Universidad Siglo 21

Especialización en Cibercrimen

[A.01]

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN DEPENDENCIAS DE GOBIERNO

"Fortalecimiento de la seguridad de la información en los organismos gubernamentales, ante las nuevas técnicas de ciberataques"

Alumna: Giubbani, Cintia Anahí

DNI: 33.020.847

Año: 2024

ÍNDICE

Introducción:

El presente trabajo tiene como objetivo abordar el tema del fortalecimiento de la seguridad de la información en los organismos gubernamentales, frente a las nuevas técnicas de ciberataques. Para lograrlo, se llevará a cabo una investigación exhaustiva y se desarrollarán propuestas concretas para mejorar la protección de la información sensible en dichas instituciones.

En primer lugar, se presenta una justificación del problema, destacando la importancia de proteger la información en los organismos gubernamentales y los desafíos que plantean los ciberataques en la actualidad. A partir de esto, se plantea una hipótesis que sirve como base para el desarrollo del trabajo.

A continuación, se establecen los objetivos del proyecto, tanto el objetivo general como los objetivos específicos, que permiten orientar las acciones y metas a alcanzar. Estos objetivos se basan en la necesidad de fortalecer la seguridad de la información y garantizar la confidencialidad, integridad y disponibilidad de los datos en los organismos gubernamentales.

En el marco teórico, se realiza una revisión de la literatura existente, abordando los conceptos clave relacionados con la seguridad de la información y las técnicas de ciberataques.

En cuanto al marco metodológico, se definen los enfoques y las estrategias de investigación para llevar a cabo el proyecto. Se describen las técnicas de recopilación de datos, el análisis de información y las herramientas que se emplean para obtener resultados válidos y confiables.

El proyecto se organiza temporalmente mediante un plan de trabajo, que detalla las actividades previstas, su duración estimada, los responsables y las fechas de inicio y finalización.

Además, se identifican las condiciones institucionales necesarias para la implementación del proyecto, incluyendo posibles convenios con otras instituciones públicas, permisos para el uso de laboratorios, instrumentos, equipos o datos, entre otros aspectos relevantes.

Finalmente, se realiza una autoevaluación de la coherencia y viabilidad del proyecto, identificando posibles áreas de mejora y desafíos a enfrentar. Esta evaluación interna permite ajustar y fortalecer el enfoque del proyecto para obtener resultados óptimos.

Tema:

[A.01]- *"Políticas de seguridad de la información en dependencias de gobierno".*

Titulo:

"Fortalecimiento de la seguridad de la información en los organismos gubernamentales, ante las nuevas técnicas de ciberataques".

Justificación del problema

Identificación del Problema:

"Necesidad de revisar políticas existentes y plantear nuevas políticas de seguridad de la información ante las permanentes actualizaciones de técnicas de ciberataques."

Las dependencias del gobierno, al igual que todas las organizaciones, deben actualizar sus políticas de seguridad y plantear nuevas, ante la evolución constante de las diferentes técnicas de ciberataques.

La actualización permanente de los ciberdelincuentes, quienes utilizan técnicas cada vez más sofisticadas y se encuentran más preparados, genera la necesidad de la revisión y actualización constante de las políticas de seguridad de la información, cuyo objetivo es el de asegurar, que las mismas, sean efectivas y adecuadas para enfrentar las nuevas amenazas.

Fundamentación:

En la norma ISO/IEC 27001 (ISOTools Excellence,2023), se menciona a la seguridad de la información como "el conjunto de medidas y procedimientos puesto en marcha por las empresas u organismos, para proteger la confidencialidad de la información y la disponibilidad e integridad de los datos".

Dichos principios son denominados como la tríada CIA (Confidentiality – Integrity - Availability), y representa las bases de la seguridad de los datos.

Cuando ocurre un ciberataque, se considera un incidente de seguridad, y esto significa que al menos uno de los tres principios de la tríada CIA fue vulnerado.

Los ataques cibernéticos, en los últimos años, se han vuelto un riesgo permanente y son considerados como una amenaza constante para las dependencias gubernamentales, debido a que comprometen la seguridad de la información. A raíz de esto, las políticas de seguridad de la información deben estar en constante actualización para mejorar la seguridad y poder enfrentar las técnicas más actuales de ciberataque.

Cabe destacar que, al igual que otros países, las políticas de seguridad deben ser específicas para cada organismo, considerando sus necesidades y requisitos.

Las políticas de seguridad de la información son documentos que establecen las normas, directrices y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información que manipulan dichas dependencias. Deben incluir medidas para la protección de datos personales, a fin de evitar su filtración o el uso indebido de los mismos; definir procedimientos para el acceso a datos confidenciales, en cuyo caso, deben incluirse medidas que eviten la suplantación de identidad y acceso no autorizado, incluyendo la autenticación, la autorización y la auditoría de los accesos; políticas de clasificación de la información, donde se categoriza la misma, y se definen los niveles de seguridad para cada una de las categorías; gestión de contraseñas; gestión de dispositivos móviles; gestión de parches y actualizaciones de software; procedimientos para la realización backup y recuperación de la información y procedimientos ante incidentes de seguridad.

