-propertyvalue-102461.html
- Ministerio de Desarrollo Social y Familia. (18 de 11 de 2025). https://www.desarrollosocialyfamilia.gob.cl/mision. https://www.desarrollosocialyfamilia.gob.cl/mision
- Ministerio de Hacienda. (2025).
- National Institute of Standards and Technology. Information Security . (2023). Obtenido de : https://doi.org/10.6028/NIST.SP.800-30r1.
- RAE. (2022). Real Lengua Española. Obtenido de https://dle.rae.es/algoritmo
- SII. (2025). Guía para educación superior, la administración pública y tu profesión. Obtenido de https://www.sii.cl/destacados/educacion/siieduca/aprende-con-nosotros/docs/91-GA-201405295249.pdf
- Sitio oficial de FOSIS. (2025). Obtenido de FOSIS: https://www.fosis.gob.cl/es/sobre-nosotros/

ANEXOS

- Anexo N°1: Encuesta y resultados.

- Anexo N°2: Reporte ejecutivo de diagnóstico y recomendaciones.

Información general sobre respuestas

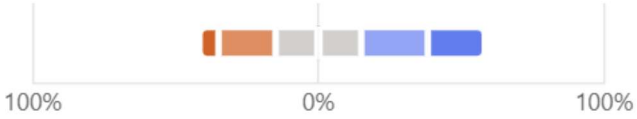
Activo

Respuestas	Tiempo promedio	Duración
30	03:43	35 Días

1. La ciberseguridad es una prioridad importante en mi trabajo diario.

1 2 3 4 5

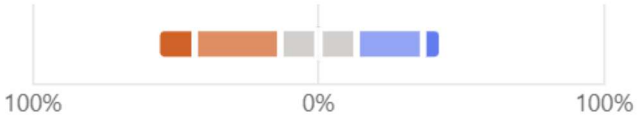
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)



2. Conozco y entiendo la Política de Seguridad de la Información de nuestra organización.

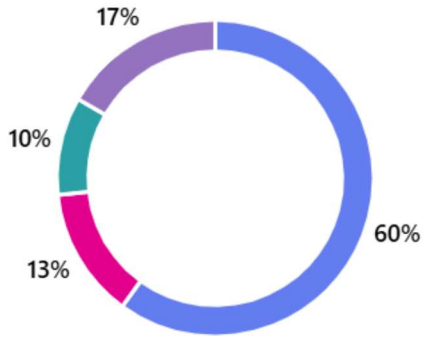
1 2 3 4 5

(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)



3. En tu opinión, ¿quién es el principal responsable de proteger la información en FOSIS?

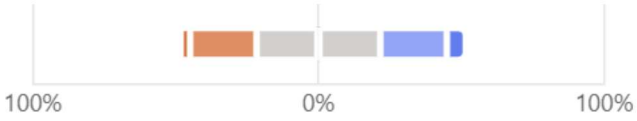
El equipo de Informática/TI.	18
Cada uno de los funcionarios/as	4
Solo las jefaturas y directivos.	3
No estoy seguro/a.	5



4. Utilizo una contraseña única y robusta para cada una de mis cuentas de trabajo.

1 2 3 4 5

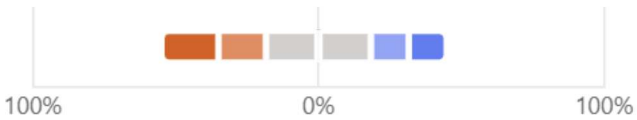
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)



5. Siempre bloqueo mi equipo cuando me ausento de mi puesto.

1 2 3 4 5

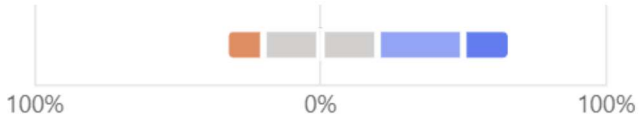
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)



6. Comparto información confidencial solo por canales autorizados y seguros.

1 2 3 4 5

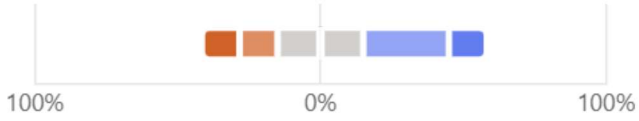
(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)



7. Me aseguro de que los dispositivos personales que uso para el trabajo estén actualizados y protegid os.

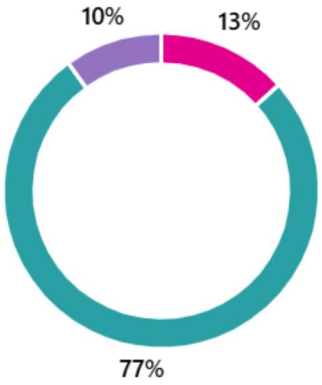
1 2 3 4 5

(1: Totalmente en desacuerdo, 5: Totalmente de acuerdo)



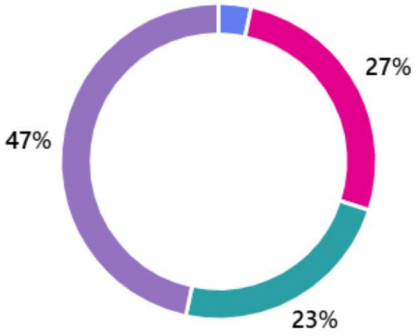
8. ¿Te consideras capaz de identificar un correo electrónico o mensaje falso?

