UNIVERSIDAD DE LA REPÚBLICA
FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN

**TRABAJO FINAL PARA OBTENER EL TÍTULO DE
MAGÍSTER EN SISTEMAS DE INFORMACIÓN DE LAS ORGANIZACIONES**

Título

Evaluación de estándares de ciberseguridad en empresas del sistema de salud privado uruguayo

por

Claudio Muzi
Jesús Fabricio Rambao

TUTOR: Jorge Luis González
COORDINADOR: Gabriel Budiño

Montevideo
URUGUAY
Noviembre 2024

Resumen

El objetivo de este trabajo es evaluar estándares de ciberseguridad en empresas del sistema de salud privado uruguayo. Para ello se realiza una evaluación inicial del sector, haciendo foco en identificar la importancia que estas empresas le asignan a la ciberseguridad para el cuidado de sus datos, y la continuidad de sus servicios. Para alcanzar este objetivo se aplica una metodología de estudio de caso, con investigación de tipo exploratoria y descriptiva. Se usa un enfoque mixto, se trabaja con datos cuantitativos y cualitativos. Los instrumentos de recolección de información consideraron variables que analizan las medidas de ciberseguridad adoptadas en esta industria, la percepción del riesgo, el conocimiento en la materia y los desafíos que se presentan para la implementación de un modelo de ciberseguridad.

La propuesta de trabajo se sustentó en la percepción de que estas empresas no implementan estándares suficientes para el cuidado de los datos clínicos, ni para asegurar la continuidad de sus operaciones ante un ciberataque.

En un contexto donde la protección de datos sensibles es crucial y existe una creciente amenaza de ciberataques, este estudio busca concientizar y establecer criterios de ciberseguridad que aseguren minimizar los riesgos de filtración de información, así como brindar continuidad operativa de los servicios médicos a sus usuarios.

En la ejecución se ha recolectado información de las empresas del sector estudiado y la mirada de expertos de diversas empresas de Uruguay, arrojando como resultado un marcado déficit en materia de ciberseguridad, con tendencia de la población de muestra en no alcanzar un nivel 2 en marcos de ciberseguridad reconocidos internacionalmente, donde la gestión de riesgos y la concientización es relativamente bajo.

En las conclusiones se obtiene un claro panorama de la realidad de Uruguay y el sector analizado, y permite realizar una serie de recomendaciones que aportan herramientas para mejorar la ciberseguridad en el sector analizado, a partir de estándares reconocidos a nivel internacional.

El trabajo pretende ser un aporte de valor para las empresas del sector, ya que no existen actualmente análisis recientes, criterios o estándares locales para guiar la implementación de políticas de ciberseguridad al contexto actual.

Abstract

The objective of this work is to evaluate cybersecurity standards in companies in the Uruguayan private health system. To do this, an initial evaluation of the sector is carried out, focusing on identifying the importance that these companies assign to cybersecurity for the care of their data, and the continuity of their services. To achieve this objective, a case study methodology is applied, with exploratory and descriptive research. A mixed approach is used, working with quantitative and qualitative data. The information collection instruments considered variables that analyze the cybersecurity measures adopted in this industry, risk perception, knowledge on the subject and the challenges that arise for the implementation of a cybersecurity model.

The work proposal was based on the perception that these companies do not implement sufficient standards for the care of clinical data, nor to ensure the continuity of their operations in the face of a cyber attack.

In a context where the protection of sensitive data is crucial and There is a growing threat of cyberattacks, this study seeks to raise awareness and establish cybersecurity criteria

that ensure minimizing the risks of information leakage, as well as providing operational continuity of medical services to its users.

In the execution, information has been collected from the companies in the studied sector and the views of experts from various companies in Uruguay, resulting in a marked deficit in cybersecurity, with a tendency for the sample population to not reach level 2 in frameworks. of internationally recognized cybersecurity, where risk management and awareness is relatively low.

The conclusions provide a clear overview of the reality of Uruguay and the sector analyzed, and allow for a series of recommendations to be made that provide tools to improve cybersecurity. in the sector analyzed, based on internationally recognized standards.

The work aims to be a valuable contribution to companies in the sector, since there are currently no recent analyses, criteria or local standards to guide the implementation of cybersecurity policies in the current context.

Palabras claves

ransomware – phishing – ciberseguridad – marco- ciberataque- SGSI – cloud computing – riesgo – incidente – disponibilidad – integridad – confidencialidad - prestador- nivel

Abreviaturas

A

Ad-hoc: Solución a medida.

AGESIC: Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.

B

BCP: por sus siglas en inglés Business Continuity Plan - Plan de continuidad de negocio.

BID: Banco Interamericano de Desarrollo.

C

CISO: por sus siglas en inglés Chief Information Security Officer - Director de seguridad de la información.

D

DLP: por sus siglas en inglés Data Loss Prevention - Prevención de pérdida de datos.

DRP: por sus siglas en ingles Disaster Recovery Plan - Plan de recuperación ante desastres.

E

EDR: por sus siglas en inglés Endpoint Detection and Response - Detección y respuesta de endpoints.

G

GDPR: por sus siglas en inglés General Data Protection Regulation - Reglamento general de protección de datos.

H

HCEN: Historia clínica electrónica nacional.

I

IAM: por sus siglas en inglés Identity and Access Management - Identificación y control de acceso.

IEC: por sus siglas en inglés International Electrotechnical Commission - Comisión electrotécnica internacional.

ISACA: Asociación de Auditoría y Control de Sistemas de Información.

IDS: por sus siglas en inglés Intrusion Detection System - Sistema de detección de intrusiones.

IPS: por sus siglas en inglés Intrusion Prevention System Sistema de prevención de intrusiones.

ISO: por sus siglas en inglés International Organization for Standardization - Organización internacional de normalización.

M

MFA: por sus siglas en inglés Multi Factor Authentication - Autenticación de múltiples factores.

N

NIST CSF: por sus siglas en inglés National Institute of Standards and Technology Cybersecurity Framework - Instituto Nacional de Estándares y Tecnología Marco de ciberseguridad.

O

OEA: Organización de los Estados Americanos.

On Premise: Entorno propio o en sitio.

P

PbD: Privacidad por Diseño.

Prestador: Entidad que brinda servicios de atención médica.

PSI: Política de seguridad de la información.

R

RBAC: por sus siglas en inglés Role-Based Access Control - Control de acceso basado en roles.

S

SGSI: Sistema de gestión de seguridad de la información.

SIEM: por sus siglas en inglés Security Information and Event Management - Información de seguridad y gestión de eventos.

SOC: por sus siglas en inglés Security Operations Center - Centro de operaciones de seguridad.

T

TI: Tecnologías de la información.

U

URCD: Unidad Reguladora y de Control de Datos Personales.

Índice general

Tabla de contenido

1. Introducción 1
2. Diseño del estudio 3
2.1 Situación problemática 3
2.2 Marco referencial para el abordaje conceptual 4
2.2.1 Estándares y marcos 4
2.2.2 Normativas y legislaciones en Uruguay 10
2.3 Definición de los objetos de estudio 13
2.4 Objetivos 19
2.4.1 Objetivo General 19
2.4.2 Objetivos Específicos 19
2.5 Hipótesis 20
2.6 Metodología 20
3. Contexto 20
3.1 Consulta con expertos 21
3.2 Análisis de informes 23
4. Protocolo de investigación 25
4.1 Fase de preparación 25
4.2 Fase de recolección de datos cuantitativos 26
4.3 Fase de recolección de datos cualitativos 26
4.4 Fase de revisión de documentos 27
4.5 Fase de análisis de datos 27
4.6 Fase de informe y presentación 27
5. Recolección de datos 28
5.1 Definición de instrumentos 28
5.2 Cuestionario de autoevaluación 29
5.3 Recopilación 43
5.4 Población de la muestra 43
5.4.1 Población prestadores privados de Uruguay 44
5.4.2 Consultores y auditores expertos 44
6. Análisis de información 45
6.1 Análisis de datos cuantitativos 45
6.2 Análisis de datos cualitativos 52

7. Conclusiones 59
7.1 Resultados y aportes 60
7.2 Recomendaciones 61
7.2.1 Inversión en formación y capacitación 61
7.2.2 Fomento de la inversión proactiva 61
7.2.3 Adopción de marcos internacionales 62
7.2.4 Fortalecimiento del marco normativo 62
7.2.5 Insumo de autoevaluación 62
7.3 Limitaciones del estudio de caso 63
8. Bibliografía 63
9. Anexos 66
9.1 Figuras 66
9.1.1 Reporte de ciberseguridad 2020 – OEA y BID 66
9.1.2 ISO/IEC 27001:2022 68
9.1.3 ISO/IEC 27001:2022 fases SGSI 68
9.1.4 NIST CSF ciclo 69
9.1.5 Marco de Ciberseguridad Agesic 69
9.2 Información recolectada 71

1. Introducción

Uruguay durante la última década ha tenido un crecimiento exponencial a nivel tecnológico. Además, se impulsaron políticas de gobierno con metas de digitalización total de los servicios, y la adopción de la historia clínica electrónica nacional HCEN[1]. Ante este contexto, surge la necesidad de definir políticas y procedimientos para proteger la integridad y confidencialidad de la información frente a amenazas cibernéticas cada vez más sofisticadas, ya que el impulso de las políticas que promueven la digitalización amplía el vector de ataque en las organizaciones.

Por otra parte, todos los equipamientos médicos modernos están cada vez más interconectados y, por lo tanto, es necesario tomar medidas para su seguridad y continuidad ante posibles amenazas cibernéticas.

A nivel local, la falta de regulaciones específicas en ciberseguridad[2] para las empresas de salud en Uruguay podría exponerlas a riesgos significativos, por lo cual resulta relevante establecer criterios y estándares de seguridad que minimicen los riesgos asociados a amenazas cibernéticas.

A su vez, la elección del tema "Evaluación de estándares de ciberseguridad en empresas del sistema de salud privado uruguayo" surge de una combinación de intereses personales de los autores de la tesis, y la creciente necesidad de mejorar la seguridad informática en el sector salud, teniendo en cuenta que esta industria es considerada como uno de los sectores sujetos a

[1] La Historia Clínica Electrónica Nacional (HCEN) es una plataforma que permite acceder a la Historia Clínica Digital de los usuarios del sistema de salud y que posibilita el registro de cualquier evento médico independientemente del lugar geográfico y prestador de salud en donde se dé la asistencia. Permite el intercambio de información clínica con fines asistenciales entre prestadores de salud, con el fin de asegurar la continuidad asistencial del usuario en el Sistema Nacional Integrado de Salud (Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento).

[2] Según define IBM la ciberseguridad se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciberamenazas (IBM, 2024).

mayor riesgo a nivel mundial, luego de la financiera, debido a la sensibilidad de los datos manejados.

Este trabajo contribuye a concienciar un problema asociado con los cambios mencionados, entre otros, mediante el estudio de la situación actual del sector en cuanto a ciberseguridad. A la vez, espera aportar herramientas tanto para la autoevaluación en relación a los riesgos asociados a la ciberseguridad, así como ser la base para desarrollar estándares sobre ciberseguridad en el sector salud adaptados al contexto local.

Los resultados de los estudios que se presentan en este trabajo se consideran pueden ser de utilidad y base para futuras investigaciones, y las conclusiones o recomendaciones del mismo, se espera serán un aporte para quienes les interese implementar y mejorar las políticas de seguridad en el sector salud, así como a nivel de supervisión o contralor por parte de autoridades gubernamentales que consideren apropiado fijar estándares mínimos para la industria.

Además, la relevancia de este trabajo se amplifica en el contexto actual, donde los ciberataques son cada vez más sofisticados y frecuentes. Al abordar esta problemática de manera integral y contextualizada, se espera que los hallazgos de la investigación beneficien a las empresas de salud y contribuyan a la sociedad uruguaya, al garantizar una mejor protección de la información relacionada con la historia clínica y la continuidad de los servicios de salud.

En resumen, el análisis planteado responde, no solo, a necesidades, sino que también aborda una problemática de alta relevancia para el sector bajo análisis en el campo de la seguridad de la información y en cierta medida a la sociedad en general, proponiendo ofrecer un aporte significativo tanto a nivel académico, como práctico.

2. Diseño del estudio

2.1 Situación problemática

En el contexto del sistema de salud privado en Uruguay, la creciente digitalización y el uso intensivo de tecnologías de la información han expuesto a estas empresas a un panorama de amenazas cibernéticas cada vez más complejo. Los datos clínicos, que contienen información altamente sensible y personal de los pacientes, se han convertido en un objetivo atractivo para los cibercriminales. Los incidentes de seguridad, como el robo de datos, los ataques de *ransomware*[3] y las violaciones de privacidad, no solo comprometen la confidencialidad, integridad y disponibilidad de la información, sino que también pueden tener consecuencias graves para la salud y el bienestar de los pacientes, ya que con base en los mismos se toman decisiones de tratamientos y procedimientos.

A pesar del aumento de conciencia sobre la importancia de la ciberseguridad, muchas empresas del sector enfrentan desafíos significativos para implementar medidas de protección efectivas. Estos desafíos incluyen la falta de recursos financieros y humanos especializados, la complejidad y constante actualización de los sistemas, y una resistencia cultural al cambio. Además, la necesidad de cumplir con regulaciones nacionales como la Ley de Protección de Datos Personales se añade una capa adicional de complejidad a la gestión de la seguridad de la información.

La eventual falta de prácticas de ciberseguridad robustas podría exponer a las empresas a riesgos operativos y reputacionales, y que también podría tener ciertas implicaciones legales y éticas. Adicionalmente, la protección insuficiente de los datos clínicos y continuidad del negocio podría resultar en la pérdida de confianza por parte de los pacientes.

[3] Según describe IBM, ransomware es un tipo de malware que retiene como rehenes los datos confidenciales o el dispositivo de una víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos que la víctima pague un rescate al atacante (IBM, 2024).

En este contexto, es crucial entender las percepciones y niveles de concientización sobre ciberseguridad dentro de estas empresas, identificar los desafíos y barreras específicas que enfrentan, y explorar estrategias futuras para mejorar y fortalecer sus prácticas de seguridad. Esta investigación pretende abordar estas áreas críticas, proporcionando una visión integral de la situación actual y brindando recomendaciones prácticas para avanzar hacia una mejor protección de los datos sensibles en el sector de salud privado en Uruguay y asegurar la continuidad de las prestaciones de los servicios relacionados.

2.2 Marco referencial para el abordaje conceptual

En el estudio de caso se han analizado los principales marcos y estándares internacionales que rigen las mejores prácticas de ciberseguridad, y se finaliza con un abordaje a marcos, normativas y buenas prácticas creadas en Uruguay.

En el comienzo se analizaron estándares internacionales utilizados en diferentes industrias, es por ello, que el punto de partida ha sido la ISO/IEC 27001, donde a continuación se describe su definición, características y relación para este trabajo.

2.2.1 Estándares y marcos

Estándar ISO/IEC 27001:2022

Norma internacional para la gestión de la seguridad de la información, publicada por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, proporciona un enfoque sistemático para gestionar información sensible de la empresa, asegurando que se mantenga segura. El estándar cubre no solo la tecnología, sino también otros aspectos cruciales como los procesos y personas involucradas en la gestión de la información (Commission International Organization for Standardization International Electrotechnical, 2022).

Importancia para el estudio de caso: este estándar establece requisitos que permiten a las organizaciones evaluar sus riesgos de seguridad de la información y aplicar los controles necesarios para mitigarlos. En el contexto de las empresas privadas de salud en Uruguay, implementar ISO/IEC 27001 es fundamental para proteger la información clínica sensible de los pacientes.

Uso: este estándar se usa internacionalmente y se lo reconoce como base sólida para desarrollar políticas de seguridad de la información a través de la implantación de un sistema de gestión de seguridad de la información. Apegarse a ISO/IEC 27001 puede ayudar a las empresas a cumplir con requisitos legales y contractuales, mejorar su seguridad y ganar la confianza de sus clientes y socios. El enfoque holístico de implementar un sistema de gestión de seguridad de la información es vital para cubrir lo mínimo requerido en la mencionada disciplina desde lo estratégico hacia lo operativo (ver anexo pirámide ISO 27001).

NIST Cybersecurity Framework

Creado por el Instituto Nacional de Estándares y Tecnología, es una agencia del Departamento de Comercio de los Estados Unidos que desarrolla estándares, directrices y buenas prácticas en ciberseguridad. El marco de ciberseguridad del NIST CSF es ampliamente reconocido y utilizado por organizaciones de todo el mundo para gestionar y reducir los riesgos relacionados con la ciberseguridad (National Institute of Standards and Technology, 2024).

Importancia para el estudio de caso: este marco proporciona un lenguaje común y una estructura organizativa para comprender, revelar y gestionar el riesgo cibernético dentro de las organizaciones. Incluye cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar, que abarcan todos los aspectos de la ciberseguridad y brindan la posibilidad de un enfoque holístico e iterativo que permite la mejora continua. A su vez, en la última versión de

NIST CSF 2.0 se suma la función de gobierno que es transversal a las anteriores mencionadas, y determina la ejecución de las otras funciones.

Uso: en el contexto de las empresas del sistema de salud privado en Uruguay, adoptar el marco puede ayudar a establecer un enfoque estructurado para mejorar la resiliencia cibernética, identificar y responder a amenazas y vulnerabilidades, y proteger los datos sensibles de los pacientes. En particular se ha centrado en las directrices desarrolladas para proporcionar un enfoque estructurado para gestionar y reducir los riesgos de ciberseguridad en organizaciones de cualquier tamaño y sector (ver anexo Ciclo NIST CSF).

Una las características más importantes es la gestión de riesgos donde se plantea una serie de pasos que al ser iterados brinda un ciclo de mejora continua.

Estas fases secuenciales del modelo en el estudio de caso tienen mucha relevancia ya que también son adoptadas por el Marco de Ciberseguridad de Agesic, que también se ha contemplado para el soporte teórico.

Reglamento General de Protección de Datos

La prioridad para el estudio de caso es tener una cobertura global, por lo que se decide analizar el Reglamento General de Protección de Datos GDPR que tiene cobertura y aplicación en Unión Europea[4]. Se desglosa a continuación los detalles y características consideradas importantes para el trabajo de estudio de caso.

El Reglamento General de Protección de Datos es una legislación de la Unión Europea que establece directrices estrictas sobre la recopilación, almacenamiento, procesamiento y protección de datos personales. Aunque se aplica principalmente a las empresas que operan

[4] La Unión Europea también conocida como UE es una asociación económica y política formada por 27 países de Europa que han delegado parte de su soberanía en instituciones comunes para tomar democráticamente decisiones sobre asuntos de interés común (Comunidad de Madrid).

dentro de la Unión Europea, su impacto es global, ya que muchas empresas internacionales deben cumplir con sus regulaciones para operar en Europa (Comisión Europea, 2018).

Importancia para el estudio de caso: enfatiza la protección de los datos personales y la privacidad de los individuos, imponiendo fuertes sanciones a las organizaciones que no cumplan con sus requisitos. Este reglamento es especialmente relevante para las empresas del sector salud, que manejan grandes cantidades de datos personales y sensibles. Es importante resaltar que el GDPR en su Art. Nº 9 (Reglamento general de protección de datos, 2018) aborda el tratamiento datos referentes a la salud y los denomina como categorías especiales e indica una serie de condicionales para su tratamiento.

Uso: Para las empresas del sistema de salud privado uruguayo, alinearse con las directrices del GDPR. Puede no solo ayudar a cumplir con los estándares internacionales de protección de datos, sino también mejorar las prácticas de gestión de la privacidad y aumentar la confianza de los pacientes en cómo se manejan sus datos.