Se podría mencionar como las técnicas de ciberataques más comunes, que amenazan los sistemas y servidores de manera permanente, a las siguientes:

- Malware: software malicioso que se instala en los sistemas para dañarlos o robar información. Suele distribuirse a partir de correos electrónicos, páginas web infectadas, entre otros.
- Phishing: técnica de ingeniería social en la que envían correos electrónicos o mensajes de texto falsificados para engañar a los usuarios y obtener información confidencial, como contraseñas.
- Ransomware: tipo de malware que cifra los archivos de los sistemas y exige un rescate para desbloquearlos.
- Ataques de fuerza bruta: método que busca obtener acceso no autorizado a los sistemas mediante el uso de programas que intentan adivinar las contraseñas de forma repetitiva.

- Ataques de denegación de servicio (DDoS): ataques que tienen como objetivo inundar los sistemas con tráfico de red, sobrecargarlos y dejarlos inoperables.
- Ataques de inyección SQL: técnica utilizada para insertar código malicioso en las bases de datos de los sistemas y obtener información confidencial.
- Ataques de redirección de DNS: técnica que consiste en redirigir el tráfico de los usuarios a sitios web falsos para obtener información confidencial.

En las dependencias gubernamentales, no suele haber procedimientos para controlar la exposición de los sistemas y servidores de datos ante los ciberataques expuestos anteriormente; ante esto se podría mencionar:

- Escasa cultura de seguridad: en algunos casos, las organizaciones no cuentan con una cultura de seguridad que incentive la necesidad de mantener actualizadas las políticas de seguridad. Según un estudio de International Business Machines Corporation (IBM (2023)), el 95% de las brechas de seguridad son causadas por errores humanos.
- Las dependencias del gobierno, como así también muchas organizaciones, solo toman conciencia de la necesidad de actualizar sus políticas de seguridad después de haber sufrido una incidencia de ciberseguridad. Por ejemplo, según un artículo publicado en el sitio web de Todo Noticias (TN (2021)), en Argentina en el año 2020, se registraron 900 millones de intentos de ciberataques, donde más de la mitad (550 millones) ocurrieron en los últimos tres meses del año.
- Falta de recursos: es caso común que, en la mayoría de las dependencias, no cuentan con los recursos necesarios para mantener actualizadas sus políticas de seguridad de forma constante. Cabe destacar, lo mencionado en un artículo en el sitio web Rosario3 (2022), donde describe que: “La falta de inversión, sumada a la escasa capacitación del personal y la incapacidad de competir económicamente con los salarios ofrecidos por las empresas privadas ponen a los sistemas informáticos del estado en una posición de precariedad; y a la información de los ciudadanos en riesgo de vulneración constante”.
- Conocimiento técnico: no se cuenta con personal capacitado para implementar y mantener actualizadas las políticas de seguridad. En el mismo artículo de Rosario3 (2022), hace referencia que “el sueldo que propone el Estado está tan retrasado con respecto al de los privados válidos, que no tenés profesionales que quieran trabajar con vos. Entonces no tenés profesionales, no tenés sistemas, no tenés presupuesto”.

Es necesario que se implementen políticas de seguridad de la información sólidas y actualizadas de manera constante.

En el año 2022, sistemas y servidores del Poder Judicial de varias provincias fueron hackeados. Esto permitió vislumbrar deficiencias en los sistemas de seguridad de los datos y la necesidad de replantear y actualizar las políticas de seguridad; ambos temas fueron reflejados en diferentes artículos periodísticos como en el sitio web de Infobae (2023) y en el diario La Nación, este último escrito por el periodista Alconada Mon (2023).

Además, según una nota publicada en la revista digital Punto a Punto (2018), influye la falta de inversión en ciberseguridad: un 60% de empresas en Argentina sufrieron algún tipo de incidente relacionado con seguridad informática y de manera específica, el 32% padeció algún caso de malware, reveló el ESET Security Report 2017; una de las posibles causas, es la falta de inversión en ciberseguridad; la actualización constante en tecnologías y herramientas que permitan reducir el riesgo de ciberataques, es algo que los altos mandos de las empresas deben considerar a la hora de administrar el presupuesto de sus organismos.

Según la Oficina de Seguridad del Internauta (OSI - 2018), otra carencia, en cuestiones de seguridad, es la falta de capacitación del personal: Según un estudio realizado por la empresa de seguridad informática IBM, el 90% de los ataques cibernéticos tienen éxito debido a errores humanos. Con esto, podemos asumir que los empleados son el eslabón más débil de la cadena de seguridad. La falta de capacitados en seguridad de la información conlleva a cometer errores que ponen en riesgo la seguridad de la organización gubernamental. A sí mismo, se considera que el factor humano propicia o habilita los escenarios donde los criminales cibernéticos pueden actuar con consecuencias económicas e institucionales negativas. (Fuente: forbesargentina, (2023)).