Sí, totalmente	0
Creo que sí, en la mayoría de los casos	4
No estoy muy seguro/a	23
No, me resulta difícil	3



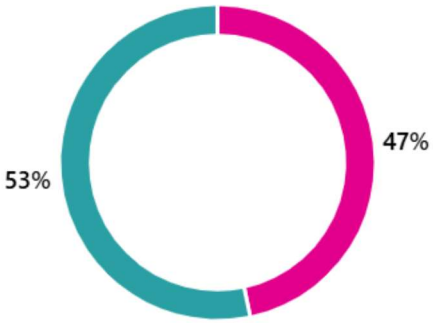
9. Recibes un mensaje de WhatsApp de un número desconocido, pero la persona dice ser tu jefatura (o un colega) y te pide con urgencia que le envíes un dato "sensible" o un código que te llegó por SMS. ¿Qué haces? ¿Cómo reaccionarías?

Hago lo que me pide	1
Le respondo para pedir más detalles	8
Intento contactar por otro medio para confirmar	7
No hago nada y lo ignoro	14



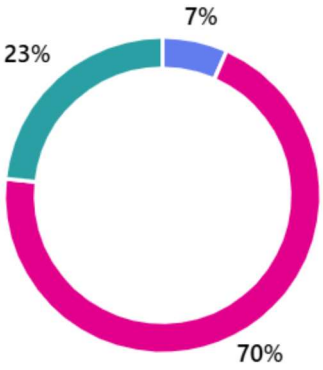
10. Si detectas algo "raro" en tu computador ahora mismo (ej. un mensaje extraño), ¿sabes exactamente a quién y cómo debes reportarlo?

Sí, tengo claro el procedimiento y a quién contactar.	0
Tengo una idea, pero no estoy 100% seguro/a.	14
No, no sabría qué hacer o a quién llamar.	16



11. ¿Has recibido alguna charla, capacitación o instructivo claro sobre ciberseguridad en el último año?

Si	2
No	21
No recuerdo	7



12. ¿Con qué frecuencia lees los correos informativos en materia de ciberseguridad del Nivel Central? (tips, posteos, consejos, charlas, etc)

13. ¿Considero que mi formación en ciberseguridad se realiza con la frecuencia adecuada?

14. ¿Qué tipo de ayuda, capacitación o información te gustaría recibir para sentirte más seguro/a al usar las herramientas digitales en tu trabajo?

30
Respuestas

Respuestas más recientes

"Más capacitaciones para entender porque es importante y c..."

"En todo el tema de la ciberseguridad mi conocimiento y for... "

"No sabría que responder, no se casi nada el tema."

• • •

UNIVERSIDAD DE ATACAMA

Ciberseguridad

en el FOSIS Atacama

FOSIS
Ministerio de Desarrollo Social y Familia
Gobierno de Chile

Basado en trabajo de titulación:

PROPUESTA DE MEJORA PARA EL FORTALECIMIENTO DE LA CULTURA DE CIBERSEGURIDAD EN FOSIS ATACAMA, EN EL MARCO DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023–2028.

Valeria Galleguillos Cerezo

Reporte de diagnóstico y recomendaciones

La ciberseguridad en FOSIS Atacama **no es hoy un problema tecnológico, sino un desafío humano**.

El diagnóstico realizado a la totalidad de los(as) funcionarios revela que, aunque manejan datos sensibles respecto a un grupo de personas de la población vulnerable, la realidad nos indicó que la principal línea de la defensa digital, es decir, los funcionarios(as) está desinformado y expuesto.

Este reporte presenta:

Brecha actual

frente a la Ley Marco de Ciberseguridad (N° 21.663)

para evitar sanciones, proteger la información y cumplir con la Política Nacional de ciberseguridad

Propuesta de plan de mejora

Elaborado para 12 meses

#1

Diagnóstico de la Situación Actual

¿Estamos preparados para un ataque hoy?

Los datos indican que NO.

100% Vulnerabilidad de Respuesta

Ningún funcionario(a) sabe con certeza el procedimiento exacto o a quién recurrir ante un incidente.

93% Sin Capacitación

La gran mayoría no ha recibido (o no recuerda) formación en el último año.