Marco de Ciberseguridad de AGESIC

En Uruguay la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento promueve las prácticas digitales en todos los niveles, y en particular establecen un marco de referencia en ciberseguridad denominado Marco de ciberseguridad de Agesic (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, 2022). Cuenta con las siguientes características:

- Gestionar los riesgos inherentes a la seguridad de la información y al uso de la infraestructura tecnológica que le da soporte.
- Adoptar una política de gestión de seguridad de la información.
- Contar con una política de gestión de incidentes.
- Modelo de madurez con niveles (ver anexo modelo).

- Adoptar las medidas necesarias para lograr centros de datos seguros.
- Cumplir con la normativa vigente en materia de seguridad de la información cómo la Ley N°18331 (Ley N° 18331, 2008).

Tiene como particularidad que sus definiciones están basadas en diferentes estándares internacionales.

Toma como referencia el marco definido por NIST CSF con el cometido de dar respuestas a las amenazas cibernéticas, la gestión de los riesgos y la seguridad de la información con un lineamiento internacional.

Importancia para el estudio de caso: el apego al marco brindado por Agesic permite alinearse a un conjunto de estándares internacionales con una visión y contexto para Uruguay, también es importante destacar que no es un documento estático, sino que se irá modificando de acuerdo a los cambios tecnológicos, la evolución de las amenazas y los cambios en las técnicas de gestión de riesgos.

Uso: para las empresas privadas permite planificar su estrategia de gestión de riesgos de ciberseguridad y desarrollarla a lo largo del tiempo en función de su actividad y con el contexto de Uruguay, pero el marco sin embargo no tiene un respaldo obligatorio y normativo que lo ampare.

Guía de implementación del marco de ciberseguridad

En el sector salud, esta guía permite asegurar que las organizaciones cumplan con los requisitos normativos y protejan la integridad, disponibilidad y confidencialidad de los datos clínicos. Además, fomenta la adopción de medidas preventivas, como el control de acceso, el cifrado de datos y la gestión de incidentes de seguridad como propone el marco.

La importancia de la Guía de Implementación del Marco de Ciberseguridad (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, 2022) de Agesic

radica en su capacidad para proporcionar información clara, estructurada y de rápido acceso para que las organizaciones pueden utilizar para mejorar su postura de seguridad. En el sector salud, donde los datos manejados son extremadamente sensibles, esta guía es esencial para garantizar la seguridad de la información y la protección de los pacientes. La implementación de este marco con la guía no solo ayuda a las organizaciones a cumplir con las regulaciones nacionales existentes, sino que también intenta reducir el riesgo de ciberataques, minimizar el impacto de incidentes de seguridad y homogenizar el ecosistema de empresas y servicios en Uruguay en el tratamiento de datos sensibles.

A su vez, seguir las directrices establecidas en la Guía de Implementación del Marco de Ciberseguridad, específicamente las organizaciones de salud en Uruguay pueden desarrollar una estrategia integral que aborde las amenazas cibernéticas, cumpla con los requisitos legales y promueva una cultura de seguridad de la información en toda la organización.

La guía demuestra la intención del gobierno en brindar una herramienta que sea adaptable a diferentes contextos de organizaciones, y que expone de forma clara y resumida lo necesario para implementar el marco.

Glosario de ciberseguridad

El glosario de ciberseguridad, que es de acceso público es donde se determina y estimula a utilizar un lenguaje común con cierto nivel técnico para la disciplina de ciberseguridad para el contexto regional de Uruguay, el mismo promueve un claro entendimiento de las partes. Se considera un aporte valioso para un contexto tecnológico en crecimiento en Uruguay (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, 2022).

Guía general de protección de datos personales en Uruguay

La guía promulgada por la Unidad Reguladora y de Control de Datos Personales URCDP propone una serie de buenas prácticas para la gestión y tratamiento de datos personales en Uruguay, la misma se presenta como una herramienta de capacitación, y también demuestra el interés por parte del gobierno en el cuidado de los datos.

Se puede encontrar que se ha realizado con el enfoque de las normativas ya vigentes y que en su lectura hace una fácil herramienta para quienes comienzan a abordar el tema (Unidad Reguladora y de Control de Datos Personales, 2022). En sus principios en relación a los datos se invocan los siguientes términos como pilares: veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva, responsabilidad; esta última debe ser de carácter proactiva. Se demuestra un objetivo claro en el cuidado y la capacidad de acción para los titulares de los datos.

2.2.2 Normativas y legislaciones en Uruguay

A continuación, se identifican las regulaciones específicas y generales en materia de datos y ciberseguridad que aplican a las empresas privadas de salud en Uruguay, como leyes y decretos específicos que impactan en el sector de la salud.

En particular se abordan las normativas vigentes en materia de tratamiento de los datos y obligaciones, las mismas se describen a continuación y han requerido el entendimiento de que en su aplicación y combinación se denota la intención por parte de las estrategias de gobierno en Uruguay en no descuidar la temática.

Un hallazgo a destacar en el estudio, es que en el Art. Nº 78 de la Ley 20.212 (Dirección Nacional de Impresiones y Publicaciones Oficiales, 2023) se propone estrategias para el cuidado de la ciberseguridad, y obligaciones para el reporte de incidencias, pero solo para entidades privadas o públicas vinculadas a Administración Central.

Decreto N° 396/003, indica de interés público la historia clínica electrónica en Uruguay, el mismo imparte pautas en varios aspectos, pero fundamentalmente indica que se deberá dotar de seguridad los datos y responsabiliza a instituciones pública y privadas en su tratamiento y cuidado de la misma (Decreto N° 396/003, 2003).

Decreto 451/009 donde se indica que el Centro Nacional de Respuestas a Incidentes de Seguridad Informática tendrá el cometido y potestades la asistencia a nivel país de las incidencias en la disciplina de ciberseguridad (Decreto N° 451/009, 2009).

Decreto 452/009 donde se establece para la administración pública que se deben ejecutar políticas de seguridad de la información, con medidas para garantizar la confianza y seguridad de los sistemas y de la información en poder de los organismos públicos (Decreto N° 452/009, 2009). Lo que directamente involucra el intercambio de información del sector de salud privado a nivel de interoperabilidad con la administración pública.

Decreto 414/009, relativo a la ley de protección de datos, el mismo indica el tratamiento de los datos, en línea general el régimen jurídico de la protección de datos personales se aplica a su recolección, registro y todo tipo de tratamiento, ya sea automatizado o no, bajo cualquier soporte y modalidad de uso, tanto sea en el ámbito público como privado (Decreto N° 414/009, 2009).

Decreto N° 242/017, indica el tratamiento de intercambio de información con fines asistenciales, a través de la historia clínica electrónica (Decreto N° 242/017, 2017).

Ley N°18331, Ley de protección de datos, la misma tiene como cometido el tratamiento de los datos e indica las pautas de tratamiento tanto a nivel público como privado (Ley N° 18331, 2008).

Artículo 19 de Ley Nº 18.331, establece que:

> Datos relativos a la salud. - Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley. (Dirección Nacional de Impresiones y Publicaciones Oficiales, 2008)

Decreto Nº 122/019, donde se regula la incorporación de las instituciones de salud y las personas al sistema de Historia Clínica Electrónica Nacional, y establece el derecho de toda persona a oponerse al acceso a su información clínica a través de la citada plataforma. También se hace foco en la regulación de las instituciones de salud públicas y privadas, la seguridad, la gestión de acceso de la información (Decreto N° 122/019, 2019).

Decreto N° 64/020, se trata exclusivamente todo sobre los mecanismos de tratamiento de datos, desde el ámbito territorial, la responsabilidad en ser proactivo en la seguridad, privacidad por diseño [5](PbD), privacidad por defecto. Éste último siendo uno de los fundamentales porque determina de forma puntos fundamentales como: técnicas de disociación y minimización de datos, tiempo de conservación de los datos, considerando sus tipos y su tratamiento (Decreto N° 64/020, 2020).

Normativas recientes

Durante la investigación se ha observado el trabajo proactivo por parte del gobierno en diversos aspectos, específicamente en el marco legal, se aprobó por el parlamento un nuevo

[5] Según establece el decreto Decreto N° 64/020 en su Artículo 9, se define que El responsable y el encargado del tratamiento, en su caso, aplicarán las medidas técnicas y organizativas apropiadas a los efectos de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación refiere a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su comunicación (Decreto N° 64/020, 2020).

proyecto (Ferrere, 2024) donde establecen nuevas normativas sobre delitos informáticos en Uruguay. Esto es importante ya que si bien no hay reglamentaciones específicas y tipificación para los delitos cometidos en el sector estas nuevas tipificaciones marcan claramente una forma de penalizar de forma clara los delitos relacionados al área informática.

Entre los más importantes que se encuentran son: acceso ilícito a datos informáticos, daño informático, y vulneración de datos. Este último con el agravante de que si se comete con una finalidad lucrativa o contra datos personales protegidos por la ley puede ser penado con hasta 6 años de penitenciaría.

A su vez, se propone un registro para los ciberdelincuentes, y habilita a instituciones de intermediación financiera y entidades emisoras de dinero electrónico a la creación de registros de personas involucradas en actividades ilícitas en el ciberespacio. En este contexto, la ley exonera a dichas entidades del secreto bancario, por lo que podrán compartir entre ellas y con las autoridades competentes sus registros a fin de realizar denuncias o gestiones para prevenir y mitigar ciberdelitos.

2.3 Definición de los objetos de estudio

Unidad de análisis: empresas del sistema de salud privado uruguayo.

Para evaluar las prácticas de ciberseguridad en las empresas del sistema de salud privado en Uruguay, se consideraron diversas variables que reflejan la implementación y efectividad de las medidas de seguridad. El foco de las variables apunta a prácticas de ciberseguridad, percepciones y concientización, desafíos y barreras y estrategias futuras. A continuación, se detallan las variables que serán utilizadas en el trabajo de investigación:

1. Políticas y procedimientos de seguridad

1.1 Existencia de un sistema de gestión de seguridad de la información.

Variable: implementación de un SGSI (ver anexo fases SGSI) basado en estándares internacionales cómo ISO/IEC 27001:2022.

Indicador: presencia de certificación o conformidad con el estándar.

1.2 Políticas de seguridad de la información

Variable: documentación y actualización de políticas de seguridad.

Indicador: frecuencia de revisiones y actualizaciones de las políticas.

2. Control de acceso

2.1 Autenticación y autorización

Variable: uso de autenticación multifactorial MFA y control de acceso basado en roles RBAC.

Indicador: porcentaje de usuarios que utilizan MFA y número de roles definidos con permisos específicos.

2.2 Gestión de identidades y accesos

Variable: implementación de sistemas IAM para gestionar el acceso de usuarios.

Indicador: número de incidentes de acceso no autorizado detectados y mitigados.

3. Cifrado y protección de datos

3.1 Cifrado de datos en reposo y en tránsito

Variable: uso de encriptación para datos almacenados y en tránsito.

Indicador: tipos de cifrados utilizados, que sean actuales y vigentes. Y alcance de cifrado de datos según criticidad.

3.2 Protección de datos sensibles

Variable: implementación de medidas para proteger datos personales y clínicos sensibles.

Indicador: número de brechas o incidencias de datos reportadas y medidas correctivas tomadas.

4. Monitoreo y detección de amenazas

4.1 Sistemas de monitoreo continuo

Variable: implementación de soluciones de sistemas de gestión de eventos e información de seguridad SIEM.

Indicador: número de alertas de seguridad procesadas y tiempos de respuesta.

4.2 Detección y respuesta a intrusiones

Variable: uso de herramientas IDS-IPS, detección de intrusos y prevención de intrusos.

Indicador: número de intentos de intrusión detectados y bloqueados.

5. Capacitación y concientización del personal

5.1 Programas de capacitación en ciberseguridad

Variable: frecuencia y cobertura de programas de capacitación para el personal.

Indicador: porcentaje de empleados capacitados anualmente y evaluación de efectividad de la capacitación.

5.2 Concientización sobre seguridad informática

Variable: iniciativas de concientización y campañas internas.

Indicador: número de campañas realizadas y participación del personal.

5.3 Concientización sobre amenazas específicas

Variable: programas de y campañas sobre amenazas y procedimientos de ataques más comunes utilizados como secuestro de información a través de ransomware, y ataques de phishing.

Indicador: cantidad de capacitaciones específicas y talleres de simulación para los empleados.

6. Gestión de incidentes

6.1 Plan de respuesta a incidentes de seguridad

Variable: existencia y pruebas regulares del plan de respuesta a incidentes.

Indicador: número de simulacros realizados y tiempo promedio de respuesta a incidentes.

6.2 Registro y análisis de incidentes

Variable: documentación y análisis de incidentes de seguridad.

Indicador: número de incidentes registrados y análisis forenses realizados.

7. Evaluaciones y auditorías de seguridad

7.1. Auditorías de seguridad internas y externas

Variable: frecuencia de auditorías y evaluaciones de seguridad.

Indicador: resultados de auditorías y número de recomendaciones implementadas.

7.2. Pruebas de penetración

Variable: realización de pruebas de penetración para identificar vulnerabilidades.

Indicador: frecuencia de pruebas y número de vulnerabilidades críticas detectadas.

7.3 Infraestructura obsoleta

Variable: auditorías de sistemas y análisis de ciclos de actualización

Indicador: Porcentaje de sistemas y software que no están actualizados o son obsoletos.

8. Gestión de riesgos

8.1. Evaluación y gestión de riesgos cibernéticos

Variable: procesos de identificación, evaluación y mitigación de riesgos cibernéticos.

Indicador: número de riesgos identificados y mitigados, y la efectividad de las medidas de mitigación.

9. Recursos financieros

9.1 Recursos destinados al área de ciberseguridad

Variable: presupuesto destinado específicamente al área de ciberseguridad en su totalidad, desde gastos de en infraestructura hasta el personal especializado.

Indicador: presupuesto asignado a ciberseguridad en relación con el presupuesto total del área de sistemas.

10. Personal especializado

10.1 Especialistas dedicados a ciberseguridad

Variable: asignación de personal especialista en ciberseguridad a roles como CISO, y con dedicación total a la disciplina.

Indicador: Número de empleados dedicados a ciberseguridad en comparación con el tamaño de la empresa, roles asignados, y tipo de dedicación.

11. Sistemas médicos

11.1 Complejidad de los sistemas

Variable: implementación de inventarios y procesos de revisión de los activos de TI.

Indicador: número de sistemas y dispositivos conectados que requieren protección.

12. Resistencia al cambio

12.1 Nivel de resistencia

Variable: medidas y programas de evaluación al personal cuando enfrentan cambios tecnológicos.

Indicador: Nivel de resistencia del personal a adoptar nuevas políticas y tecnologías de seguridad.

13. Cumplimiento normativo y legal

Variable: revisión permanente del cumplimiento normativo y grado de entendimiento de los colaboradores acerca de las normas.

Indicador: grado de dificultad percibida para cumplir con las normativas y regulaciones de ciberseguridad.

14. Estrategias futuras

14.1 Planificación de inversiones en ciberseguridad

Variable: planes estratégicos de la dirección

Indicador: monto proyectado de inversiones en tecnología y soluciones de ciberseguridad para los próximos años.

14.2 Mejora de capacitación y concientización

Variable: planes de capacitación para los de recursos humanos.

Indicador: programas futuros planificados de capacitación planificados y objetivos de concientización.

14.3 Fortalecimiento de políticas y procedimientos

Variable: documentación de políticas de seguridad y sus planes de acción a futuro.

Indicador: número de nuevas políticas de seguridad planificadas y revisiones de procedimientos y políticas actuales.

14.4 Colaboración y alianzas

Variable: registros de acuerdos de colaboración

Indicador: número de alianzas y colaboraciones con otras organizaciones y entidades de gobierno para mejorar la ciberseguridad.

14.5 Implementación de estándares y cumplimiento de normativas

Variable: análisis de planes de cumplimiento

Indicador: proporción de empresas que planean adoptar o mejorar la implementación de estándares como ISO/IEC 27001 o marcos como NIST CSF.

La evaluación de las prácticas de ciberseguridad en las empresas del sistema de salud privado uruguayo requiere un análisis detallado de múltiples variables que cubran desde la gestión de la seguridad, la capacitación del personal y la gestión de incidentes. Siempre transitando desde lo estratégico hacia lo operativo, estas variables permiten al caso de estudio obtener una visión integral de la efectividad de las medidas y técnicas de seguridad implementadas en las empresas de salud, y proporcionan una base sólida para ponderar frente a niveles de madurez de marcos como el propuesto por Agesic.

2.4 Objetivos

2.4.1 Objetivo General

El objetivo general del trabajo es establecer criterios para la definición de un modelo de ciberseguridad en empresas del sistema de salud privado uruguayo.

2.4.2 Objetivos Específicos

Los objetivos específicos planteados en el trabajo son:

- Determinar el estado actual de la ciberseguridad en empresas del sistema de salud privado uruguayo.
- Identificar la existencia de estándares o marcos de referencia locales e internacionales para la ciberseguridad que sean aplicables a la industria y contexto de Uruguay.
- Formular recomendaciones de criterios a utilizar, para que los interesados puedan aplicar una guía de autoevaluación y un modelo de estándares de ciberseguridad en

la industria, con el objetivo de alcanzar estrategias sólidas y fortalecer la ciberseguridad.

2.5 Hipótesis

El estudio de caso plantea como base una hipótesis que se basa en la percepción general y permite contrastar con los resultados de la investigación, y brinda la capacidad de medir la percepción con los resultados analizados de forma científica. La hipótesis se describe a continuación:

Las empresas que brindan servicios de salud en Uruguay a nivel privado no cuentan con estándares, políticas o procedimientos adecuadamente implementados para el cuidado de los datos clínicos de los pacientes ni para asegurar la adecuada continuidad de sus operaciones ante un ciberataque.

2.6 Metodología

El enfoque del estudio de caso se establece como mixto, se recolectan datos para analizar de forma cualitativa y cuantitativa. Este enfoque permite obtener una visión holística de las percepciones, desafíos y estrategias en ciberseguridad. A su vez, se define el tipo de investigación más a adecuado para el estudio de caso, que tiene carácter descriptivo en cuanto a la caracterización de las prácticas de ciberseguridad y exploratorio en la identificación de falencias, desafíos y estrategias futuras.

Se plantea como estrategia que el diseño sea mixto y secuencial, en primer lugar, la ejecución con foco cuantitativo seguido de cualitativo.

3. Contexto

Durante el proceso de investigación previamente a la fase de la recolección de datos se ha hecho énfasis en obtener información sobre el contexto de las empresas del sector, para esto se han realizado entrevistas con actores del gobierno como Agesic, y asociaciones

internacionales cómo ISACA Montevideo Chapter[6]. Es muy importante analizar el contexto para entender el porqué de los hallazgos en la etapa recolección y análisis de datos.

3.1 Consulta con expertos

ISACA Montevideo Chapter

Asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

En reunión mantenida con la presidente del capítulo de ISACA Montevideo Chapter, ha brindado un panorama general donde se describe algunas características del sector de salud y argumenta que hay bastante por avanzar, pero se han generado directrices para acompañar el avance tecnológico, en sus actividades explica que ha sido parte del equipo de trabajo en la creación del Marco de Ciberseguridad de Agesic, por lo que su aporte en comentarios en la investigación es de mucha importancia.

Explica que se trabaja a nivel de gobierno en materia de ciberseguridad pero que queda mucho trabajo aún a nivel de normativas y de concientización.