Otros de los riesgos constante, es la exhibición de datos personales: En 2021, se descubrió el uso indebido de una clave otorgada al Registro Nacional de las Personas (Renaper) en Argentina, que expuso información personal de millones de ciudadanos. La falla se debió a la falta de actualización de políticas de seguridad (Fuente: Argentina.gob.ar, (2021).

Habiendo recabado toda esta información, podemos vislumbrar una necesidad urgente de que, las dependencias de gobierno, cuenten con un proceso de revisión y actualización permanente de las políticas de seguridad de la información, donde se realice una adecuada inversión en ciberseguridad, se evalúen, constantemente, los nuevos riesgos y amenazas, se identifican nuevas herramientas de seguridad, y se promueva una cultura de seguridad, a fin

de minimizar los riesgo de sufrir ciberataques y proteger los datos sensibles de los ciudadanos.

Formulación del problema

La revisión y actualización de las políticas de seguridad de la información, en los organismos estatales, es indispensable, debido a la constante evolución de las técnicas de ciberataques; lo que implica que las políticas y estrategias de seguridad deben ser revisadas y ajustadas constantemente para mantener su efectividad y asegurar adecuadamente la información. Es por ello que las entidades gubernamentales tienen la responsabilidad de proteger la información confidencial, lo que implica la implementación de políticas y estrategias de seguridad efectivas.

Los límites para el desarrollo del presente trabajo, dependen de la existencia de información actualizada e importante, acerca de las políticas de seguridad y las técnicas de ciberataques, como así también, de la disponibilidad de recolección y análisis de dicha información en el tiempo establecido.

El proyecto se basará en la revisión y análisis de políticas y técnicas de ciberataques. Para ello, se llevará a cabo una investigación exhaustiva y actualizada sobre las técnicas de ciberataques más recientes y las mejores prácticas en seguridad de la información. De esta manera, se podrá identificar los puntos débiles en las políticas de seguridad existentes y proponer soluciones específicas para abordar estas vulnerabilidades.

Se tomarán en consideración las últimas tendencias tecnológicas y su impacto en la seguridad de la información, como parte de la investigación para la actualización de las políticas de seguridad.

La investigación se enfocará en el análisis de casos concretos de ciberataques exitosos y la identificación de las debilidades en las políticas de seguridad, además de considerar las últimas tendencias tecnológicas en el análisis de la situación.

Una vez obtenida dicha información, se definirán las áreas de debilidad en las políticas existentes y se propondrán soluciones específicas para abordar estas vulnerabilidades. Es importante destacar que estas soluciones deben ser prácticas, efectivas y adaptadas a las necesidades específicas de cada organismo.

El problema a tratar es una cuestión crítica para la gestión de la información y la seguridad, y es necesario que se aborde de manera efectiva para garantizar la protección de la información confidencial, lo que significa que la solución propuesta tendría un alcance amplio y una proyección futura importante.

Este proyecto representa una oportunidad valiosa para adquirir nuevos conocimientos y experiencia en el ámbito de la seguridad de la información, los cuales podrían aplicarse de manera efectiva en mi contexto laboral. Además, el proceso de investigación y desarrollo de soluciones prácticas y efectivas es un desafío enriquecedor que puede ofrecer una experiencia gratificante.

Para respaldar lo planteado, se consultó diferentes fuentes de información especializada y autores prestigiosos en el campo de la seguridad de la información; uno de los autores más reconocidos es Bruce Schneier, quién está considerado internacionalmente como un experto de la seguridad informática. Ha publicado varios libros y artículos sobre el tema. En su libro "Secrets and Lies: Digital Security in a Networked World", Schneier destaca la importancia de la seguridad de la información y cómo los ciberataques pueden tener consecuencias graves para las empresas y organizaciones.

Otro autor importante en el campo de la seguridad de la información es Kevin Mitnick, quien es un consultor de seguridad informática, autor y conferenciante de Los Ángeles, California. Se le conoce sobre todo por su sonada detención y posterior encarcelamiento en 1995 por varios delitos informáticos y relacionados con las comunicaciones. Aparece a menudo hablando de ciberseguridad y temas relacionados con la piratería informática. Ha publicado varios libros, incluyendo "The Art of Deception" y "The Art of Intrusion", en los que destaca las técnicas utilizadas por los hackers para comprometer la seguridad de la información y cómo las empresas pueden protegerse contra ellas.

Al consultar estas fuentes de información, se pueden obtener argumentos y evidencias sólidas para respaldar la presente investigación y garantizar su calidad y relevancia.

Es importante considerar que, la elaboración de políticas de seguridad efectivas, es un proceso complejo que requiere la comprensión de los riesgos y amenazas a la información, la identificación de las áreas de debilidad, la definición de medidas de seguridad y la implementación de controles y monitoreo efectivos.

Hipótesis

La implementación de políticas de seguridad de la información actualizadas y eficaces, basadas en las mejores prácticas y tecnologías disponibles, contribuirá a prevenir y proteger contra ciberataques y garantizará la integridad, disponibilidad y confidencialidad de la información en los organismos estatales.