90% Inseguridad ante Phishing

Casi la totalidad del personal no confía en su capacidad para detectar un correo falso o estafa.

60% Responsabilidad Delegada

La mayoría cree erróneamente que la seguridad digital es de responsabilidad exclusiva de TI.

#2

La Brecha Normativa
(Riesgo Legal)

FOSIS Atacama, como Servicio Esencial del Estado, está incumpliendo mandatos críticos.

Obligación legal	Estado actual
Deber de Reporte (Ley 21.663): Informar al CSIRT en máx. 3 horas.	**CRÍTICO:** Sin protocolo conocido, el reporte oportuno es imposible.
Principio de Seguridad (Ley 19.628): Proteger datos sensibles.	**ALTO RIESGO**: El 70% usa contraseñas débiles y 73% no bloquea equipos.
Cultura de Ciberseguridad (PNC): Capacitación obligatoria.	**INCUMPLIDO**: Estrategia de correos informativos no funciona (el 60% casi nunca los lee).

#3

Estrategia de 4 Ejes

La Solución:

Eje I: Liderazgo y Gobernanza

Acción

Designar un "**Campeón de Ciberseguridad**" dentro de la jefatura/equipo directivo.

Herramienta

Hacer visible el compromiso y medir la cultura anualmente con indicadores de gestión.

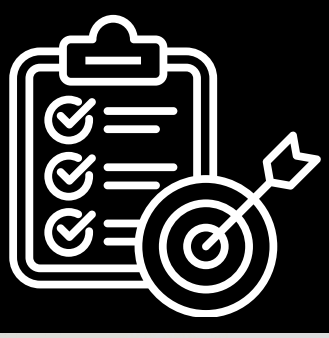
PROPUESTA DE MEJORA PARA EL FORTALECIMIENTO DE LA CULTURA DE CIBERSEGURIDAD EN FOSIS ATACAMA, EN EL MARCO DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023–2028.

#4

Estrategia de 4 Ejes

La Solución:

EJE II: Comunicación (Canal CURI)



Herramienta

Acción

Crear el Canal Único de Reporte de Incidentes (CURI).

Sticker o tarjeta en cada escritorio: "¿Incidente digital? Llama al anexo X o escribe a alerta@..." para asegurar la reacción rápida.

#4

Estrategia de 4 Ejes

La Solución:

EJE III: Formación "Cápsulas"

(No más correos largos)

Acción

Implementar "Cápsulas de 15 Minutos"

Talleres cortos, mensuales y prácticos sobre casos reales (ej. "Estafas en WhatsApp")

Entrenamiento

Simulacros de Phishing trimestrales

(sin castigo, solo aprendizaje).

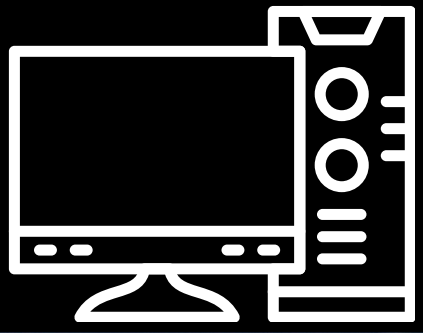
PROPUESTA DE MEJORA PARA EL FORTALECIMIENTO DE LA CULTURA DE CIBERSEGURIDAD EN FOSIS ATACAMA, EN EL MARCO DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023–2028.

#4

Estrategia de 4 Ejes

La Solución:

EJE IV: Ciberhigiene Operativa



Acción

Política de "Escritorio Limpio y Pantalla Bloqueada" con rondas de revisión formativas.

Tecnología

Exigir Doble Factor de Autenticación (2FA) en cuentas críticas.

PROPUESTA DE MEJORA PARA EL FORTALECIMIENTO DE LA CULTURA DE CIBERSEGURIDAD EN FOSIS ATACAMA, EN EL MARCO DE LA POLÍTICA NACIONAL DE CIBERSEGURIDAD 2023–2028.

#5

Hoja de Ruta:

Plan de 12 Meses

1° trimestre

Designar al "Campeón", lanzar el Canal CURI y realizar la primera ronda de escritorio limpio.

2° trimestre

Iniciar las "Cápsulas de 15 minutos" y ejecutar el 1° Simulacro de Phishing.

3° trimestre

Implementar 2FA obligatorio y reforzar protocolos de Ingeniería Social.

4° trimestre

Auditoría final de cultura y medición de mejora (Simulacro 2).

Conclusión

El personal de FOSIS Atacama no es resistente al cambio.

La encuesta revela que ellos piden capacitación práctica.

La ciberseguridad es una responsabilidad compartida, no un problema de TI

Solicitud al servicio

Aprobar la creación del rol "Campeón de Ciberseguridad".

Autorizar el inicio del cronograma de trabajo lo más próximo posible.