A su vez, revela que el gobierno sigue trabajando en nuevas propuestas que seguramente tendrán un fondo normativo y obligatorio pero que aún falta tiempo para que se llegue a un estado óptimo de madurez en las organizaciones, siendo un problema ya que con la globalización y la diversidad de regiones que son atacadas por ciberdelincuentes es un problema hoy y no en el futuro.

Agesic

Uno de los principales actores ya que es la agencia de gobierno que imparte las directrices en todo lo referente a servicios electrónicos y de información en Uruguay, permitió

[6] Según se define en su portal, ISACA Montevideo Chapter es una Asociación de miembros profesionales sin fines de lucro, dedicados a la práctica de la Auditoría, Control y Seguridad de Sistemas, y comprometidos con la Educación, la Certificación, y los Estándares (ISACA Montevideo Chapter).

orquestar una entrevista con dos especialistas en la materia y muy relacionados al estudio de caso, con roles a nivel de implementación de historia clínica electrónica y en ciberseguridad.

La entrevista mantenida brindo un excelente aporte para la investigación, ya que, validó la hipótesis planteada para el trabajo.

La falta de normativa específica que marquen obligatoriedad de estandarización de políticas y procedimientos, así como la existencia de controles de auditoria hacen que el sector tienda a tener un enfoque reactivo a medida que ocurren incidentes o reportes que indican aumento de riesgo de ciberataque, pero no hay aún un estándar adecuado de implementación de medidas preventivas con base a un análisis de riesgo adecuado.

Otro punto que se analizó fue la Historia Clínica Electrónica Nacional, donde se comenta que Uruguay viene con grandes avances en sus etapas de implantación de la historia, pero que los esfuerzos son claramente a nivel funcional por parte de los prestadores de servicios de salud. Un punto importante que se analiza durante la entrevista es que las características de la infraestructura y aplicaciones dispuestas por parte del gobierno para la historia clínica electrónica demuestran gran fortaleza a nivel de seguridad informática, ya que es una red que requiere certificados y es cerrada. El ecosistema (AGESIC, 2016) de intercambio utiliza una tecnología actualizada y que deja registros de toda actividad, por otra parte, se resalta que esta plataforma que permite a los usuarios de cualquier prestador de salud tanto privado como público pueda ver su historial clínico sin importar desde donde se encuentre o donde se la brinde la atención. Por último, se remarca que el sistema HCEN es una infraestructura que permite la indexación de los documentos clínicos por lo que no guarda los mencionados documentos, sino que, es el prestador del usuario el que contiene los documentos electrónicos. En este último punto por parte de los especialistas de AGESIC comentan que la debilidad a nivel de seguridad informática se encuentra en el ecosistema de aplicaciones e infraestructura que disponen los prestadores de salud, por lo que el intercambio de información no presenta un riesgo, pero si

como el prestador mantiene los datos y qué grado de medidas y buenas prácticas dispone para hacerlo.

3.2 Análisis de informes

Informe: Ecosistema de Ciberseguridad en Uruguay

Durante el estudio de caso se ha identificado un informe (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento, 2020) realizado en el año 2020 por parte de Agesic y KPMG con importantes detalles del estado del país en relación con la ciberseguridad.

El informe reveló que el sector salud, junto con los sectores financiero y de tecnología, enfrenta desafíos significativos en ciberseguridad. El estudio se realizó mediante entrevistas a 40 empresas nacionales y 8 instituciones educativas para evaluar el desarrollo de la seguridad de la información en Uruguay. Los principales hallazgos del informe son:

- Desafíos significativos en ciberseguridad: destaca que tanto el sector salud como los sectores financiero y tecnológico enfrentan desafíos importantes en la protección de sus datos. Estos desafíos están relacionados con la creciente complejidad de las amenazas cibernéticas y la necesidad de adoptar medidas de seguridad más robustas.
- Evaluación del desarrollo en seguridad de la información: a través de las entrevistas, se evaluó cómo las organizaciones en Uruguay están desarrollando sus capacidades en seguridad de la información. Esto incluyó la identificación de vulnerabilidades, la implementación de políticas de seguridad y la respuesta a incidentes cibernéticos.
- Sector salud: el informe subraya que el sector salud es particularmente vulnerable debido al tipo de datos sensibles que maneja, lo que requiere una atención especial en la implementación de medidas de seguridad adecuadas.

Algunas de las estadísticas arrojadas indican que el 45% no cuentan con un área específica que trabaje en ciberseguridad y el 33% lo asocia a un problema de falta de asignación presupuestal de las empresas hacia el sector ciberseguridad.

Informe: Estado de la ciberseguridad en las empresas uruguayas.

También en la investigación se ha analizado informes de empresas expertas para obtener una visión no vinculada al estado, es por esto, que se ha relevado los resultados del último informe provisto por la empresa DataSec (DataSec, 2024), la que durante los últimos años viene lanzando un informe anual con una visión general de las empresas uruguayas y su relación con las prácticas de ciberseguridad.

En sus conclusiones del informe lanzado en inicios del año 2024 exponen las siguientes tendencias, un 21% se sienten completamente preparadas en términos de ciberseguridad y entienden están seguras, este número bajo considerablemente al informe del año 2022, donde un 34% aseguraban estar preparadas. Este indicador es muy importante ya que demuestra que se está tomando consciencia de su verdadero estado de situación, y los incidentes que han sucedido demuestran la gravedad y consecuencias que las organizaciones pueden tener. Revela que no se sienten tan seguros y entienden que la ciberseguridad es un área que merece gran dedicación y recursos en una organización.

Reporte de ciberseguridad 2020 – OEA y BID

El reporte por OEA y BID (Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2020) realiza un aporte muy importante informando en la evolución del estado de situación en América Latina y el Caribe, el mismo propone en base a dimensiones una serie de indicadores para Uruguay, con la capacidad de comparar con reportes anteriores, donde se puede identificar las tendencias. Dentro de lo principal que se puede analizar en la

entrega del año 2020, es que en todas sus dimensiones se denota un crecimiento positivo, por ejemplo, política y estrategia de ciberseguridad demuestra un aumento en casi la totalidad de sus indicadores, ellos se encuentran estrategia nacional de seguridad cibernética, respuesta a incidentes, protección de la infraestructura crítica y manejo de crisis (ver anexo indicadores).

Otra dimensión muy importante que hace referencia a marcos legales y regulatorios demuestra casi ser nulo en el reporte de 2016 a tener un gran aumento en todos sus indicadores, incluso alguno puntuados con un 100% como legislación sobre protección de datos protección de datos, y el referente a privacidad y libertad de expresión en línea (ver anexo indicadores).

Esta tendencia si bien puede ser reactiva a los eventos que vienen sucediendo en los últimos años, también demuestra que se trabaja en mejorar.

Estos informes son cruciales para entender el estado de la ciberseguridad en Uruguay y sirve como base para el estudio de caso y para la formulación de estrategias que fortalezcan la protección de datos en sectores críticos cómo la salud.

4. Protocolo de investigación

A continuación, se exponen en detalle cómo se ha definido el protocolo de investigación para el estudio de caso. Se ha establecido la secuencia más adecuada para el tipo de investigación y las características de esta, tomando en cuenta los factores como disponibilidad, recursos humanos y calendario académico.

4.1 Fase de preparación

Diseño: se diseñan y validan los instrumentos, este punto tiene un enfoque integral donde se espera a través de nuestras experiencias y entrevistas con expertos en el área de ciberseguridad encontrar las claves para la recolección de los datos. A su vez, cuando se concluyó el diseño de los cuestionarios y entrevistas, se propone una validación de los expertos

y una ejecución de plan piloto para evaluar las capacidades de los instrumentos de recolección con respecto al estudio de caso.

Solicitudes y permisos: se enviaron solicitudes a los participantes de la muestra, dando conocimiento de nuestro trabajo de tesis y temática, en la comunicación se exponen las características principales del trabajo y lo que se pretende abordar.

Se elaboran comunicaciones formales, donde se expone de forma clara la temática, la forma de abordaje y el tipo de datos que se pretende recolectar. Aquí una de las características y foco principal es que no se abordarán temas de configuraciones, tecnologías especificas ni especificaciones de sus proveedores de tecnología. Se establece que los datos expuestos de las organizaciones de salud encuestadas son anonimizados.

4.2 Fase de recolección de datos cuantitativos

Distribución de las encuestas: se enviaron las encuestas a través de Google Forms a todos los participantes de la muestra de las organizaciones del sector salud que han aceptado previamente participar. También se les envió un aviso vía correo electrónico.

Monitoreo: en base al monitor de respuestas que provee la herramienta de formularios utilizada se dio seguimiento a la tasa de respuestas, utilizando recordatorios en el caso de no recibir actividad en los formularios enviados. Se planificó un seguimiento activo para obtener la interacción máxima posible de los participantes.

4.3 Fase de recolección de datos cualitativos

Se contacto vía correo electrónico a los participantes para acordar una entrevista, la misma de carácter presencial o virtual dependiendo de la disponibilidad del participante, se pretendió captar al participante en la forma que se sienta más cómoda ya optimiza la capacidad de obtener más cobertura en respuestas, este punto es mixto ya que las organizaciones de salud que tienen disponibilidad podrán participar pero a su vez se realizó contacto con empresas

expertas en servicios de consultoría y auditoria en el área de ciberseguridad, con esto se pretende lograr obtener información desde otra perspectiva, la que brinda la posibilidad de cruzar datos y validar los resultados de la información recolectada.

4.4 Fase de revisión de documentos

Se analiza la información obtenida de los participantes externa a las encuestas y entrevistas realizadas, se pretende que cualquier información obtenida como posibles documentos de políticas, protocolos es valiosa y merece ser evaluada para ser analizada posteriormente.

4.5 Fase de análisis de datos

Análisis de datos cuantitativos: se utilizan herramientas estadísticas provistas por la suite de Google.

Análisis de datos cualitativos: se realiza el análisis por los participantes del equipo de trabajo del estudio de caso, el mismo identifica los patrones de moda de lo analizado, se pretende encontrar tendencias y coincidencias que aporten en validar los datos y resultados del análisis cuantitativo.

4.6 Fase de informe y presentación

Informe: Se realiza elaboración y revisión integra del estudio de caso, y se culmina la redacción del trabajo final.

Presentación: se prepara una presentación donde se expondrá el estudio de caso.

Recursos humanos: para la ejecución de la investigación del estudio de caso se contará con los dos investigadores que abordan el trabajo de tesis, los tutores y coordinador académico. También será de vital apoyo los expertos externos que apoyan el trabajo de forma meramente colaborativa y honoraria.

Consideraciones éticas: el consentimiento de todos los participantes encuestados donde se explica los objetivos, la voluntariedad y la confidencialidad, se realiza mediante comunicaciones vía correo electrónico donde registra constancia.

Confidencialidad: se protege la identidad de los participantes de los prestadores de salud utilizando códigos en lugar de nombres para anonimizar y asegurar el almacenamiento seguro de los datos recolectados.

5. Recolección de datos

Durante el estudio de caso se busca tener un enfoque integral y detallado en la recolección de datos. Dado el conocimiento adquirido durante la investigación, se busca que los métodos de recolección cualitativos tengan como característica ser abiertos y en modalidad de entrevista, a diferencia de una respuesta binaria como es el objetivo en el foco cuantitativo.

5.1 Definición de instrumentos

Encuestas cuantitativas

Instrumento: se diseñó un cuestionario estructurado que incluirá preguntas cerradas, múltiple opción y escalas para medir percepciones, conocimientos, y prácticas de ciberseguridad.

Distribución: las encuestas se distribuirán electrónicamente a través formularios en línea a los actores del área de tecnología y afines a la ciberseguridad de las empresas en el área de salud que hayan aceptado participar.

Alcance: percepciones sobre la importancia de la ciberseguridad, conocimientos sobre amenazas específicas, participación en programas de capacitación, uso de tecnologías y prácticas de ciberseguridad.

Entrevistas cualitativas

Instrumento: se realizaron entrevistas semiestructuradas con especialistas y responsables de tecnologías y ciberseguridad, teniendo foco en empresas que representen el sector en Uruguay.

Alcance: desafíos y barreras para la implementación de medidas de ciberseguridad, estrategias actuales y futuras, y experiencias con incidentes de seguridad.

Número estimado de entrevistas a realizar: se planificó un rango entre 5 y 10 entrevistas, dependiendo de la cantidad de información obtenida y disponibilidad de los expertos.

5.2 Cuestionario de autoevaluación

Prácticas de ciberseguridad en empresas del sistema de salud privado en Uruguay

Gracias por tomarse el tiempo para participar en esta encuesta. Su colaboración es crucial para entender las prácticas de ciberseguridad en el sistema de salud privado en Uruguay. La información proporcionada será tratada con total confidencialidad y se utilizará únicamente con fines académicos. A continuación, encontrará una serie de preguntas relacionadas con diversas áreas de ciberseguridad.

Instrucciones

Por favor, responda cada pregunta seleccionando la opción que mejor describa la situación en su organización.

Posición en la empresa:

- Gerente/Responsable de TI
- CISO/Responsable de Ciberseguridad
- Administrador de sistemas
- Otros: _____

Tamaño de la empresa:

- Pequeña (0-300 empleados)
- Mediana (300–1.000 empleados)
- Grande (+1000 empleados)

Sección general:

1. **¿La empresa cuenta con políticas de seguridad de la información (PSI) y un documento de gestión de seguridad?**
   - Sí
   - No
2. **¿La empresa tiene un Chief Information Security Officer (CISO) designado?**
   - Sí
   - No
3. **¿Existe un proceso para gestionar y controlar los riesgos relacionados con la ciberseguridad?**
   - Sí
   - No
4. **¿Se realizan actividades de capacitación interna y comunicación referentes con ciberseguridad para todo el personal?**
   - Sí
   - No
5. **¿Se monitorean y revisan los controles de seguridad, incluyendo pruebas de penetración y auditorías, por personal especializado?**
   - Sí
   - No

6. **¿Se realizan pruebas de penetración y/o auditorías de ciberseguridad con regularidad?**
   - Sí
   - No
7. **¿Los sistemas se actualizan regularmente mediante VCS (sistemas de control de versiones) y parches de seguridad?**
   - Sí
   - No
8. **¿Se realiza una evaluación de riesgos de ciberseguridad de los proveedores críticos?**
   - Sí
   - No
9. **¿Existe un plan formal para la gestión y reporte de incidentes de seguridad?**
   - Sí
   - No
10. **¿Existe un plan de contingencia y recuperación ante desastres?**
    - Sí
    - No
11. **¿Se aplican técnicas de cifrado para proteger los datos sensibles?**
    - Sí
    - No
12. **¿Se realizan respaldos periódicos de la información crítica?**
    - Sí
    - No

13. **¿Existe un sistema de monitoreo continuo para detectar amenazas y vulnerabilidades, incluyendo tecnologías como IPS e IDS?**
    - Sí
    - No
14. **¿El acceso a los sistemas y datos sensibles se gestiona a través de roles?**
    - Sí
    - No
15. **¿Se aplica el principio de "privacidad por diseño" en el desarrollo de sistemas y aplicaciones?**
    - Sí
    - No
16. **¿Se usan servicios de cloud computing y están considerados aspectos de ciberseguridad en este tipo de ambientes y servicios?**
    - Sí
    - No
17. **¿La empresa cuenta con personal específico dedicado al área de ciberseguridad, además del CISO?**
    - Sí
    - No
18. **En una escala del 1 al 5, ¿cómo evaluaría el nivel de conciencia sobre ciberseguridad desde la alta gerencia y el resto del personal (donde 1= menor compromiso, 5=mayor compromiso?**
    - Alta Gerencia: (1 a 5)
    - Resto del Personal: (1 a 5)

19. **¿Cuáles son los principales desafíos en la implementación de medidas de ciberseguridad? (Seleccione todas las que apliquen)**
    - Falta de recursos financieros
    - Falta de personal capacitado
    - Resistencia al cambio
    - Complejidad técnica
    - Falta de apoyo de la alta dirección
    - Otro (especifique): _____

Sección: Business Continuity Plan (BCP)

A continuación, realizaremos una serie de preguntas relacionadas con la existencia de un Plan de Continuidad del Negocio, así como la puesta en prueba de simulacros de recuperación en caso de desastre (DRP).

20. **¿La empresa tiene implementado un Plan de Continuidad del Negocio (BCP)?**
    - Sí
    - No
    - En proceso

En caso de contestar "No" la pregunta veinte puede omitir las siguientes y continuar con la sección de plan de contingencia.

21. **¿Con qué frecuencia se actualiza el BCP de la empresa?**
    - Anualmente
    - Semestralmente
    - Trimestralmente
    - Cuando se identifican cambios significativos
    - No se actualiza

22. ¿La empresa realiza pruebas y simulacros del BCP?

- Sí
- No
- En proceso
- No conoce

23. ¿Con qué frecuencia se realizan estas pruebas y simulacros?

- Anualmente
- Semestralmente
- Trimestralmente
- Ocasionalmente
- No se realizan

24. ¿La empresa tiene definido un objetivo de punto de recuperación (RPO) y un objetivo de tiempo de recuperación (RTO) para sus sistemas de información?

- Sí
- No
- En proceso
- No conoce

25. ¿Qué aspectos se evalúan durante las pruebas y simulacros del BCP? (Seleccione todas las que apliquen)

- Eficacia de los procedimientos de emergencia
- Tiempo de recuperación
- Comunicación y coordinación del equipo
- Disponibilidad de recursos
- Otros: _____

Sección: Plan de contingencia

El Plan de Contingencia es un conjunto de procedimientos diseñados para responder a emergencias y minimizar el impacto de eventos no previstos.

26. ¿La empresa tiene implementado un plan de contingencia?

- Sí
- No
- En proceso
- No conoce

****En caso de contestar "No" la pregunta veinte y seis puede omitir las siguiente y continuar con la sección de Implementación de Marcos de Ciberseguridad.***

27. ¿Qué componentes y aspectos incluye y se evalúan en el plan de contingencia? (Seleccione todas las que apliquen)

- Identificación de riesgos
- Estrategias de mitigación
- Planificación de respuesta
- Procedimientos de recuperación
- Comunicación y coordinación
- Capacitación y concientización
- Eficacia de los procedimientos de emergencia
- Tiempo de recuperación
- Disponibilidad de recursos
- Otros: _____

Sección: Implementación de Marcos de Ciberseguridad

A continuación, encontrará una serie de preguntas relacionadas con la implementación de la norma ISO/IEC 27001:2022 y el Marco de Ciberseguridad del NIST (NIST CSF).

***Recuerde que puede que no siga los lineamientos estrictos de los marcos/estándares pero sí se puede haber implementado alguno de los lineamientos de forma intuitiva.**

ISO 27001

La norma ISO 27001 es un estándar internacional para la gestión de la seguridad de la información (SGSI). Se centra en la implementación de un sistema de gestión que asegure la confidencialidad, integridad y disponibilidad de la información.

28. **¿La empresa ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001?**
    - Sí
    - No
    - En proceso
    - No conoce
29. **¿Qué etapas de implementación de la ISO 27001 ha completado la empresa? (Seleccione todas las que apliquen)**
    - Evaluación inicial
    - Análisis de riesgos
    - Diseño del SGSI
    - Implementación de controles
    - Auditorías internas
    - Certificación externa
    - Revisión y mejora continua

30. **¿La empresa ha realizado y revisa regularmente una evaluación de riesgos de seguridad de la información según los lineamientos de ISO 27001?**
    - Sí
    - No
    - En proceso
    - No conoce
31. **¿La empresa cuenta con políticas y procedimientos documentados para la gestión de la seguridad de la información según ISO 27001?**
    - Sí
    - No
    - En proceso
    - No conoce
32. **¿La alta dirección está comprometida con la implementación y mantenimiento de un SGSI conforme a ISO 27001?**
    - Sí
    - No
    - En proceso
    - No conoce

Sección: NIST Cybersecurity Framework

El Marco de Ciberseguridad del NIST proporciona directrices y mejores prácticas para gestionar y reducir los riesgos de ciberseguridad. Está compuesto por cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar.