Objetivos

- **Objetivo General**

El objetivo general del presente trabajo consiste en **analizar y proponer políticas de seguridad de la información actualizadas y eficaces para prevenir y proteger, a los organismos estatales, contra ciberataques**, con el fin de garantizar la integridad, disponibilidad y confidencialidad de la información en las organizaciones.

- **Objetivos específicos**

Los objetivos específicos, que se describen a continuación, contribuyen de manera importante a la consecución del objetivo general:

1. **Realizar una revisión bibliográfica** de las políticas de seguridad de la información existentes, identificando sus fortalezas y debilidades.
2. **Analizar las técnicas de ciberataques más recientes y su impacto en la seguridad de la información**, para comprender los riesgos actuales a los que están expuestas las organizaciones.
3. **Identificar las mejores prácticas en seguridad de la información y las nuevas tecnologías** disponibles para la protección contra ciberataques, evaluando su viabilidad y pertinencia para las organizaciones.
4. **Proponer políticas de seguridad de la información actualizadas y eficaces** para prevenir y proteger contra ciberataques, basadas en las mejores prácticas identificadas y en las tecnologías disponibles.

5. **Desarrollar estrategias de concientización y capacitación para el personal** del organismo, a fin de mejorar su comprensión sobre la importancia de la seguridad de la información y su papel en la protección contra ciberataques.
6. **Realizar pruebas de vulnerabilidades** para evaluar la eficacia de las políticas propuestas y realizar los ajustes necesarios antes de su implementación.
7. **Evaluar la viabilidad de la implementación** de las políticas propuestas, considerando factores como los recursos necesarios, el costo y el tiempo requerido.
8. **Diseñar un plan de acción para la implementación de las políticas propuestas**, incluyendo los pasos necesarios para llevar a cabo su implementación y las responsabilidades correspondientes.

Marco Teórico

En este apartado, se desarrolla el marco conceptual que sustenta la solución propuesta para fortalecer la seguridad de la información en los organismos gubernamentales frente a las nuevas técnicas de ciberataques. Se exploran las teorías, conceptos y principios relevantes que respaldan la propuesta, brindando una base teórica sólida para su implementación. Además, se analizan las posibles limitaciones en el enfoque dado a la solución del problema, y se consideran las restricciones y desafíos potenciales que podrían surgir al implementar la propuesta.

Aunque existen investigaciones y artículos que tratan sobre la protección de la información crítica ante daños cibernéticos, en el contexto específico de los organismos gubernamentales en Argentina, se ha encontrado una falta de información sustancial. Además de mencionar algunos manuales o recomendaciones, no se han identificado investigaciones específicas que aborden este tema en detalle. Esto destaca la necesidad de investigaciones adicionales y enfoques específicos para fortalecer la seguridad de la información en los organismos gubernamentales de Argentina frente a las amenazas cibernéticas.

Asimismo, se proporciona una lista detallada de las principales fuentes de información utilizadas para respaldar y fundamentar el marco conceptual.

Marco conceptual:

1.1 Políticas de seguridad de la información: Las políticas deben establecer directrices claras para la protección de la información en los organismos gubernamentales. Se deben considerar aspectos como la clasificación de la información, el acceso y control de los datos, la gestión de riesgos, la respuesta a incidentes, la confidencialidad, integridad y disponibilidad de la información.

1.2 Mejores prácticas en seguridad de la información: Es esencial identificar y aplicar las mejores prácticas reconocidas internacionalmente en materia de seguridad de la información. Esto implica la implementación de controles de seguridad adecuados, como la autenticación de usuarios, el cifrado de datos, el monitoreo de sistemas, segmentación de redes, autenticación multifactor, educación y concientización de los empleados, gestión de parches y actualizaciones, entre otros.

1.3 Tecnologías de seguridad: Se requiere el uso de tecnologías específicas para fortalecer la seguridad de la información. Se deben evaluar soluciones como firewall, antivirus, detección de intrusiones y sistemas de gestión de identidad y acceso, entre otros.

1.4 Capacitación y concientización: Los empleados pueden ser víctimas de técnicas de ingeniería social, como el phishing, y comprometer la seguridad de la información sin intención. Es fundamental brindar capacitación continua al personal en temas de seguridad de la información. Se deben promover buenas prácticas de seguridad y fomentar una cultura de seguridad en la organización.

Limitaciones y respaldo argumental:

2.1 Resistencia al cambio: La implementación de nuevas políticas y prácticas de seguridad puede provocar resistencia por parte del personal. Según un estudio de D'Arcy et al (2014), los empleados pueden sentirse estresados por las demandas de seguridad de la información impuestas por la organización, como seguir procedimientos específicos, manejar contraseñas complejas y someterse a auditorías de seguridad. Este estrés puede afectar negativamente el cumplimiento de la política de seguridad, ya que los empleados podrían tomar atajos o ignorar medidas de seguridad para agilizar su trabajo. Para abordar este problema, las organizaciones deben reconocer el impacto del estrés en el cumplimiento de la política de seguridad y pueden implementar medidas como reducir la carga de trabajo percibida,

proporcionar capacitación adecuada y fomentar un entorno de apoyo. Una adecuada gestión del cambio y una comunicación efectiva son fundamentales para superar esta limitación.