33. **¿La empresa utiliza el Marco de Ciberseguridad del NIST para gestionar sus riesgos de ciberseguridad?**
    - Sí
    - No
    - En proceso
    - No conoce

34. **¿Qué componentes del NIST CSF ha implementado la empresa? (Seleccione todas las que apliquen)**
    - Identificar (gestión de activos, análisis de riesgos)
    - Proteger (controles de acceso, protección de datos)
    - Detectar (monitorización, detección de anomalías)
    - Responder (planificación de respuesta, comunicaciones)
    - Recuperar (recuperación de sistemas, mejora continua)

35. **¿La empresa ha implementado medidas de protección, como controles de acceso y protección de datos, conforme al NIST CSF?**
    - Sí
    - No
    - En proceso
    - No conoce

36. **¿La empresa cuenta con capacidades de detección de incidentes de ciberseguridad?**
    - Sí
    - No
    - En proceso
    - No conoce

37. **¿La empresa tiene planes de respuesta y recuperación ante incidentes de ciberseguridad siguiendo el NIST CSF o diseñados por la misma?**
    - Sí
    - No
    - En proceso
    - No conoce

Sección: Conocimiento y aplicación de normativas

En esta sección se encuentran marcos y principales normativas de Uruguay.

38. **¿La empresa sigue el Marco y Guía de Ciberseguridad de AGESIC?**

    (Este marco establece los lineamientos y estrategias para la protección de la información en las entidades públicas y privadas)
    - Sí
    - No
    - No conoce
39. **¿La empresa cumple con la Ley N° 18331 de Protección de Datos Personales?**

    (Esta ley regula la protección de datos personales y los derechos de las personas respecto a sus datos en Uruguay).
    - Sí
    - No
    - No conoce

40. ¿La empresa cumple con el Decreto N° 396/003 sobre protección de datos personales?

(Este decreto establece medidas específicas para la protección de datos personales en el país)

- Sí
- No
- No conoce

41. ¿La empresa cumple con el Decreto N° 451/009 sobre medidas de seguridad en el tratamiento de datos personales?

(Este decreto establece las medidas de seguridad que deben adoptarse en el tratamiento de datos personales para garantizar su protección).

- Sí
- No
- No conoce

42. ¿La empresa cumple con el Decreto N° 452/009 sobre reglamentación de la ley de protección de datos personales?

(Este decreto reglamenta diversos aspectos de la Ley N° 18331, incluyendo las obligaciones de los responsables de tratamiento de datos)

- Sí
- No
- No conoce

43. ¿La empresa cumple con el Decreto N° 414/009 sobre seguridad de la información?

(Este decreto establece las directrices y normativas para la seguridad de la información en organizaciones públicas y privadas)

- Sí

- No
- No conoce

44. ¿La empresa cumple con el Decreto N° 242/017 sobre la regulación de la ciberseguridad en el sector público y privado?

(Este decreto regula la ciberseguridad en ambos sectores, estableciendo las obligaciones y responsabilidades para proteger la infraestructura crítica)

- Sí
- No
- No conoce

45. ¿La empresa tiene conocimiento del Decreto N° 122/019 sobre la creación de un comité de ciberseguridad?

(Este decreto establece la creación de un comité de ciberseguridad para coordinar y supervisar las políticas y acciones para HCEN)

- Sí
- No
- No conoce

46. ¿La empresa cumple con el Decreto N° 64/020 sobre la implementación de medidas de ciberseguridad en el sector salud?

(Este decreto establece medidas específicas de ciberseguridad para proteger la información y los sistemas en el sector salud)

- Sí
- No
- No conoce

Sección: Modelo de madurez

47. **¿Si tuviera que categorizar la empresa en base a las preguntas anteriores, en que nivel de madurez entiende que se encuentra la misma?**

    (Seleccione el nivel que entienda más adecuado de 0 a 4)

    - Nivel 0: La organización no ha reconocido la necesidad de realizar esfuerzos en ciberseguridad y no hay acciones en marcha.
    - Nivel 1: Se realizan esfuerzos aislados en ciberseguridad, con un enfoque ad-hoc y alta dependencia del personal, sin documentación de tareas. La organización es reactiva ante incidentes.
    - Nivel 2: Existen lineamientos y cierta documentación para las tareas, aunque persiste la dependencia del conocimiento individual. Se ha avanzado en el desarrollo de procesos.
    - Nivel 3: Se han formalizado y documentado políticas y procedimientos. Se implementan automatizaciones y se establecen controles y métricas, centrando los esfuerzos en procesos, personas y tecnología.
    - Nivel 4: El RSI juega un rol clave en la mejora continua del SGSI. Se informan periódicamente a las partes interesadas y se alinean los esfuerzos de ciberseguridad con los objetivos de la organización.

48. **¿La empresa tiene previsto en los próximos seis meses comenzar a implementar un marco, norma o algún cambio relevante en la forma que maneja su ciberseguridad?**

    - Sí
    - No

5.3 Recopilación

Se realiza a través del formularios enviados y entrevistas a través de videoconferencia, en base a la disponibilidad de los participantes. Se procede de la siguiente forma:

- Encuestas cuantitativas: cuestionarios estructurados a través de Google Forms, los que devuelven la información de forma clara y con la que se establecerán los análisis estadísticos a posterior.
- Encuestas cualitativas: entrevista semiestructurada, se propone un guion en paralelo a las encuestas cualitativas, pero dando la posibilidad de una charla abierta, donde se espera recolectar datos relevantes y no precisamente específicos, pero sí que devuelvan niveles de percepción del tema con el entrevistado.

Las encuestas propuestas abarcan un amplio rango de aspectos relacionados con la ciberseguridad y la continuidad del negocio en las empresas del sistema de salud privado en Uruguay. A través de estas encuestas, se busca obtener una visión integral de las prácticas actuales, identificar áreas de mejora y entender los desafíos y oportunidades para fortalecer la seguridad y resiliencia en el sector salud.

5.4 Población de la muestra

Durante la investigación se han obtenido datos de la cantidad de prestadores integrales de salud del Uruguay, los datos obtenidos de un sitio del Ministerio de Salud Pública, nos muestra una totalidad de 40 prestadores en el ámbito privado (A tu servicio, 2024).

El dato a nivel país nos brinda también información sobre el porte de cada una de las organizaciones, donde se puede observar cómo indicador la cantidad de usuarios de cada una, siendo este un dato muy relevante ya que nos hace la idea de la cantidad de servicios que brinda y la cantidad de información que maneja a nivel de datos clínicos.

5.4.1 Población prestadores privados de Uruguay

Se ha obtenido la participación de 6 prestadores de servicio de salud, los que tienen un número de afiliados desde el entorno de 13.000 a 62.000, se entiende que la capacidad de abarcar una diversidad de tamaño, y sumado que el tamaño de la muestra sobrepasa el 10% del total de prestadoras privadas en Uruguay, se estima que la información recolectada es una representación diversa y adecuada para el estudio de caso. Es importante recordar que la sensibilidad y criticidad del tema hace que sea difícil la obtención de datos y empresas voluntarias.

Por último, es importante destacar que según los datos brindados el Ministerio de Salud Pública la población de afiliados en el ámbito privado supera los dos millones de personas a Julio de 2024 (Evolución Afiliados FONASA Julio 2007 - Julio 2024, 2024), lo que representa un 60% por ciento de la población total de Uruguay, que según censo de 2023 se encuentra en los tres millones cuatrocientos cuarenta y cuatro mil doscientos sesenta y tres habitantes (Censo 2023, 2023).

En la investigación del contexto destaca la relevancia del tema tratado en el estudio de caso, ya que la cantidad de datos sensibles y nivel de involucrados es muy alta.

5.4.2 Consultores y auditores expertos

Es muy importante y relevante el cruce de información para validar la información recolectada de las organizaciones que forman parte en la recolección de información, ya que se confía el conocimiento y el sentido de autocrítica del encuestado. Es por esto que se estableció en contra partida realizar una serie de entrevistas con empresas de gran porte de Uruguay que brindan servicios de consultoría a nivel de sistemas de información y en la disciplina de ciberseguridad, se pretende capturar su percepción en base a su experiencia y trabajos que realizan en el medio y conocer de primera mano las estrategias que se utilizan en la industria

uruguaya para la defensa de sus activos de información. También tratar de encuadrar su percepción con los modelos de madurez que se establecen en el marco teórico como NIST CSF y Marco de Ciberseguridad de Agesic. Se alcanza un número de 7 empresas en fase de recolección de datos.

6. Análisis de información

En esta sección se encuentran los análisis de la información recolectada.

Cabe destacar que en el análisis cuantitativo se consideran los datos obtenidos exclusivamente de las empresas del sector bajo análisis que respondieron las encuestas realizadas, mientras que el cualitativo posee un análisis basado en entrevistas con empresas que brindan servicios de consultoría y cuentan con gran experiencia en materia de ciberseguridad en Uruguay.

Para presentar el análisis se han agrupado los ítems en base a su vínculo dentro de la disciplina de ciberseguridad.

6.1 Análisis de datos cuantitativos

Perfil y tamaño de las empresas

El perfil de las personas que respondieron las encuestas está asociado directamente a especialistas de TI cuyos sus roles son directivos o realizan gestión dentro del sector, con un 50% de las respuestas correspondientes a personas que ocupan cargos de gerente o responsable de TI, un 33.3% como administradores de sistemas y el porcentaje restante a puestos de analista funcionales. Las empresas encuestadas se concentran principalmente en el segmento de medianas empresas, alcanzando estas un 83.3% de las respuestas, mientras que el restante 16.7% que respondieron corresponde a grandes empresas basándose en que su plantilla supera los 1000 trabajadores.

Análisis: el hecho de que las respuestas provengan principalmente de gerentes y responsables de TI sugiere que, aunque estas empresas tienen un enfoque en la gestión tecnológica, podría haber una desconexión en la adopción de prácticas avanzadas de ciberseguridad, dado que no se reportan en ninguna de las respuestas roles especializados como el de CISO o personal dedicado exclusivamente a la ciberseguridad. Es importante destacar que las encuestas fueron realizadas por quienes se sentían más a fin en la disciplina de ciberseguridad.

Gobernanza y políticas de seguridad

Ninguna de las empresas cuenta con políticas de seguridad de la información formalmente documentadas. Además, como se mencionaba anteriormente, no existe la figura de un CISO o responsable de seguridad de la información en ninguna de ellas.

Esto marca desde el inicio del análisis una tendencia que demuestra debilidades en la organización y falta de recursos y estrategias claramente definidas por parte de las empresas referente a la ciberseguridad.

Análisis: la ausencia de políticas de seguridad formalmente aprobadas o implementadas, y la falta de personal responsable exclusivo y especializado que sea responsable para estas tareas, refleja un nivel básico de gobernanza en ciberseguridad. Esto incrementa el riesgo de no contar con directrices claras para gestionar amenazas o incidentes de seguridad, afectando la capacidad de la organización para prevenir y responder adecuadamente a situaciones de riesgo relacionados con ciberataques.

Gestión de riesgos y controles de seguridad

El 66.7% de las empresas indican que gestionan riesgos de ciberseguridad, mientras que el restante 33.3% no lo hace, dejando expuesta a una nula gestión de riesgos a una porción muy

significativa de las empresas en el sector. Adicionalmente, ninguna de las organizaciones que respondieron las encuestas cuentan con auditorías internas que cubran con especialistas estás áreas, o pruebas de penetración para verificar sus controles de seguridad. En cuanto a las actualizaciones y parches de seguridad, el 66.7% de las empresas actualizan sus sistemas con regularidad, mientras que el restante 33.3% declara que no lo hace al menos adecuadamente. Además, cabe destacar que solo una empresa que representa el 16.7% de los encuestados evalúa a sus proveedores críticos en términos de riesgos de ciberseguridad.

Análisis: a pesar de que la aproximación al 67 % indica que de alguna forma se gestionan riesgos, la falta de auditorías formales, pruebas de penetración y evaluaciones de proveedores señala una debilidad considerable en los mecanismos para identificar y gestionar vulnerabilidades de manera proactiva que es prácticamente aplicable a la gran mayoría de las empresas encuestadas. El hecho de que un tercio del total no realice actualizaciones de seguridad periódicas aumenta el riesgo de exposición a ataques que explotan vulnerabilidades conocidas, y que dicha actividad forma parte de una parte muy básica en lo que refiere a mantención de la infraestructura.

Capacitación y concienciación en ciberseguridad

Solo el 16.7% de las empresas declara brindar capacitaciones sobre ciberseguridad a sus trabajadores. En términos de conciencia sobre la importancia de la ciberseguridad a nivel de alta gerencia y el resto de los trabajadores, el 66.7% responde a una conciencia intermedia a baja, mientras que el 16.7% muestra un nivel básico, y solo una de las empresas entiende estar en intermedio, lo que indica una comprensión limitada de las amenazas, riesgos que enfrentan, y las medidas de seguridad que necesitan.

Análisis: la falta de capacitación adecuada es un indicador de debilidad en la materia, ya que los trabajadores pueden convertirse en vectores de ataque si no están adecuadamente

preparados o informados de los riesgos. Aunque la mayoría de las empresas reportan cierto nivel de conciencia con tendencia a la baja, esta percepción como se demuestra no parece estar respaldada por acciones tangibles, como la implementación de políticas de ciberseguridad, el establecimiento de controles estrictos, o la existencia de personal dedicado y especializado a la ciberseguridad.

Preparación y respuesta ante incidentes

Ninguna de las empresas que respondieron la encuesta tiene un plan de gestión de incidentes de seguridad formalmente aprobado, lo cual es preocupante dado el incremento de ciberataques a nivel global y con preferencias al sector salud. Aunque el 66.7% cuenta con algún tipo de plan de contingencia para recuperación en caso de desastre, un 33.3% no está preparado para responder específicamente ante diversos escenarios de un incidente especifico, e incluso en la mayoría de los casos el plan de contingencia no cuenta con pruebas recientes que aseguren su éxito o plazos de recuperación en caso de necesidad. Sin embargo, el 100% de las empresas realizan respaldos de su información crítica, de manera regular. En lo referente a los planes de continuidad del negocio, el 66.7% no cuenta con un plan formal, mientras que solo el 16.7% lo tiene en proceso de desarrollo, y solo una dice tener implementado un plan de continuidad.

Por lo anterior, se puede decir que hay una evidente falta de pruebas de recuperación y simulacros de situaciones de desastre, y quienes las realizan no poseen una documentación formal o integral de cómo ocurrirá dicho proceso, sus plazos, sistemas críticos, entre otros ítems importantes que deben ser abordados como parte de un plan de recuperación de desastre.

Análisis: la ausencia de planes de gestión de incidentes es alarmante, ya que, sin ellos, las empresas podrían no estar preparadas para enfrentar eventos que interrumpan sus operativas, como ciberataques o fallas en el equipamiento en la infraestructura crítica. Si bien los respaldos de información son una práctica positiva, la falta de planes de continuidad formales y la

insuficiente preparación frente a eventuales incidentes graves, dejan a estas organizaciones en una situación vulnerable ante cualquier interrupción significativa.

Cifrado y gestión de acceso

Solo el 33.3% de las empresas implementa algún tipo de cifrado de sus datos sensibles, mientras que el 66.7% no lo hace, lo cual supone un riesgo importante para la protección de información crítica. En términos de gestión de acceso, el 100% de las empresas asegura haber implementado el acceso a sistemas y datos mediante la asignación de roles y acceso a recursos.

Análisis: la falta de cifrado en la gran mayoría de las empresas encuestadas representa una brecha crítica en la seguridad de la información. En caso de filtraciones, la exposición de datos sin mecanismos de cifrado o disociación podría tener consecuencias significativas para las empresas y funcionamiento de los servicios. Por otra parte, la implementación mayoritaria de controles basados en roles muestra un enfoque adecuado en la gestión de acceso, mitigando el riesgo de accesos no autorizados.

Adopción de tecnologías y principios

Solo el 16.7% de las empresas utiliza servicios de *cloud computing*, lo que indica una baja adopción a nuevas tecnologías demostrando la preferencia por la modalidad on premise. Así mismo, solo un 16.7% que corresponde a una de las empresas expresa no aplicar el principio de privacidad por diseño en sus procesos y sistemas, mientras que el porcentaje restante lo aplica.

Análisis: la baja adopción de servicios en la nube, que suelen ser alternativas robustas y con fuertes medidas de seguridad y pensadas para las amenazas actuales hacen que los mecanismos de seguridad sean aplicados por las propias empresas en sus modelos on premise, delegando en ellos una gran responsabilidad y compromiso sin las herramientas y personal adecuado. La integración de la privacidad por diseño, sugieren que estas empresas están en su

mayoría están intentando aplicar los principios de control de los individuos sobre sus datos, transparencia, y privacidad por defecto en sus sistemas. Esto se alinea con tendencias o normativas internacionales como el GDPR.

Recursos dedicados a ciberseguridad

Ninguna empresa tiene personal exclusivo dedicado a la ciberseguridad, lo que subraya una falta de recursos específicos en esta área. El 100% de las empresas señala la falta de personal capacitado como el principal desafío, junto con la resistencia al cambio en un 50%, la complejidad técnica en un 33.3%, y la falta de apoyo de la alta dirección en 50% entre las principales barreras significativas para abordar la ciberseguridad de manera formal en las empresas.

Se destaca en la siguiente en gráfica una tendencia muy clara en cuáles son los mayores obstáculos y desafíos (ver anexo Desafíos).

Es muy claro que se sitúan los indicadores de recursos financieros y personal capacitado como los mayores impedimentos que padecen las empresas del sector.

Análisis: la falta de personal especializado en ciberseguridad es un obstáculo para el desarrollo e implementación de políticas y controles eficaces. La percepción de complejidad técnica y la falta de respaldo por parte de la alta dirección indican que los esfuerzos en ciberseguridad no están siendo priorizados adecuadamente, lo cual afecta la capacidad de las empresas para implementar soluciones de seguridad robustas y adecuadas al servicio que brinda y necesitan.

Cumplimiento de normativas

En relación con el Marco y Guía de Ciberseguridad de AGESIC, el 50% de las empresas sigue este marco, mientras que el 33.3% no lo aplica y el 16.7% lo desconoce. Esto sugiere que,

aunque la mitad de las empresas está alineada con este marco, existe una proporción significativa que no lo sigue o no lo conoce, lo que evidencia la necesidad de una mayor difusión y adopción de estos lineamientos en el sector privado.

El cumplimiento de la Ley N° 18331 de Protección de Datos Personales es total, con el 100% de las empresas cumpliendo con esta normativa. Esto también se refleja en el cumplimiento del Decreto N° 396/003, el Decreto N° 451/009 y el Decreto N° 452/009, donde también se observa un 100% de cumplimiento en todos los casos. Las empresas declaran un alto nivel de alineación con las leyes de protección de datos, lo que indica que están en conocimiento con la normativa, aunque en la práctica no se demuestre tan claramente su implementación.

En cuanto al Decreto N° 414/009 sobre seguridad de la información, también se observó un cumplimiento total, con todas las empresas siguiendo esta normativa. Sin embargo, en el caso del Decreto N° 242/017, que regula la ciberseguridad en el sector público y privado referente a la historia clínica, el 66.7% de las empresas cumple con esta normativa, mientras que el 33.3% lo desconoce. Esto muestra que algunas organizaciones no están completamente al tanto de las obligaciones que impone este decreto, especialmente en lo que respecta a la protección de la infraestructura crítica, y responsabilidad de la historia clínica en su completitud y seguridad.

Respecto al Decreto N° 122/019, que establece la creación de un comité de ciberseguridad, solo el 50% de las empresas ha implementado este comité, lo que sugiere que la otra mitad no ha coordinado adecuadamente sus políticas y acciones de ciberseguridad de manera formal. Este es un aspecto clave que necesita fortalecerse dentro de las organizaciones.

En el caso del Decreto N° 64/020, que establece medidas específicas de ciberseguridad para el sector salud, el 83.3% de las empresas cumple con esta normativa, aunque el 16.7%

indicó desconocerla, lo que representa una brecha de concienciación dentro del sector respecto a normativas específicas.

Análisis: El análisis de los datos anteriores revela un alto grado de cumplimiento en ciertas normativas relacionadas con la protección de datos personales por parte de los encuestados, pero existen desafíos importantes en el ámbito de la ciberseguridad, donde algunos decretos clave, como los que requieren la creación de comités de ciberseguridad y la protección de la infraestructura crítica, no son plenamente conocidos o implementados.

Esto sugiere la necesidad de mayor capacitación y difusión sobre las normativas específicas del sector para garantizar que todas las empresas del sistema de salud en Uruguay estén alineadas con los estándares de ciberseguridad exigidos y la normativa vigente.

6.2 Análisis de datos cualitativos

Es importante destacar que cada uno de los entrevistados son referentes de excelencia en empresas de consultoría y auditoría que operan Uruguay. Entre las empresas encuestadas se destacan por un lado las Big Four[7] de Auditoría (Deloitte, EY, KPMG y PwC), así como, por otra parte, empresas especializadas en ciberseguridad como es el caso de: Data Sec, Security Advisor y Tilsor, todos referentes en prestación de servicios de consultoría y auditoría en ciberseguridad en Uruguay.

A continuación, se exponen los principales comentarios que aportaron estas empresas de consultoría abordadas en este trabajo:

[7] Big Four es el término inglés utilizado para referirse a las firmas más importantes del mundo en el sector de la consultoría y auditoría. Estas empresas son responsables de auditar los informes financieros de muchas de las mayores compañías del mundo y ofrecen asesoramiento estratégico en diversas áreas, incluyendo fusiones y adquisiciones, gestión de riesgos, entre otras. Las firmas integrantes son Deloitte, PwC, Ernst & Young y KPMG. (Economia3)

Nivel de madurez en ciberseguridad

Los aspectos más destacables son que la mayoría de las organizaciones en Uruguay aún operan en niveles bajos de madurez en ciberseguridad. De acuerdo con el modelo propuesto por Agesic, muchas empresas se sitúan en un nivel 2 o inferior según la mirada de expertos, lo que significa que las políticas de seguridad son reactivas y no están integradas en la estrategia corporativa a largo plazo. Este nivel denota que las organizaciones responden a las amenazas una vez que ocurren los incidentes, en lugar de prevenirlas proactivamente. Los expertos todos han concluido en esta reflexión.

Factores que contribuyen al bajo nivel de madurez

- Falta de planificación estratégica: la ciberseguridad no está incorporada como un aspecto esencial de la estrategia organizacional. No se identificaron planes claros para desarrollar y mejorar la ciberseguridad a lo largo del tiempo, lo que hace que las respuestas a incidentes sean improvisadas.
- Documentación y procedimientos inadecuados: las organizaciones no siguen marcos normativos o estándares internacionales de ciberseguridad como ISO 27001 o NIST CSF, lo que afecta negativamente la formalidad y estandarización de los procesos de seguridad.
- Reactividad frente a amenazas: la tendencia dominante es adoptar medidas de seguridad solo después de sufrir una violación de seguridad o incidente grave. Esto genera un enfoque a corto plazo y limita la efectividad de las soluciones.

Falta de normativa específica y sanciones

En el ámbito normativo, Uruguay ha avanzado en la protección de datos personales, pero las regulaciones específicas para la ciberseguridad son insuficientes, especialmente en sectores críticos como la salud. La Ley 18.331 regula la protección de datos, clasificando los

datos clínicos como sensibles, pero no impone sanciones severas en caso de incumplimiento de medidas de seguridad.

Comparación internacional

Países como Chile y Estados Unidos han implementado leyes más estrictas. En Chile, una nueva legislación exige a las empresas que demuestren la implementación de medidas de seguridad adecuadas o enfrentarán sanciones que pueden llegar al 3% de su facturación bruta anual. En Estados Unidos, las multas por incumplimientos en el manejo de datos de salud pueden alcanzar o superar los 50.000 dólares por incidente. Estas normativas han incentivado a las empresas a adoptar enfoques preventivos y a invertir en ciberseguridad como una prioridad empresarial.

Escasez de capital humano especializado

Otro de los grandes obstáculos es la falta de profesionales especializados en ciberseguridad. Muchas organizaciones dependen de equipos de TI que no están dedicados exclusivamente a la ciberseguridad, sino que realizan múltiples tareas que van desde la gestión de sistemas hasta la atención de incidentes de seguridad.

Consecuencias de la Falta de Especialización:

- Múltiples tareas y falta de enfoque: el personal de TI está sobrecargado con tareas no relacionadas directamente con la ciberseguridad, lo que limita la capacidad de monitorear, prevenir y responder eficazmente a las amenazas.
- Escasa automatización: debido a la falta de recursos humanos, las empresas no logran automatizar procesos de seguridad clave, como el monitoreo en tiempo real o la implementación de tecnologías avanzadas como detección y respuesta de terminales EDR.

Crecimiento del vector de ataques y amenazas

El aumento de la digitalización ha ampliado significativamente el vector de ataque en las organizaciones, especialmente en aquellas del sector salud que dependen de equipos médicos interconectados y sistemas de gestión de información. Este incremento en el uso de tecnologías aumenta la vulnerabilidad ante ataques cibernéticos, como el *ransomware* y otros tipos de secuestro de información.

Falta de recursos financieros y actitud reactiva

En Uruguay, la inversión en ciberseguridad sigue siendo baja porque se percibe como un gasto sin retorno inmediato. La actitud reactiva prevalece, lo que significa que muchas empresas solo invierten en seguridad cibernética después de haber sufrido pérdidas significativas. Este enfoque no solo aumenta la probabilidad de nuevos incidentes, sino que también incrementa los costos asociados a la recuperación y a la pérdida de reputación.

Patrones identificados

Enfoque reactivo en lugar de preventivo, es uno de los patrones más recurrentes en las organizaciones uruguayas. La ciberseguridad se maneja predominantemente de forma reactiva, es decir, las empresas toman medidas solo después de haber sufrido un ataque o incidente. A pesar de la creciente digitalización y la expansión del vector de ataques, pocas organizaciones implementan estrategias preventivas robustas que incluyan monitoreo continuo, simulaciones de ataques o pruebas regulares de vulnerabilidades.

Factores clave de este patrón

Prioridad a corto plazo: muchas empresas priorizan proyectos funcionales y operativos inmediatos, relegando la ciberseguridad hasta que ocurre una crisis. Este comportamiento genera una tendencia a asignar recursos solo cuando ya se ha sufrido una pérdida importante.

Falta de inversión en prevención: las organizaciones no perciben el valor de invertir en tecnologías y procesos preventivos, ya que estos no tienen un retorno inmediato o tangible, a diferencia de otras inversiones operativas.

Impacto: la falta de preparación ante posibles ataques eleva significativamente los costos de recuperación y las pérdidas reputacionales, especialmente en sectores sensibles como el de la salud. Las respuestas tardías incrementan el tiempo de recuperación y dejan a las empresas expuestas a nuevas vulnerabilidades.

Disparidad en la implementación de medidas de seguridad

Existe una marcada disparidad entre empresas en cuanto a la implementación de medidas de ciberseguridad. Algunas organizaciones han logrado algunos avances al adoptar soluciones avanzadas como sistemas de monitoreo y herramientas de detección y respuesta, mientras que otras apenas han comenzado a implementar estrategias mínimas de protección, o incluso operan sin ellas.

Factores clave de este patrón

Diferencias en la percepción de riesgo: las organizaciones más avanzadas y de mayor porte parecen tener una mayor conciencia de los riesgos asociados con la ciberseguridad, especialmente aquellas que ya han experimentado algún tipo de incidente. Sin embargo, otras empresas en el sector de servicios de salud, especialmente las pequeñas y medianas, subestiman las posibles amenazas y no invierten en medidas adecuadas y acordes a los datos que almacenan.

Limitaciones presupuestarias: las empresas que no han implementado medidas de seguridad robustas, a menudo, citan razones económicas. La inversión en tecnologías avanzadas, automatización y servicios externos como el monitoreo puede ser costosa, y muchas

empresas prefieren optar por soluciones más económicas, incluso en conocimiento de que son de menor calidad.

Esta disparidad genera un entorno de vulnerabilidad heterogénea donde algunas empresas están medianamente protegidas, mientras que otras quedan bastante expuestas. En sectores interconectados como la salud, esta desigualdad puede resultar peligrosa, ya que una brecha en una organización puede poner en riesgo a otras a través de interacciones o servicios compartidos.

Baja conciencia del riesgo y cultura de seguridad

Un patrón persistente es la baja percepción del riesgo en muchas organizaciones uruguayas, lo que genera una falta de urgencia para adoptar medidas de seguridad eficaces. A pesar del aumento de incidentes de ciberseguridad a nivel global, muchas empresas no consideran que puedan ser objetivos de ataques y, por lo tanto, no priorizan la implementación de políticas y procedimientos sólidos de seguridad.

Factores clave de este patrón

Subestimación de las amenazas: muchas empresas, especialmente en el sector de la salud, no consideran que su información sea un objetivo atractivo para los ciberdelincuentes. Sin embargo, los datos clínicos y personales están entre los activos más valiosos para los atacantes debido a su uso en actividades como el fraude de identidad.

Falta de programas de concientización: a nivel organizacional, hay una escasa inversión en programas de concientización y formación sobre ciberseguridad para los empleados. Esto significa que muchos incidentes siguen ocurriendo debido a errores humanos o desconocimiento de los riesgos asociados a acciones como el phishing o la ingeniería social.

Esta baja percepción de riesgo no solo expone a las organizaciones a ataques, sino que también las deja menos preparadas para responder cuando se produce una brecha. La falta de

concientización también favorece el comportamiento inseguro dentro de las empresas, haciendo que los esfuerzos de seguridad sean ineficaces.

Inversión limitada en tecnologías y servicios de ciberseguridad

La inversión en ciberseguridad sigue siendo limitada en la mayoría de las empresas uruguayas. En muchos casos, las organizaciones optan por alternativas más económicas y de menor calidad si es que lo hacen, aun cuando se conozca que no cumplen con los estándares de protección que necesitan. Este patrón es especialmente visible en los sectores más críticos, como el de la salud, donde la inversión en ciberseguridad debería ser una prioridad dada la sensibilidad de los datos manejados.

Factores clave de este patrón

Ciberseguridad como gasto y no como inversión: muchas empresas ven la ciberseguridad como un costo operativo sin retorno inmediato. Esto lleva a que los presupuestos destinados a la seguridad sean mínimos y se prioricen otros gastos que se perciben como más urgentes o rentables.

Preferencia por servicios extranjeros más baratos: algunas organizaciones optan por contratar servicios de ciberseguridad en el extranjero debido a los costos reducidos, aunque estos sean de calidad inferior en comparación con servicios nacionales especializados.

La inversión limitada genera un entorno de protección no óptima, donde las organizaciones pueden parecer seguras superficialmente, pero en realidad carecen de las herramientas y recursos adecuados para hacer frente a ataques sofisticados. En casos graves, esto puede llevar a violaciones de seguridad con consecuencias financieras y reputacionales significativas.

Desarrollo incipiente de estrategias basadas en marcos internacionales

A pesar de que muchos expertos en Uruguay están familiarizados con los marcos internacionales de ciberseguridad, como NIST CSF e ISO 27001, el desarrollo y adopción de estos marcos es limitado por parte de las organizaciones que brindan servicios de salud. Esto se debe, en gran parte, a la falta de exigencias normativas específicas y a una baja cultura organizacional en cuanto a la formalización de procesos de seguridad.

Factores clave de este patrón

Falta de normativas locales que exijan su implementación: si bien algunas empresas adoptan estos marcos de forma voluntaria, no existe una normativa que obligue a las organizaciones a cumplir con estos estándares internacionales, lo que deja un vacío en la implementación sistemática de buenas prácticas.

Bajo nivel de formalización de los procesos: la documentación y formalización de los procesos de seguridad es escasa. En muchos casos, los procedimientos de seguridad se llevan a cabo de manera informal o ad-hoc, lo que dificulta su seguimiento y mejora a lo largo del tiempo.

La falta de adopción de marcos internacionales limita la capacidad de las organizaciones uruguayas para alinear sus prácticas de ciberseguridad con los estándares globales, esto hace que las empresas uruguayas sean más vulnerables a los ataques.

7. Conclusiones

En la sección se encuentran los resultados del estudio de caso y una serie de recomendaciones que son de utilidad para las empresas del sector analizado, el trabajo brinda el estado actual de situación del sector en relación a la ciberseguridad, e importantes lineamientos producto del hallazgo.

7.1 Resultados y aportes

Las empresas encuestadas presentan un nivel de madurez en ciberseguridad que va desde bajo a medio en relación a los marcos analizados. Los resultados indican que las empresas en promedio se acercan a un nivel 2 en el marco de ciberseguridad de Agesic(ver pregunta 47 de 9.2 Información recolectada). Las respuestas obtenidas son consistentes con el resto del análisis realizado en el presente trabajo, en particular con las opiniones obtenidas en el análisis cualitativo a partir de entrevistas con especialistas en ciberseguridad y expertos del área. La falta de políticas de seguridad formales y de personal especializado en ciberseguridad revela una estrategia de gobernanza insuficiente para enfrentar las amenazas actuales. Además, la escasa capacitación en ciberseguridad y la limitada conciencia en la alta gerencia dificultan la adopción de medidas proactivas y robustas.

Aunque algunas prácticas como la gestión de acceso mediante roles y la realización de respaldos de información están bien implementadas, otras áreas claves, como la auditoría de riesgos, el cifrado de datos, la preparación para incidentes y la evaluación de proveedores críticos, presentan deficiencias significativas. Las carencias representan un riesgo elevado frente a ciberataques, fugas de información y fallas en la continuidad del negocio.

A su vez, los patrones identificados reflejan una tendencia general hacia un enfoque reactivo, con baja inversión y disparidad en la implementación de medidas de ciberseguridad en Uruguay. A pesar de que algunas organizaciones han avanzado en la adopción de tecnologías y estrategias más robustas, la mayoría aún enfrenta importantes desafíos para mejorar su estrategia de ciberseguridad. Las soluciones deberían enfocarse en el fortalecimiento de la concientización organizacional, la inversión proactiva, un alto nivel de adopción de marcos internacionales y locales de ciberseguridad para garantizar un nivel adecuado de protección frente a las amenazas cibernéticas y contexto actual.

Para avanzar hacia una mayor resiliencia en ciberseguridad es crucial que estas empresas adopten una estrategia integral que incluya la formalización de políticas de seguridad, la capacitación de su personal, la incorporación de tecnologías de vanguardia en ciberseguridad y la designación de recursos dedicados exclusivamente a la protección de sus activos de información y la continuidad de negocio. Es importante resaltar que, si bien las empresas intentan ajustarse a las normativas locales vigentes, al no haber un marco normativo integral y que contemple sanciones específicas, no resulta suficiente ni eficaz los esfuerzos de adopciones parciales. Cabe destacar que, el sector salud, al manejar información altamente sensible y proveer servicios críticos, debería estar entre las primeras industrias en implementar integralmente marcos de ciberseguridad reconocidos local o internacionalmente.

7.2 Recomendaciones

Se identifican los siguientes lineamientos en los cuales se detectaron debilidades significativas en las que se recomienda hacer foco, tanto por parte de las empresas, como por parte del gobierno, como forma de estandarizar la situación actual de las empresas del sector salud en materia de ciberseguridad.

7.2.1 Inversión en formación y capacitación

Es crucial aumentar la formación en ciberseguridad dentro de las organizaciones, no solo a nivel técnico, sino también a nivel administrativo. Programas de concientización o entrenamiento continuo para todo el personal pueden reducir significativamente la vulnerabilidad ante ataques dirigidos, especialmente aquellos que explotan debilidades relacionadas con acciones o inacciones de los recursos humanos.

7.2.2 Fomento de la inversión proactiva

Las empresas del sistema de salud privado uruguayo deben adoptar un enfoque proactivo, invirtiendo en tecnologías de prevención como los sistemas de detección y respuesta,

la inteligencia de amenazas y los planes de monitoreo continuo. La automatización de procesos y la implementación de servicios especializados de ciberseguridad les puede ayudar a mitigar la falta de personal.

7.2.3 Adopción de marcos internacionales

La adopción de marcos internacionales como NIST CSF 2.0, estándar ISO/IEC 27001:2022 para la gestión de amenazas y la evaluación de riesgos es esencial. Estos marcos proporcionan un conjunto de tácticas y técnicas que permiten a las organizaciones comprender y mitigar mejor las amenazas cibernéticas, aportando un enfoque integral, que en su iteración cubre la organización en todas las áreas. Es relevante que las empresas evalúen la implementación del SGSI o fases propuestas por el marco NIST CSF.

7.2.4 Fortalecimiento del marco normativo

Se sugiere como prioritario implementar regulaciones que obliguen a las empresas a cumplir con estándares mínimos de ciberseguridad, especialmente en sectores críticos como el de la salud. Esto incluye establecer sanciones económicas severas, pero a su vez realizar un ciclo de implementación por fases, que puedan ser auditadas y posteriormente pasibles de sanción en caso de incumplimiento. Es de destacar que los lineamientos deberían impartirse desde las autoridades de gobierno.

Si bien, durante el trabajo de investigación se obtuvo conocimiento de que existe una prioridad en la estrategia nacional de ciberseguridad de implementar estándares y normativas para el sector salud en los próximos 5 años, a la fecha el grado de avance resulta insuficiente.

7.2.5 Insumo de autoevaluación

Producto del estudio de caso se ha elaborado un instrumento de autoevaluación (ver anexo Instrumento), donde la empresa que desee conocer su estado de situación podrá completar una serie de preguntas. El referido cuestionario contempla las normativas que rigen

al momento en Uruguay, y proporciona en sus preguntas lineamientos de marcos y estándares internacionales que se podrían aplicar en las empresas. Recorrer el conjunto de preguntas invita al encuestado a la reflexión y expone una serie de actividades que podrán ser de utilidad como guía de implementación.

7.3 Limitaciones del estudio de caso

En la ejecución de la investigación encontramos una limitante relacionada con la criticidad y sensibilidad de los datos a recolectar.