2.2 Recursos limitados: Las restricciones de recursos financieros y técnicos son comunes en los organismos gubernamentales al implementar soluciones de seguridad. Es crucial realizar una evaluación objetiva de los recursos disponibles y explorar alternativas factibles. El informe "2015 Cost of Cyber Crime Study: Global" del Ponemon Institute y HP revela que el costo del cibercrimen sigue aumentando, con un incremento del 19% en el último año y una pérdida promedio global de más de 7,7 millones de euros. Aunque estas cifras son alarmantes, las organizaciones están adoptando medidas para defenderse mediante el uso de tecnología y mejores prácticas, lo que ha demostrado ser efectivo y generar un mayor retorno de inversión. Este informe brinda datos significativos sobre los costos del cibercrimen, lo que permite a las organizaciones comprender los desafíos económicos que enfrentan y tomar acciones para fortalecer su seguridad cibernética y minimizar las pérdidas.

2.3 Evolución constante de las amenazas: Las técnicas de ciberataques evolucionan rápidamente, lo que requiere soluciones flexibles y actualizadas. El seguimiento de las tendencias en ciberseguridad y la actualización continua de las medidas de seguridad son fundamentales.

Fuentes de información:

Las principales fuentes de información que respaldan el marco conceptual presentado abarcan:

- Literatura especializada en seguridad de la información: Libros, artículos científicos y periodísticos, y documentos técnicos relacionados con la seguridad de la información en organismos gubernamentales y en industrias. Dicha lectura, brinda conocimientos sobre los desafíos y soluciones en materia de seguridad de la información.
- Informes de ciberseguridad del gobierno: Estos informes proporcionan datos actualizados sobre las amenazas y tendencias en el ámbito de la ciberseguridad, revisando los informes y publicaciones del gobierno relacionados con la ciberseguridad y los ataques informáticos.

- Políticas y manuales de seguridad de la información del gobierno: Documentos oficiales emitidos por el gobierno, como el Manual de Seguridad de la Información de la Provincia de Buenos Aires, Gobierno de la Nación Argentina (2022), y la Política de Seguridad de la Información del INDEC (2020), lo que permite orientar, el presente trabajo, hacia políticas específicas para fortalecer la seguridad de la información en los organismos gubernamentales. Además, la Universidad Nacional de Córdoba ha elaborado su Manual de Políticas de Seguridad de la Información con el objetivo de cumplir con las leyes aplicables y asegurar una gestión eficiente de la seguridad de la información, los sistemas informáticos y el entorno tecnológico en la institución. Este manual sirve como un ejemplo destacado para el desarrollo de políticas de seguridad de la información en organismos gubernamentales, ya que proporciona directrices claras y prácticas adecuadas para abordar los desafíos en materia de seguridad. Al analizar este tipo de documentación, se pueden obtener pautas fundamentales sobre cómo enfrentar las amenazas y proteger la confidencialidad, integridad y disponibilidad de los datos en entornos gubernamentales.
- Estándares internacionales de seguridad de la información, como ISO 27001 (2005): "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos": uno de los estándares más reconocidos y utilizados en el campo de la seguridad de la información. Se centra en la protección de la confidencialidad, integridad y disponibilidad de la información, así como en la gestión de los riesgos relacionados con la seguridad de la información.

Al respaldarse en estas fuentes de información, el marco conceptual se nutre de conocimientos actualizados y basados en evidencia.

Marco Metodológico

Este proyecto de investigación de naturaleza cualitativa y descriptiva se enfoca en fortalecer las políticas de seguridad de la información. Se emplea el examen exhaustivo de documentos y la recopilación de información a través de entrevistas, cuestionarios o encuestas para obtener datos relevantes en este contexto. Los datos recolectados son analizados tanto cualitativa como cuantitativamente, permitiendo identificar pautas, tendencias y relaciones de importancia en el ámbito de la seguridad de la información. Además, se incluyen ejemplos

de casos como punto de referencia para validar los resultados obtenidos y fortalecer las conclusiones de la investigación. El objetivo primordial de este estudio es generar conocimiento y obtener una comprensión profunda de las problemáticas y fenómenos relacionados con la seguridad de la información. A partir de los hallazgos, se busca proporcionar recomendaciones efectivas que contribuyan a mejorar las políticas y prácticas de seguridad en este campo.

Recursos previstos para la resolución del problema planteado:

En el proceso de investigación, es fundamental contar con datos válidos y confiables que respalden las afirmaciones y conclusiones obtenidas. Para asegurar la validez de la hipótesis planteada, es necesario llevar adelante una serie de trabajos previstos que permitan disponer de los datos necesarios. Estas tareas previstas se refieren a las actividades planificadas y diseñadas, específicamente, para recolectar la información necesaria. A su vez, es importante establecer criterios claros para la selección de participantes o fuentes de información, así como garantizar la calidad y validez de los datos obtenidos.