En la etapa de recolección de datos, surgió que alguno de los invitados declinó en participar de las entrevistas o completar el cuestionario. Esta limitación fue contrarrestada con entrevistas a terceros especialistas del tema y de la industria. En particular, se introdujeron siete entrevistas con consultores y especialistas de ciberseguridad, cuatro de ellos pertenecientes a las empresas de auditoría conocidas como las Big Four, así como tres especialistas de consultoría de ciberseguridad que trabajan en el mercado local. Todas las entrevistas realizadas con estos especialistas confirmaron la hipótesis inicial, así como los datos recopilados de las empresas participantes en la encuesta, por lo que, si bien hubiera sido deseable contar con un muestreo más amplio de la industria analizada, la información obtenida es considerada suficiente para realizar las conclusiones y recomendaciones del presente trabajo.

8. Bibliografía

A tu servicio. (01 de Enero de 2024). *A tu servicio*. https://atuservicio.msp.gub.uy/

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (23 de Octubre de 2020). *Informe 2020: Ciberseguridad en Uruguay.* AGESIC: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/datos-y-estadisticas/estadisticas/informe-2020-ciberseguridad-uruguay

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (27 de Mayo de 2022). *Glosario de ciberseguridad.* Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/glosario-marco-ciberseguridad/3-definiciones/a

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (26 de Mayo de 2022). *Guía de implementación.* Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-implementacion/guia-implementacion-0

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. (28 de diciembre de 2022). *Marco de ciberseguridad*. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad

Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento. (s.f.). *Historia Clínica Electrónica Nacional.* Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento: https://www.gub.uy/ministerio-salud-publica/tramites-y-servicios/servicios/historia-clinica-electronica-nacional

AGESIC. (5 de Mayo de 2016). *Ecosistema de Salud de Uruguay - Arquitectura Salud.uy.* AGESIC: https://centroderecursos.agesic.gub.uy/web/arquitectura-salud.uy/inicio/-/wiki/Arquitectura+para+Salud/Ecosistema+de+Salud+de+Uruguay

Banco Interamericano de Desarrollo y Organización de los Estados Americanos. (01 de Julio de 2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe.* BID: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Censo 2023. (27 de Noviembre de 2023). *Presidencia.* https://www.gub.uy/presidencia/comunicacion/noticias/poblacion-uruguay-aumento-1-se-contabiliza-3444263-habitantes

Comisión Europea. (2018). *Reglamento General de Protección de Datos.* General Data Protection Regulation: https://gdpr-info.eu/

Commission International Organization for Standardization International Electrotechnical. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*

Comunidad de Madrid. (s.f.). *Cuatro décadas caminando juntos en Europa.* Comunidad de Madrid: https://www.comunidad.madrid/servicios/madrid-mundo/es-union-europea-funciona-hace

DataSec. (21 de Marzo de 2024). *Estado de la ciberseguridad en las empresas uruguayas, encuesta 2023-2024.* DataSec: https://datasec-soft.com/wp-content/uploads/2024/04/Informe-Datasec-2024_21MAR24.pdf

Decreto N° 122/019. (13 de Mayo de 2019). *Dirección Nacional de Impresiones y Publicaciones Oficiales.* https://www.impo.com.uy/bases/decretos-originales/122-2019

Decreto N° 242/017. (31 de Agosto de 2017). *Dirección Nacional de Impresiones y Publicaciones Oficiales.* https://www.impo.com.uy/bases/decretos/242-2017

Decreto N° 396/003. (30 de Setiembre de 2003). *Dirección Nacional de Impresiones y Publicaciones Oficiales.* https://www.impo.com.uy/bases/decretos/396-2003

Decreto N° 414/009. (31 de agosto de 2009). *Dirección Nacional de Impresiones y Publicaciones Oficiales.* https://www.impo.com.uy/bases/decretos/414-2009

Decreto N° 451/009. (28 de setiembre de 2009). *Dirección Nacional de Impresiones y Publicaciones Oficiales.* https://www.impo.com.uy/bases/decretos/451-2009

Decreto N° 452/009. (28 de setiembre de 2009). *Dirección Nacional de Impresiones y Publicaciones Oficiales.* https://www.impo.com.uy/bases/decretos/452-2009

Decreto N° 64/020. (17 de Febrero de 2020). *Dirección Nacional de Impresiones y Publicaciones Oficiales.* https://www.impo.com.uy/bases/decretos/64-2020

Dirección Nacional de Impresiones y Publicaciones Oficiales. (18 de Agosto de 2008). *CAPITULO IV - DATOS ESPECIALMENTE PROTEGIDOS.* Dirección Nacional de Impresiones y Publicaciones Oficiales: https://www.impo.com.uy/bases/leyes/18331-2008/19

Dirección Nacional de Impresiones y Publicaciones Oficiales. (06 de Noviembre de 2023). *Ley N° 20212.* Dirección Nacional de Impresiones y Publicaciones Oficiales: https://www.impo.com.uy/bases/leyes/20212-2023/78

Economia3. (s.f.). *Big Four: ¿Qué son, cuáles son y por qué lideran el mercado empresarial?* Economia3: https://economia3.com/big-four/

Evolución Afiliados FONASA Julio 2007 - Julio 2024. (01 de Julio de 2024). *Ministerio de Salud Pública.* https://www.gub.uy/ministerio-salud-publica/datos-y-estadisticas/datos/evolucion-afiliados-fonasa-julio-2007-julio-2024

Ferrere. (19 de Agosto de 2024). *Parlamento aprueba normativa sobre delitos informáticos en Uruguay.* Ferrere: https://ferrere.com/es/novedades/parlamento-aprueba-normativa-sobre-delitos-informaticos-en-uruguay/

IBM. (4 de Junio de 2024). *¿Qué es el ransomware?* IBM: https://www.ibm.com/es-es/topics/ransomware

IBM. (12 de Agosto de 2024). *¿Qué es la ciberseguridad?* IBM: https://www.ibm.com/es-es/topics/cybersecurity

ISACA Montevideo Chapter. (s.f.). *ISACA Montevideo Chapter.* ISACA Montevideo Chapter: https://engage.isaca.org/montevideochapter/aboutchapter/acerca-de

Ley N° 18331. (11 de agosto de 2008). *Dirección Nacional de Impresiones y Publicaciones Oficiales.* https://www.impo.com.uy/bases/leyes/18331-2008

National Institute of Standards and Technology. (23 de Abril de 2024). *NIST Cybersecurity Framework 2.0.* NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Reglamento general de protección de datos. (25 de Mayo de 2018). *Artículo 9 RGPD*. Reglamento general de protección de datos: https://gdpr-text.com/es/read/article-9/

Unidad Reguladora y de Control de Datos Personales. (24 de Enero de 2022). *Guía general de protección de datos personales en Uruguay.* GUB.UY: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-general-proteccion-datos-personales-uruguay

9. Anexos

9.1 Figuras

9.1.1 Reporte de ciberseguridad 2020 – OEA y BID

Fuente: (https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe)

Volver

Fuente: (https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe)

Volver

9.1.2 ISO/IEC 27001:2022

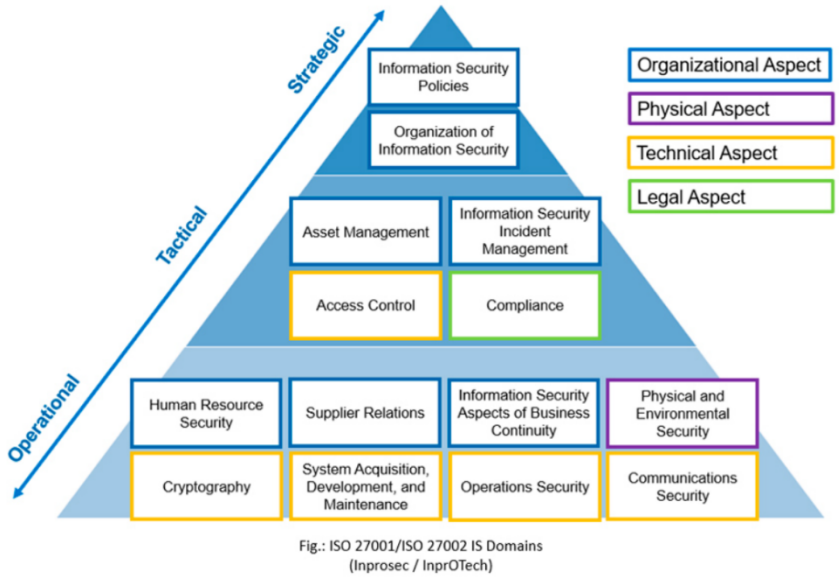
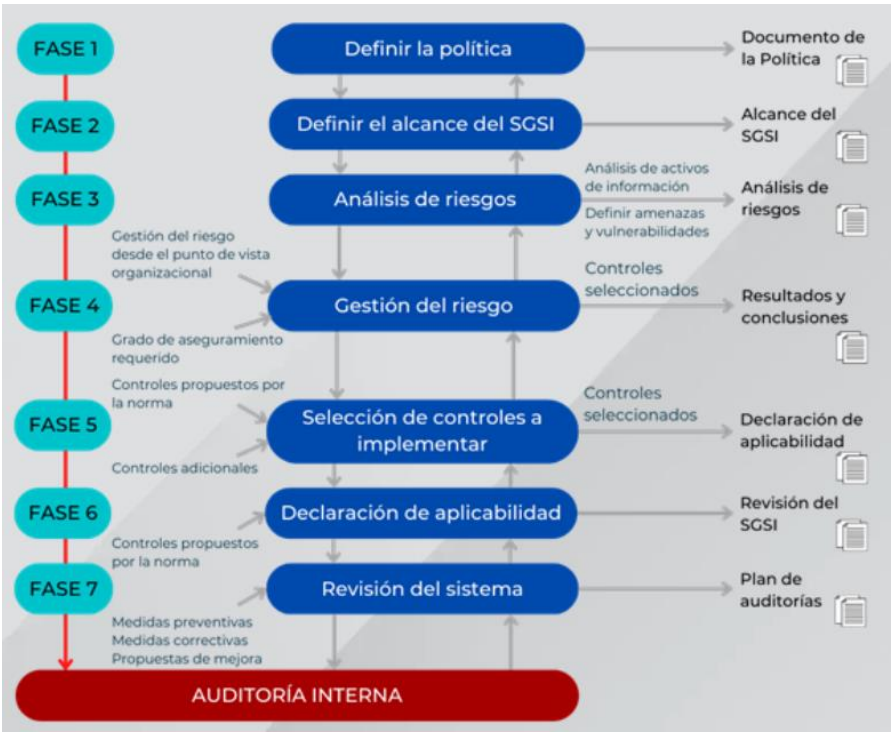


Fig.: ISO 27001/ISO 27002 IS Domains
(Inprosec / InprOTech)

Fuente:(https://www.inprosec.com/iso-27001-iso-27002-novedades-beneficios/)

Volver

9.1.3 ISO/IEC 27001:2022 fases SGSI



Fuente:(https://www.hacker-mentor.com/blog/iso-27001-version-2022)

Volver

9.1.4 NIST CSF ciclo

Fuente:(https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf)

Volver

9.1.5 Marco de Ciberseguridad Agesic

Nivel 1	Nivel 2	Nivel 3	Nivel 4
Mejor esfuerzo. Centrado en el centro de datos.	Extensión al resto de la organización.	Políticas y procedimientos formales.	Mejora continua. Auditoría.

Fuente: (https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad/estructura-del-marco-ciberseguridad/modelo-madurez)

Volver

- Nivel 0: Es el primer nivel del modelo de madurez donde las acciones vinculadas a seguridad de la información y ciberseguridad son casi o totalmente inexistentes. La organización no ha reconocido aún la necesidad de realizar esfuerzos en ciberseguridad. Este nivel no es incluido en la tabla del modelo de madurez.
- Nivel 1: Es el segundo nivel del modelo. Existen algunas iniciativas sobre ciberseguridad, aunque los esfuerzos se realizan en forma aislada. Se realizan

implementaciones con enfoques ad-hoc y existe alta dependencia del personal que lleva a cabo las tareas que habitualmente no se encuentran documentadas. Existe una actitud reactiva ante incidentes de seguridad.

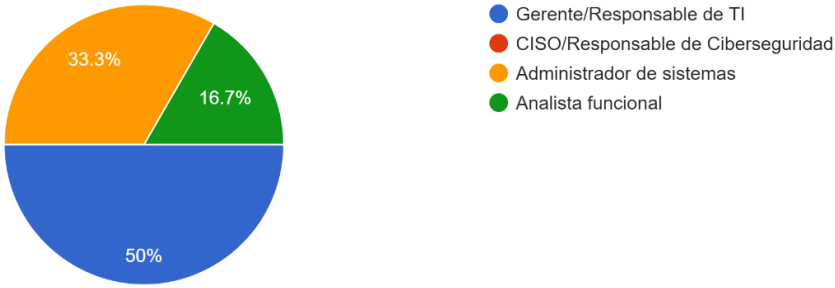
- Nivel 2: Es el tercer nivel del modelo de madurez. Se han establecido ciertos lineamientos o pautas para la ejecución de las tareas, pero aún existe dependencia del conocimiento individual. Se ha avanzado en el desarrollo de los procesos y existe cierta documentación para realizar las tareas.
- Nivel 3: Es el cuarto nivel del modelo de madurez y se caracteriza por la formalización y documentación de políticas y procedimientos, así como implementaciones de alta complejidad y/o automatizaciones que centralizan y permiten iniciativas de gobernanza. Las políticas y procedimientos son difundidos, facilitan la gestión y posibilitan establecer controles y métricas. Los esfuerzos en ciberseguridad se enfocan en los procesos, las personas y la tecnología.
- Nivel 4: Es el último nivel del modelo de madurez. El responsable de la Seguridad de la Información (RSI) tiene un rol clave en el control y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) realizando o coordinando actividades de control interno para verificar cumplimientos y desvíos. Se desarrollan las lecciones aprendidas que, junto con los controles determinan las acciones para la mejora continua. Las partes interesadas son informadas periódicamente, lo cual permite alinear los esfuerzos, estrategias y tecnologías de ciberseguridad con los objetivos y estrategias de la organización.

9.2 Información recolectada

En la sección se encuentran los resultados de la recolección de datos con las empresas privadas que accedieron a ser encuestadas, a continuación, se anexan las más relevantes y las que ejemplifican la realidad analizada.

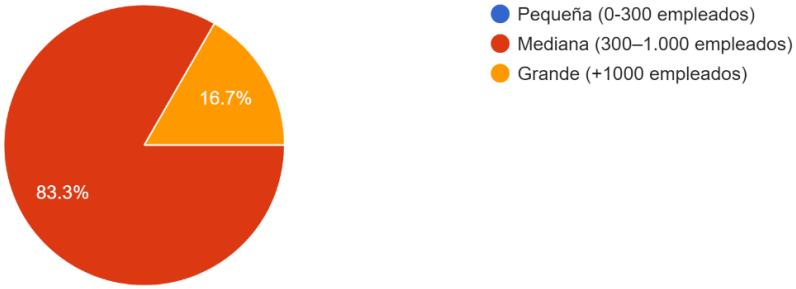
Posición en la empresa

6 respuestas

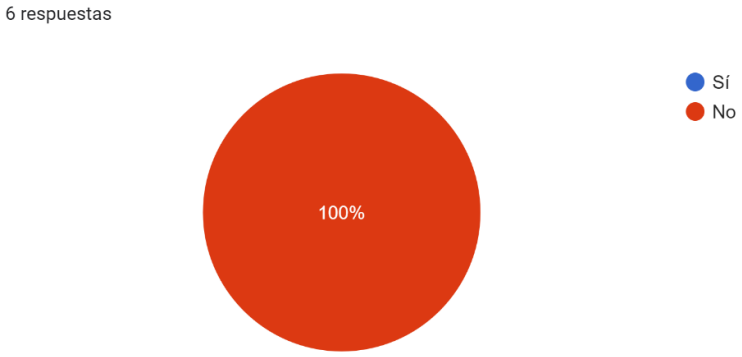


Tamaño de la empresa

6 respuestas

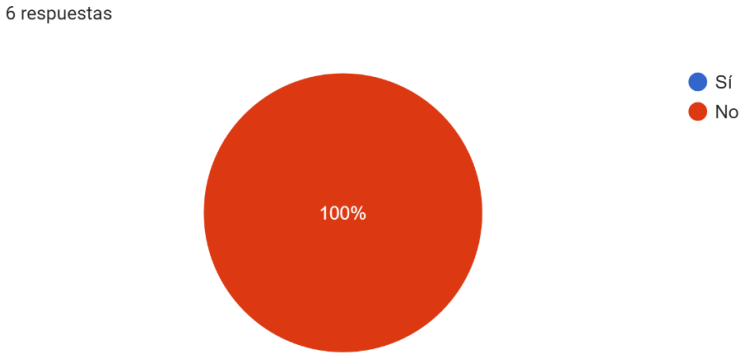


1. ¿La empresa cuenta con políticas de seguridad de la información (PSI) y un documento de gestión de seguridad?



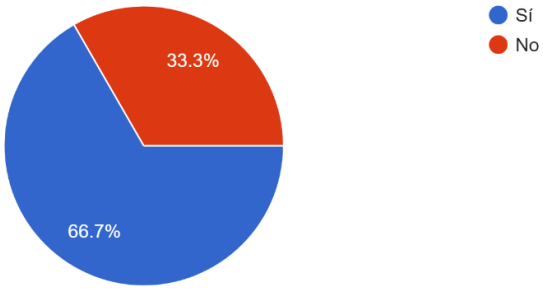
Volver

2. ¿La empresa tiene un Chief Information Security Officer (CISO) designado?



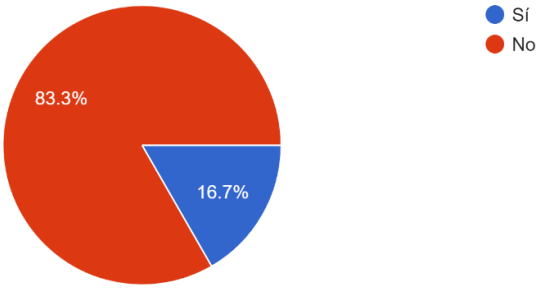
3. ¿Existe un proceso para gestionar y controlar los riesgos relacionados con la ciberseguridad?

6 respuestas



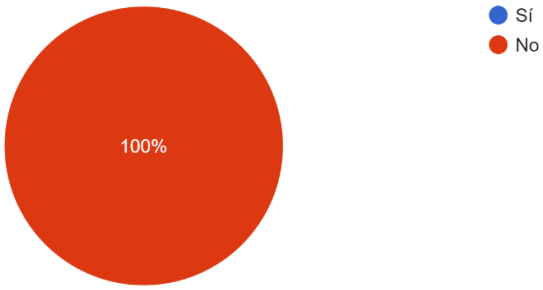
4. ¿Se realizan actividades de capacitación interna y comunicación referentes con ciberseguridad para todo el personal?

6 respuestas

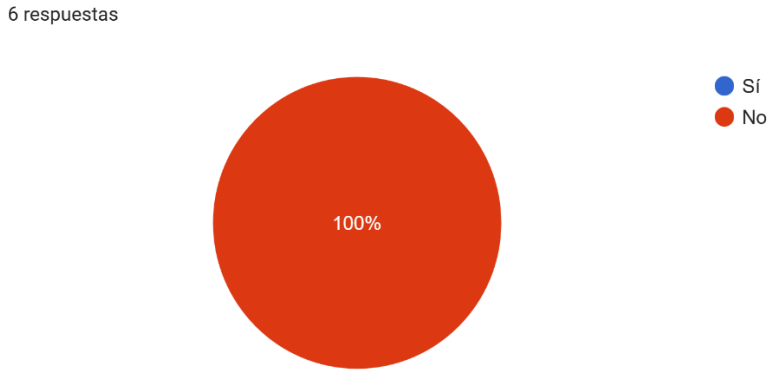


5. ¿Se monitorean y revisan los controles de seguridad, incluyendo pruebas de penetración y auditorias por personal autorizado?

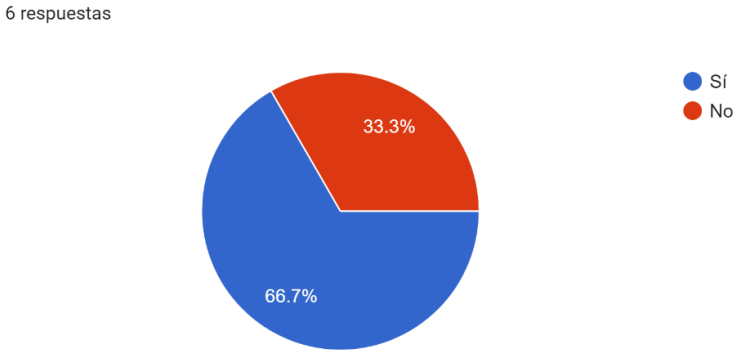
6 respuestas



6. ¿Se realizan pruebas de penetración y/o auditorías de ciberseguridad con regularidad?

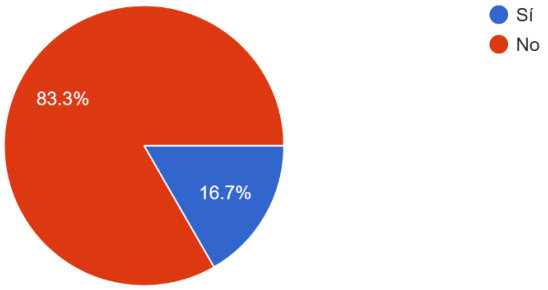


7. ¿Los sistemas se actualizan regularmente mediante VCS (sistemas de control de versiones) y parches de seguridad?



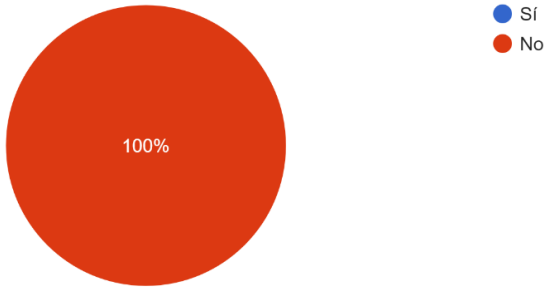
8. ¿Se realiza una evaluación de riesgos de ciberseguridad de los proveedores críticos?

6 respuestas



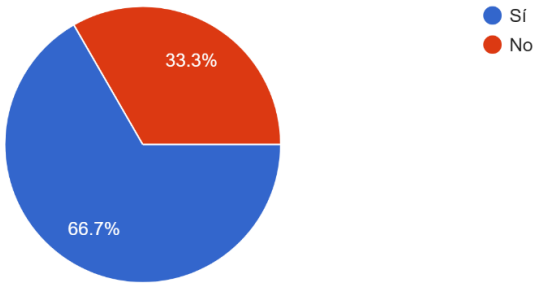
9. ¿Existe un plan formal para la gestión y reporte de incidentes de seguridad?

6 respuestas



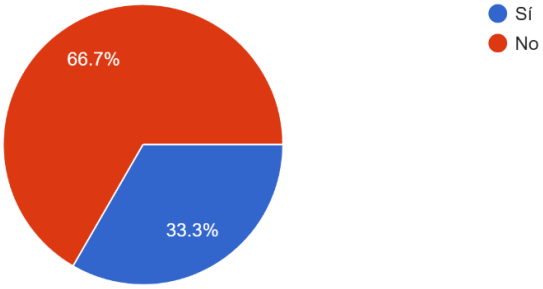
10. ¿Existe un plan de contingencia y recuperación ante desastres?

6 respuestas



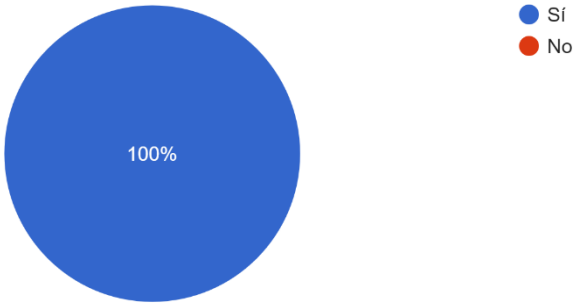
11. ¿Se aplican técnicas de cifrado para proteger los datos sensibles?

6 respuestas



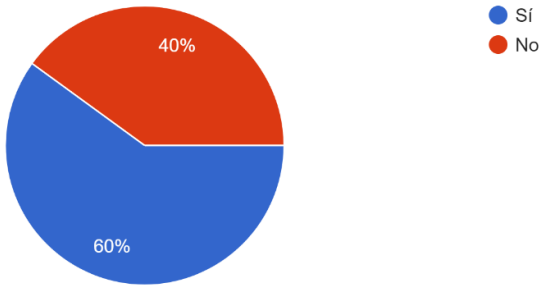
12. ¿Se realizan respaldos periódicos de la información crítica?

6 respuestas



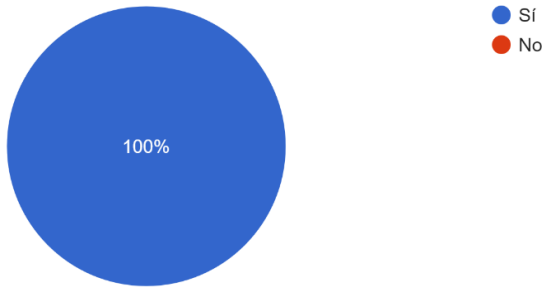
13. ¿Existe un sistema de monitoreo continuo para detectar amenazas y vulnerabilidades, incluyendo tecnologías como IPS e IDS?

5 respuestas



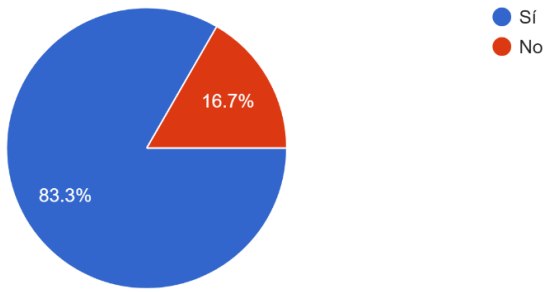
14. ¿El acceso a los sistemas y datos sensibles se gestiona a través de roles?

6 respuestas

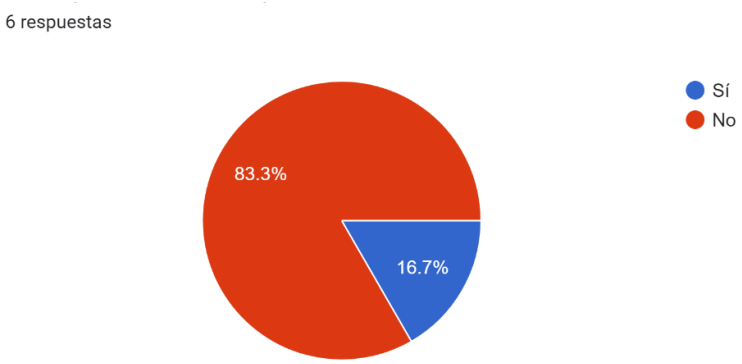


15. ¿Se aplica el principio de "privacidad por diseño" en el desarrollo de sistemas y aplicaciones?

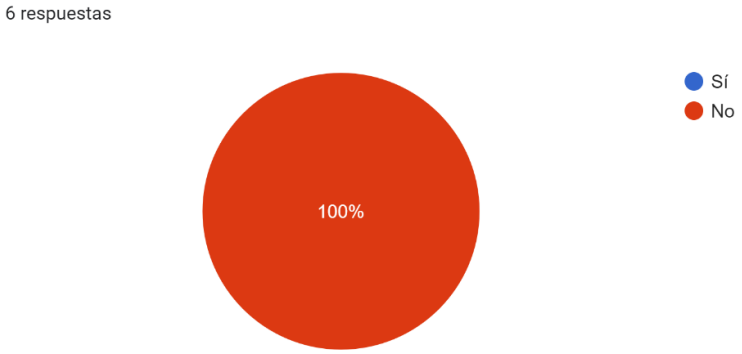
6 respuestas



16. ¿Se usan servicios de cloud computing y están considerados aspectos de ciberseguridad en este tipo de ambientes y servicios?

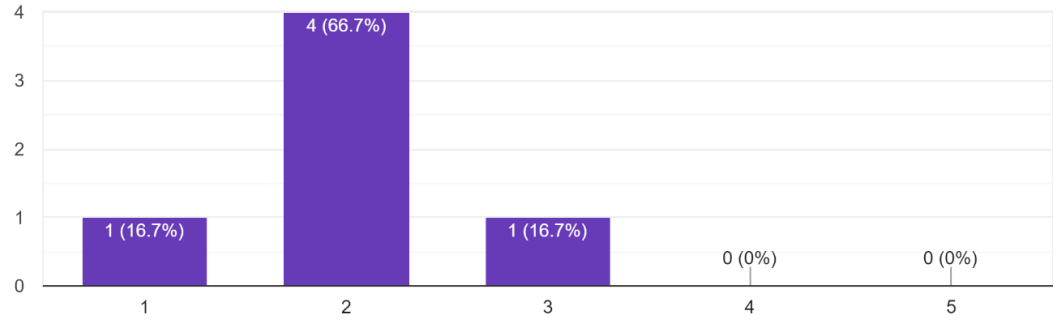


17. ¿La empresa cuenta con personal específico dedicado al área de ciberseguridad además del CISO?



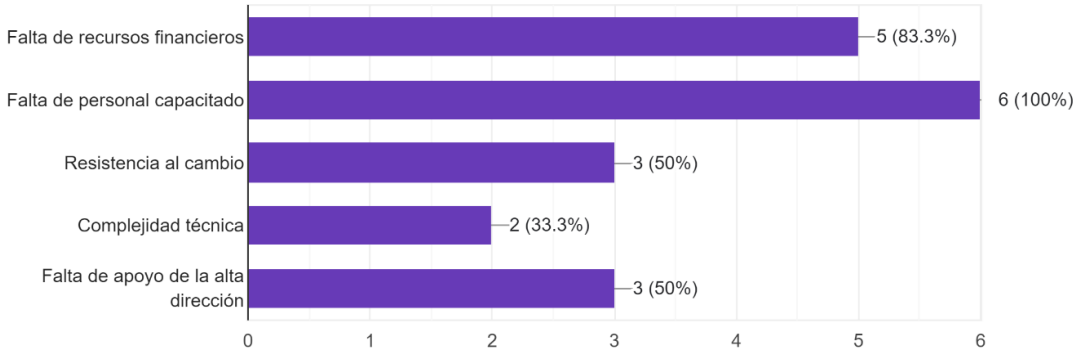
18. En una escala del 1 al 5. ¿Cómo evaluaría el nivel de conciencia sobre ciberseguridad desde la alta gerencia y el resto del personal? (Donde 1 indica menor compromiso y 5 mayo compromiso).

6 respuestas



19. ¿Cuáles son los principales desafíos en la implementación de medidas de ciberseguridad? (Seleccione todas las que apliquen).

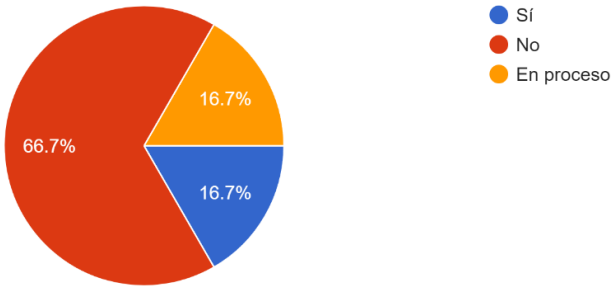
6 respuestas



Volver

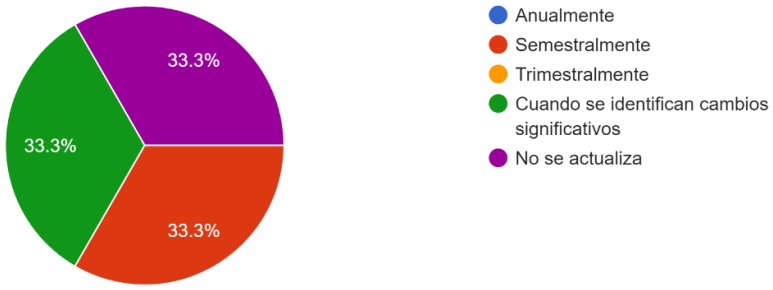
20. ¿La empresa tiene implementado un Plan de Continuidad del Negocio (BCP)?

6 respuestas



21. ¿Con qué frecuencia se actualiza el BCP de la empresa?

3 respuestas

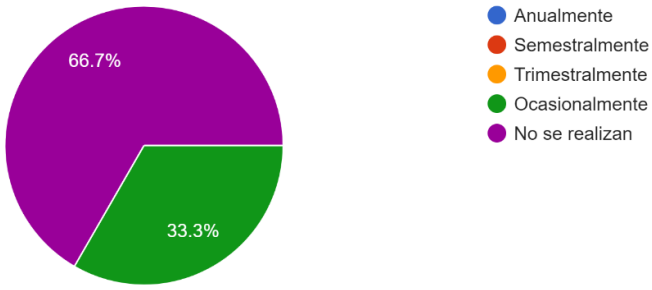


22. ¿La empresa realiza pruebas y simulacros del BCP?

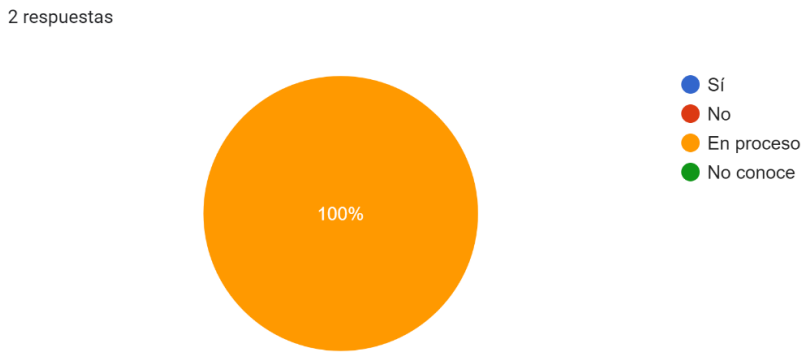
3 respuestas

23. ¿Con qué frecuencia se realizan estas pruebas y simulacros?

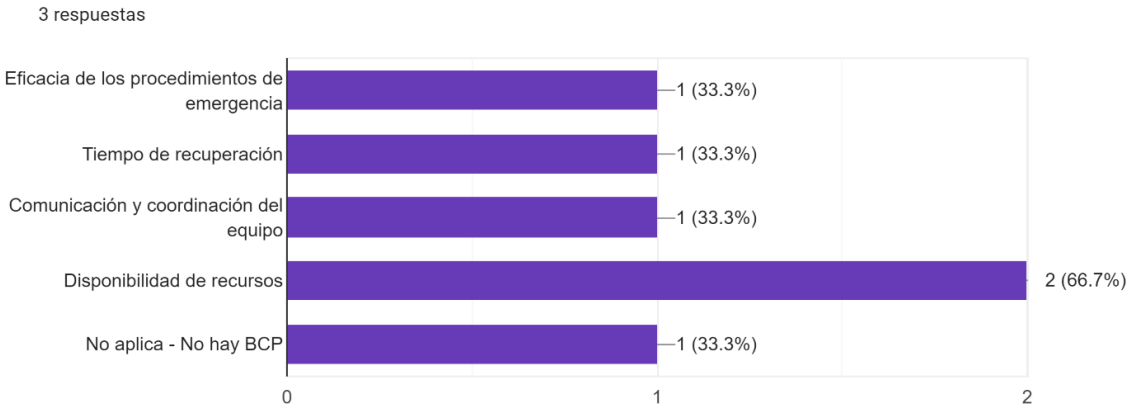
3 respuestas



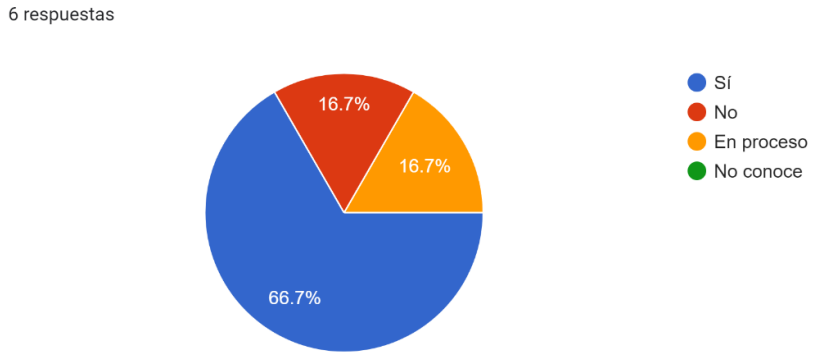
24. ¿La empresa tiene definido un objetivo de punto de recuperación (RPO) y un objetivo de tiempo de recuperación (RTO) para sus sistemas de información?



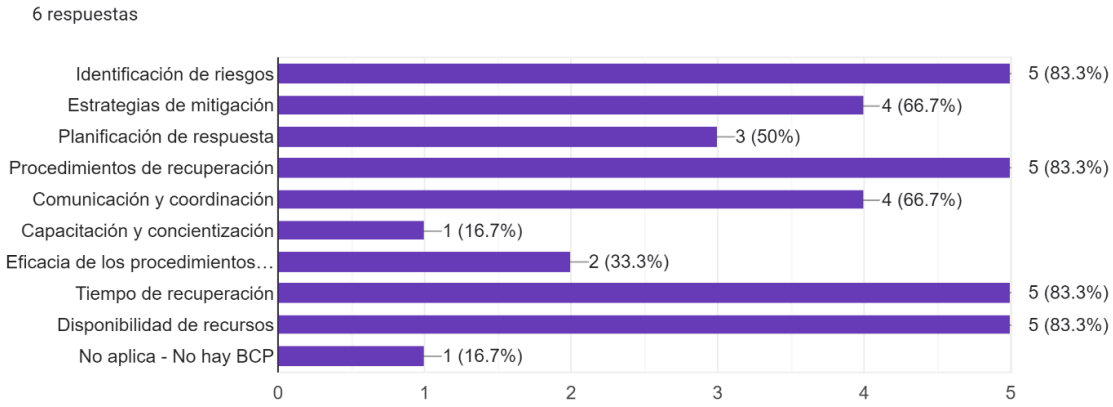
25. ¿Qué aspectos se evalúan durante las pruebas y simulacros del BCP? (Seleccione todas las que apliquen).



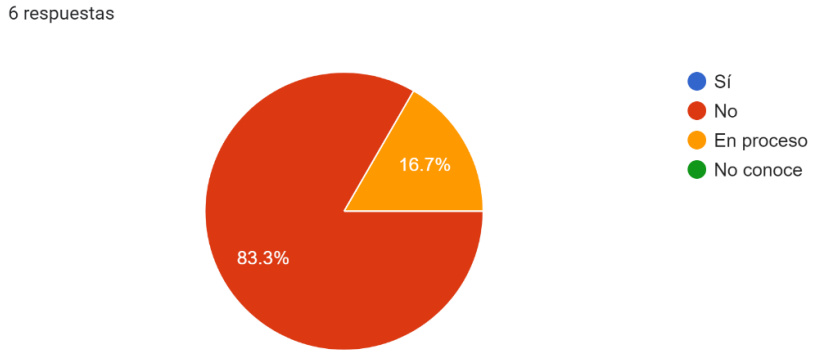
26. ¿La empresa tiene implementado un plan de contingencia?