Recursos planificados:

Exploración documental: Se realizará una exhaustiva búsqueda y revisión de la literatura académica y técnica relacionada con la seguridad de la información en organismos gubernamentales y las nuevas estrategias de ciberataques. Se emplearán recursos como libros, artículos científicos, informes gubernamentales y documentos técnicos.

Recopilación de datos: Se llevará a cabo la recolección de datos relevantes, a través de la aplicación de entrevistas, cuestionarios o encuestas dirigidas a profesionales especializados en seguridad de la información. Además, se analizarán políticas y documentos internos relacionados con la seguridad de la información.

Análisis de datos: Los datos recolectados serán sometidos a un análisis minucioso utilizando técnicas de análisis cualitativo y cuantitativo, según sea pertinente. Se buscarán patrones, tendencias y relaciones significativas entre los datos para respaldar la hipótesis planteada y obtener conclusiones sólidas.

Además, se considerarán recursos adicionales, como herramientas informáticas especializadas para el procesamiento de datos y software de análisis estadístico, con el fin de optimizar el análisis de los resultados obtenidos.

Posibles dificultades y cursos de acción alternativos:

La anticipación de posibles dificultades y la identificación de cursos de acción alternativos son aspectos cruciales en cualquier proyecto de investigación. Es importante estar preparado y contar con estrategias de contingencia que permitan superar obstáculos y asegurar el avance del trabajo.

En este contexto, es importante anticiparse a posibles dificultades que podrían surgir durante la ejecución del proyecto, las cuáles pueden estar relacionadas con la disponibilidad de recursos, limitaciones de tiempo, acceso restringido a información relevante, participación limitada de expertos u otros factores imprevistos.

En caso de enfrentar dificultades, se contemplarán posibles cursos de acción alternativos, como ampliar la muestra de participantes, modificar las técnicas de recolección de datos o utilizar fuentes de información complementarias.

Para la presentación, interpretación y discusión de los resultados obtenidos, se utilizarán recursos de representación visual, tales como gráficos, tablas y esquemas, con el propósito de ilustrar de manera clara y precisa los hallazgos obtenidos en la investigación. Estos recursos visuales permitirán una mejor comprensión de los datos y facilitarán su análisis por parte de los lectores.

Acceso limitado o restringido a información: En caso de enfrentar dificultades para acceder a ciertos documentos internos, se explorarán opciones alternativas. Las cuáles pueden incluir requerir información adicional a través de solicitudes formales, buscar fuentes de información complementarias como informes públicos o investigaciones previas, o establecer colaboraciones con otros investigadores que puedan proporcionar acceso a recursos adicionales.

Participación limitada de expertos: Si la participación de expertos en seguridad de la información es limitada, se buscarán colaboraciones con otros investigadores, que posean experiencias relevantes, participación en conferencias, seminarios o foros especializados, o

la exploración de comunidades en línea donde sea posible interactuar con profesionales en el campo.

Casos de estudio previstos como referencia para la validación de los resultados:

Para garantizar la solidez y la credibilidad de los resultados obtenidos en una investigación, es importante contar con una validación adecuada, ya que permite respaldar las conclusiones obtenidas y brindar una base sólida para la toma de decisiones. En este sentido, se hace necesario presentar casos de estudio como puntos de referencia que respalden y ejemplifican la aplicación práctica de los hallazgos alcanzados.

Al presentar los casos de estudio previstos, se establece una conexión directa entre los conceptos teóricos y su aplicación práctica en el contexto de la seguridad de la información.

A continuación, se presentan casos de estudio relevantes relacionados con la seguridad de la información, destacando la importancia de la protección de datos y la implementación de medidas de seguridad adecuadas. Los casos de estudio incluyen la filtración de información de la empresa Globant, el hackeo del sitio Argentina.gob.ar, la difusión online de datos personales del Registro Nacional de las Personas (Renaper) en Argentina y el hackeo efectuado a los sistemas del Poder Judicial de Chaco. El objetivo es utilizar estos casos como referencia para validar los resultados de esta investigación y respaldar las conclusiones obtenidas.

Un ejemplo relevante, de la importancia de la seguridad de la información, se observa en el caso de Globant, una de las firmas tecnológicas más valiosas a nivel mundial. Esta compañía, en el año 2022, se convirtió en víctima del grupo LAPSUS$, reconocido por filtrar información de grandes empresas como Microsoft, Samsung, Nvidia y Mercado Libre. En este caso, LAPSUS$ publicó alrededor de 70 GB de datos internos de Globant, incluyendo información confidencial y claves maestras de acceso a diversos servicios internos.

Entre los datos filtrados se encontraba aproximadamente 70 GB de código fuente, que contiene instrucciones esenciales para el desarrollo de aplicaciones. Además, se revelaron carpetas asociadas a clientes importantes de Globant, tanto públicos como privados, como DHL, Citibank, Banco Galicia, Disney y BNP Paribas. También se expuso un listado de usuarios y contraseñas utilizados en los servicios internos de la compañía, junto con herramientas de desarrollo de software muy utilizadas, como Confluence y Jira.