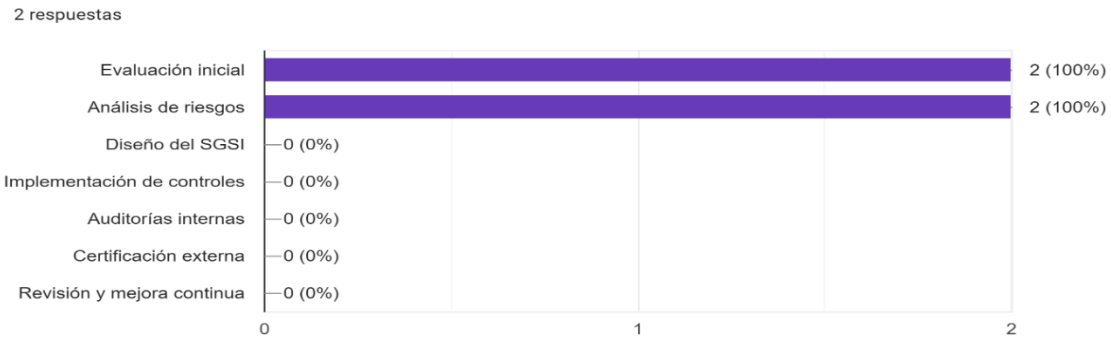
27. ¿Qué componentes y aspectos incluye y se evalúan en el plan de contingencia? (Seleccione todas las que apliquen).



28. ¿La empresa ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001?

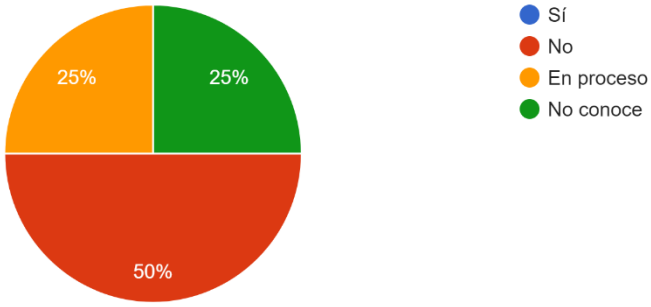


29. ¿Qué etapas de implementación de la ISO 27001 ha completado la empresa? (Seleccione todas las que apliquen, puede que haya completado alguna de ellas no necesariamente siguiendo la ISO 27001).



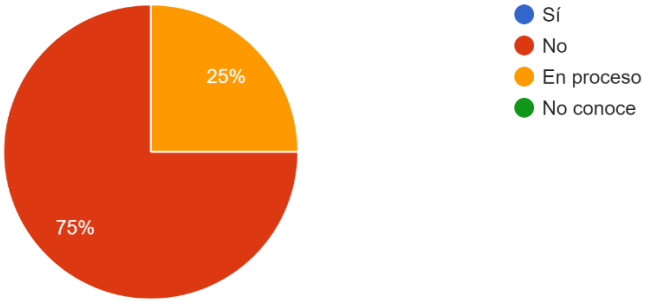
30. ¿La empresa ha realizado y revisa regularmente una evaluación de riesgos de seguridad de la información según los lineamientos de ISO 27001?

4 respuestas



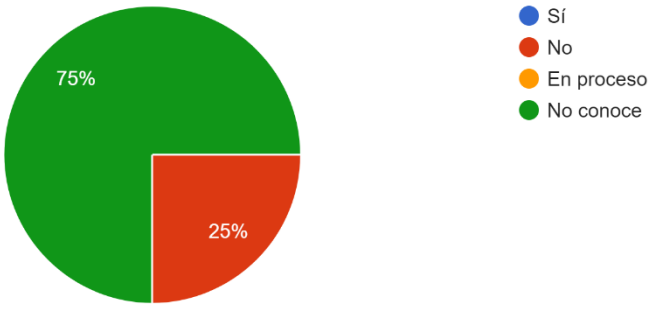
31. ¿La empresa cuenta con políticas y procedimientos documentados para la gestión de la seguridad de la información según ISO 27001?

4 respuestas



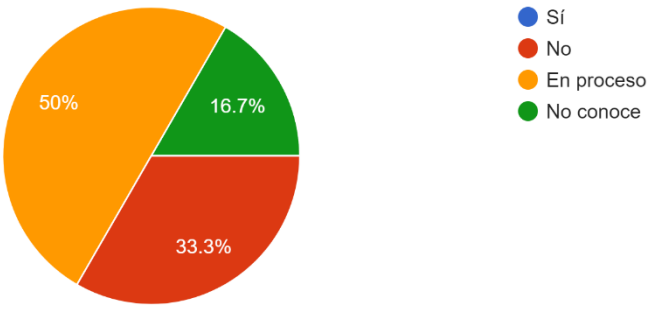
32. ¿La alta dirección está comprometida con la implementación y mantenimiento de un SGSI conforme a ISO 27001?

4 respuestas

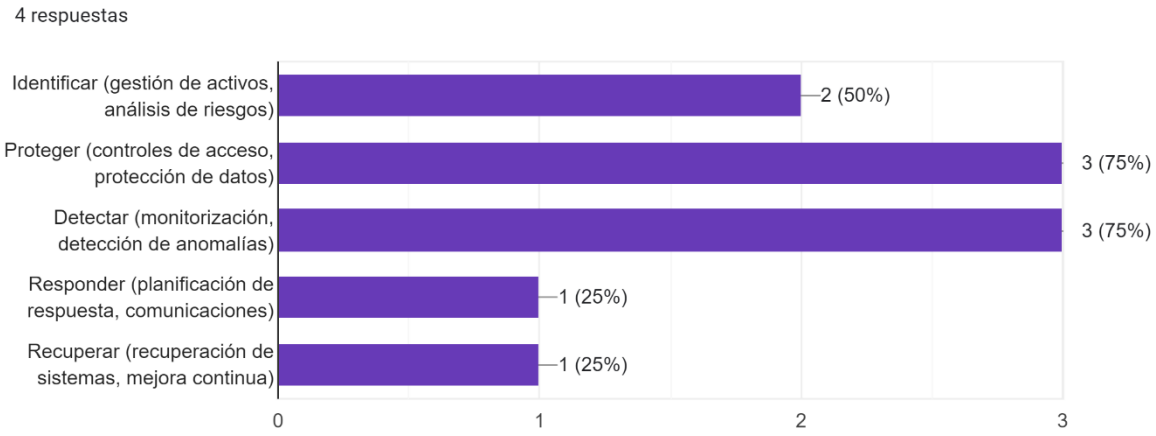


33. ¿La empresa utiliza el Marco de Ciberseguridad del NIST para gestionar sus riesgos de ciberseguridad?

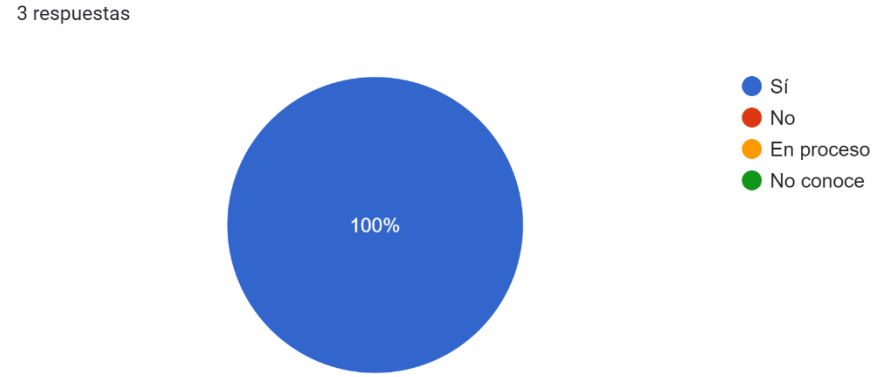
6 respuestas



34. ¿Qué componentes del NIST CSF ha implementado la empresa? (Seleccione todas las que apliquen).

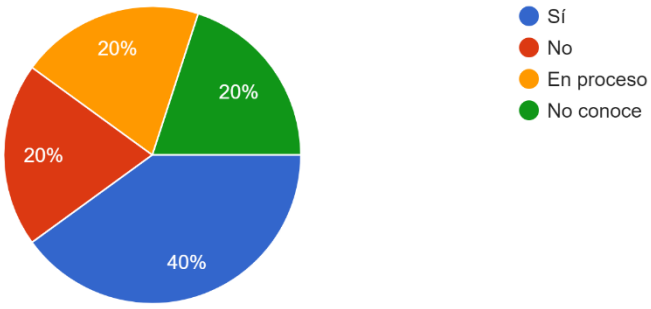


35. ¿La empresa ha implementado medidas de protección, como controles de acceso y protección de datos, conforme al NIST CSF?



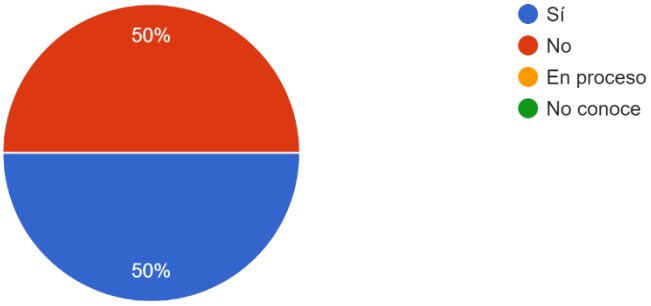
36. ¿La empresa cuenta con capacidades de detección de incidentes de ciberseguridad?

5 respuestas



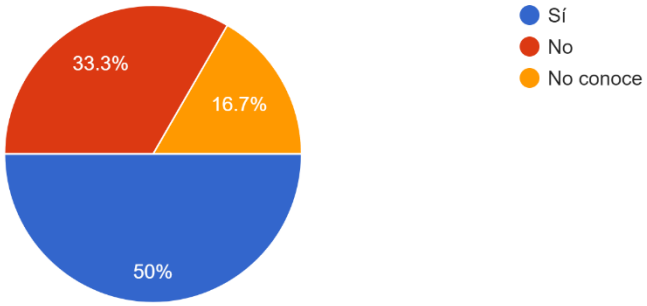
37. ¿La empresa tiene planes de respuesta y recuperación ante incidentes de ciberseguridad siguiendo el NIST CSF o diseñados por la misma?

4 respuestas



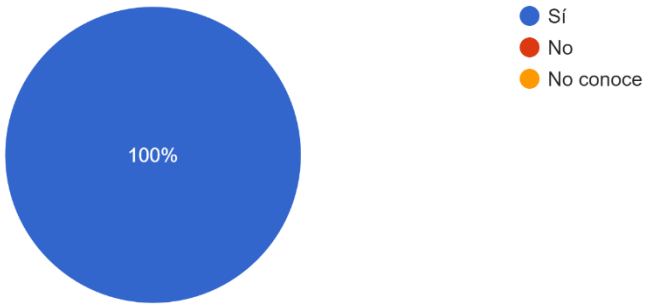
38. ¿La empresa sigue el Marco y Guía de Ciberseguridad de AGESIC? (Este marco establece los lineamientos y estrategias para la protección de la información en las entidades públicas y privadas).

6 respuestas



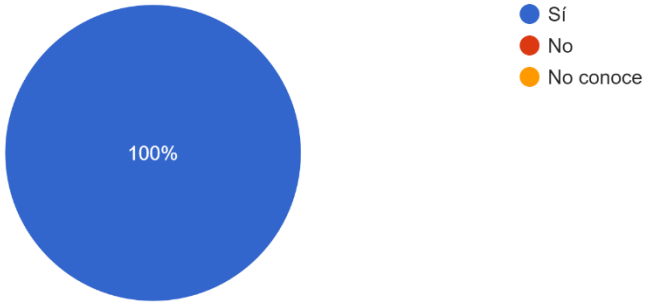
39. ¿La empresa cumple con la Ley N° 18331 de Protección de Datos Personales? (Esta ley regula la protección de datos personales y los derechos de las personas respecto a sus datos en Uruguay).

6 respuestas



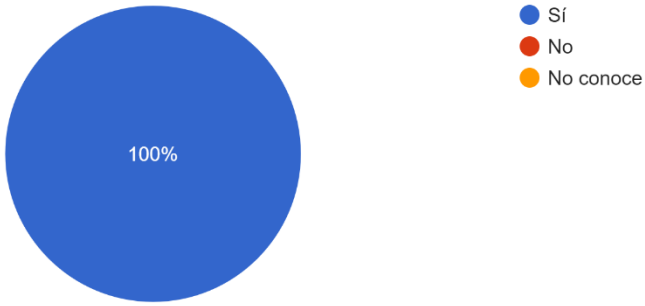
40. ¿La empresa cumple con el Decreto N° 396/003 sobre protección de datos personales? (Este decreto establece medidas específicas para la protección de datos personales en el país).

5 respuestas



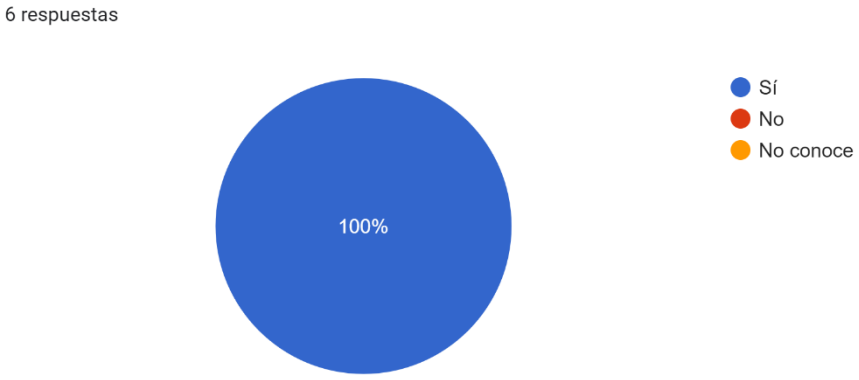
41. ¿La empresa cumple con el Decreto N° 451/009 sobre medidas de seguridad en el tratamiento de datos personales? (Este decreto establece las medidas de seguridad que deben adoptarse en el tratamiento de datos personales para garantizar su protección).

6 respuestas

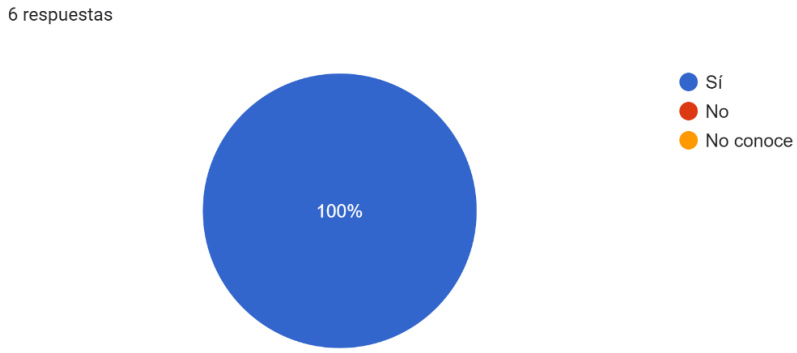


42. ¿La empresa cumple con el Decreto N° 452/009 sobre reglamentación de la ley de protección de datos personales? (Este decreto reglamenta diversos aspectos de la

Ley N° 18331, incluyendo las obligaciones de los responsables de tratamiento de datos).

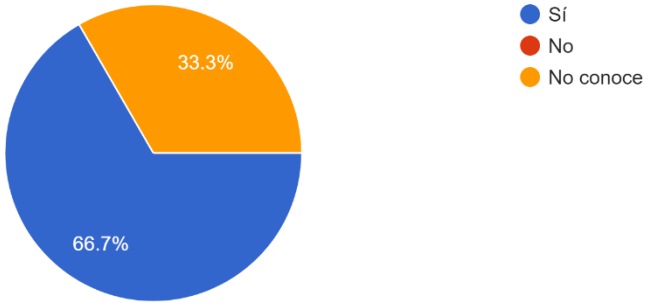


43. ¿La empresa cumple con el Decreto N° 414/009 sobre seguridad de la información? (Este decreto establece las directrices y normativas para la seguridad de la información en organizaciones públicas y privadas).



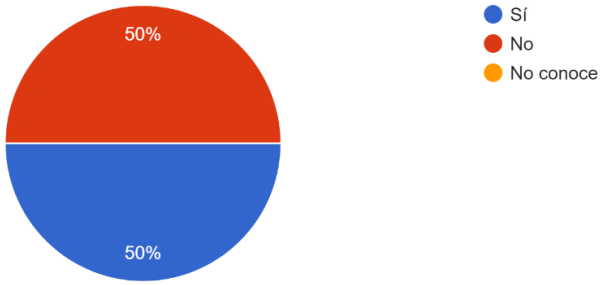
44. ¿La empresa cumple con el Decreto N° 242/017 sobre la regulación de la ciberseguridad en el sector público y privado? (Este decreto regula la ciberseguridad en ambos sectores, estableciendo las obligaciones y responsabilidades para proteger la infraestructura crítica).

6 respuestas



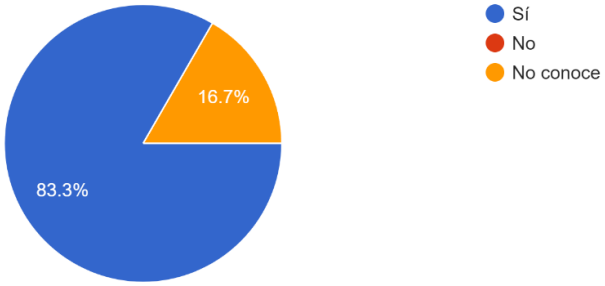
45. ¿La empresa cumple con el Decreto N° 122/019 sobre la creación de un comité de ciberseguridad? (Este decreto establece la creación de un comité de ciberseguridad para coordinar y supervisar las políticas y acciones en esta materia).

6 respuestas



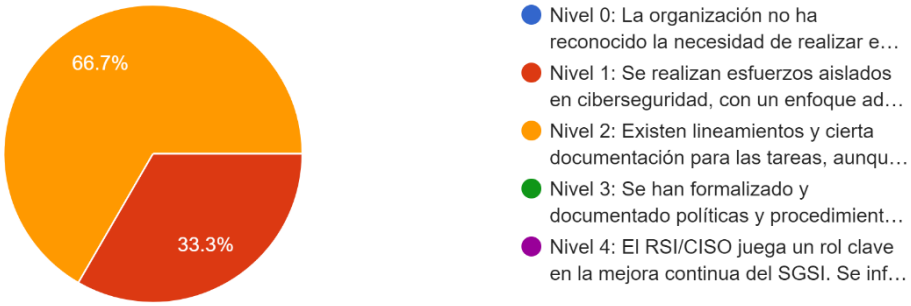
46. ¿La empresa cumple con el Decreto N° 64/020 sobre la implementación de medidas de ciberseguridad en el sector salud? (Este decreto establece medidas específicas de ciberseguridad para proteger la información y los sistemas en el sector salud).

6 respuestas



47. Si tuviera que categorizar la empresa en base a las preguntas anteriores, ¿en qué nivel de madurez entiende que se encuentra la misma?

6 respuestas



Volver

48. ¿La empresa tiene previsto en los próximos seis meses comenzar a implementar un marco, norma o algún cambio relevante en la forma que maneja su ciberseguridad?

6 respuestas