Es alarmante destacar que las contraseñas filtradas no cumplían con los estándares de seguridad recomendados, y muchas de ellas eran reutilizadas en distintos servicios, lo que viola las buenas prácticas de seguridad de la información.

Este caso ejemplifica de manera contundente la imperante necesidad de implementar medidas robustas de seguridad de la información en las organizaciones. La gestión adecuada de contraseñas, el cifrado eficiente de datos y la promoción de las mejores prácticas en materia de seguridad se vuelven fundamentales para salvaguardar la integridad y confidencialidad de la información sensible. En un entorno digital cada vez más propenso a brechas de seguridad, es vital que las empresas permanezcan en constante alerta y adopten un enfoque proactivo para mitigar los riesgos y proteger los datos de sus clientes y socios comerciales de posibles amenazas. La implementación de controles de seguridad sólidos y una cultura organizacional orientada a la seguridad se convierten en pilares fundamentales para prevenir incidentes de seguridad y mantener la confianza en el entorno digital.

Otro caso adicional, relevante en el ámbito de la seguridad informática, fue el hackeo del sitio oficial Argentina.gob.ar, que desempeña un papel fundamental en la gestión de trámites esenciales y la divulgación de información de interés público. Durante aproximadamente una hora, un mensaje de hackeo interrumpió la sección de noticias del sitio, lo que llevó a la intervención del CERT a nivel nacional, responsable de atender y responder a emergencias informáticas en el país.

Aunque se determinó que no hubo compromiso de información ni acceso al servidor, el incidente puso de manifiesto la existencia de alguna vulnerabilidad en la sección de carga de novedades del sitio, lo que permitió la inyección de un script de redirección. El equipo de Argentina.gob.ar y Arsat trabajaron conjuntamente para resolver la situación, modificando el código del script afectado. Además, el CERT mantuvo un monitoreo constante de las infraestructuras críticas del país como medida de precaución.

En este caso, se resalta la necesidad de implementar protocolos de seguridad informática en cada Ministerio, estableciendo la figura de un oficial en jefe de seguridad de la información (CISO) en cada jurisdicción. Este responsable se encargaría de proteger la información frente a posibles ataques cibernéticos y fugas de datos, asegurando así la integridad de la información sensible.

El incidente también pone de relieve la urgencia de establecer requisitos mínimos en materia de seguridad informática a nivel gubernamental, con el fin de prevenir y mitigar riesgos. La

colaboración entre organismos de seguridad informática y la implementación de mejores prácticas son fundamentales para salvaguardar la información y garantizar la confianza de los ciudadanos en los servicios digitales ofrecidos por el Estado.

El análisis de incidentes reales, como el hackeo a Argentina.gob.ar, permite desarrollar estrategias efectivas para prevenir y responder a futuros incidentes de seguridad.

Continuando con los casos de estudios, también podemos mencionar un caso relacionado con la difusión online de datos personales del Registro Nacional de las Personas (Renaper) en Argentina. El caso ocurrió en octubre de 2021 y generó preocupación en términos de seguridad de la información y protección de datos.

Su importancia radicó en la revelación de los accesos indebidos al sistema del Renaper, donde se almacenan los datos de 45 millones de argentinos. Aunque el organismo oficial, negó un robo masivo, confirmó la existencia de un acceso no autorizado. El Ministerio de Salud, entidad que consultó al Renaper, informó sobre dos accesos que permitieron la consulta de datos, incluyendo direcciones, teléfonos, fotos y números de trámite de DNI.

No es dato menor que, el Renaper, es utilizado por más de 150 instituciones públicas y privadas en Argentina, lo que destaca la importancia de asegurar la confidencialidad y protección de sus datos. Se sospecha que el acceso indebido fue realizado por alguien con permisos de acceso, quien obtuvo información de un grupo reducido de personas. Posteriormente, se publicaron 60.000 datos como prueba, y se amenazó con divulgar más información y vender acceso a la base de datos completa.

El caso del ataque informático al Poder Judicial de Chaco en 2022 se presenta como un relevante estudio de seguridad de la información. En este incidente, un grupo de hackers logró infiltrarse en los sistemas del Poder Judicial, tomando el control de la información y exigiendo un rescate para su devolución. Este ataque tuvo un impacto significativo, afectando la plataforma de gestión de expedientes y otros sistemas del Poder Judicial de la provincia.

Las autoridades judiciales de Chaco decidieron no negociar con los atacantes, rechazando el pago del rescate. Confiaron en el respaldo de un servicio de copias de seguridad (backup) realizado por una empresa externa, lo que les permitió recuperar la mayoría de la información afectada.

A partir de este incidente, se instó a los organismos judiciales de todo el país a fortalecer sus medidas de seguridad y a acelerar los procesos de respaldo de datos como medida de prevención frente a futuros ciberataques. La colaboración entre las diferentes jurisdicciones y la concienciación sobre los riesgos existentes son fundamentales para fortalecer la seguridad de la información en el ámbito gubernamental y preservar la confianza en el sistema judicial.

Este caso, junto a los mencionados anteriormente, ilustran la importancia de contar con medidas sólidas de seguridad de la información en los organismos gubernamentales. Además, destaca la necesidad de implementar estrategias de respaldo y recuperación de datos, como los servicios de copias de seguridad, para mitigar los efectos de los ataques cibernéticos. También resalta la importancia de establecer protocolos de comunicación y colaboración entre los organismos estatales, empresas privadas y las autoridades de ciberseguridad a nivel nacional.

Ejemplifican los riesgos y desafíos que enfrentan las organizaciones en términos de seguridad de la información. La filtración de datos de Globant, el hackeo del sitio Argentina.gob.ar, la difusión de información del Renaper, y el hackeo al Poder Judicial de Chaco, resaltan la importancia de implementar medidas sólidas de seguridad y protección de datos.

Se vislumbra la necesidad de adoptar una constante vigilancia en la protección de la información sensible. Es primordial que las organizaciones establezcan políticas y prácticas de seguridad robustas, que incluyan la gestión adecuada de contraseñas, el cifrado de datos, la detección temprana de vulnerabilidades y una cultura de seguridad arraigada en todos los niveles.

Además, los casos de estudio destacan de manera contundente la necesidad de fomentar la colaboración entre las instituciones públicas y privadas en la lucha contra las amenazas a la seguridad de la información. La implementación de regulaciones y estándares de seguridad informática a nivel gubernamental se vuelve imperativa para establecer un marco sólido de protección de datos.

Recursos de representación de resultados:

La presentación efectiva de los resultados de una investigación es fundamental para transmitir de manera clara y concisa los hallazgos obtenidos.

Para lograrlo, es primordial anticipar y planificar los recursos de representación adecuados. En este apartado, se detallarán los recursos visuales empleados, como gráficos, tablas y esquemas, que servirán para ilustrar, interpretar y debatir los resultados de manera accesible y comprensible. Estos recursos cumplen una función vital al proporcionar una comprensión más profunda de los datos, destacar patrones y tendencias, y respaldar las conclusiones alcanzadas.

A continuación, se describen los posibles gráficos, tablas y esquemas que se utilizarán:

a) Gráficos**:**

- Diagramas de barras: Permitirán comparar y visualizar datos cuantitativos de diferentes variables, mostrando las diferencias entre ellas de manera clara y efectiva.
- Gráficos de líneas: Ayudarán a representar tendencias y cambios en los datos a lo largo del tiempo, lo que facilita la identificación de patrones y comportamientos.
- Gráficos circulares: Se utilizarán para mostrar la distribución proporcional de un conjunto de datos, lo que permite visualizar la contribución relativa de cada categoría en un todo.

b) Tablas**:**

- Tablas comparativas: Se emplearán para mostrar los resultados obtenidos en diferentes casos de estudio, permitiendo comparar y contrastar los datos y las conclusiones extraídas.
- Resúmenes de datos: Se utilizarán tablas para presentar datos relevantes de forma concisa, como estadísticas clave, porcentajes o medidas de rendimiento.

c) Esquemas**:**

- Diagramas de flujo: Ayudarán a representar visualmente los procesos involucrados en la seguridad de la información, mostrando la secuencia de pasos, decisiones y acciones.

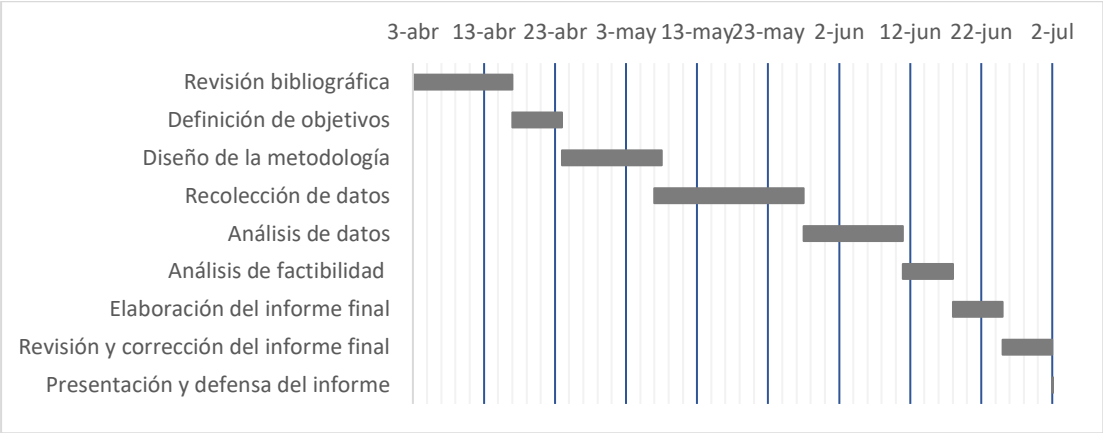
Los recursos visuales seleccionados se adaptarán a la naturaleza de los datos y los objetivos de comunicación de los resultados. Al utilizar estos recursos de representación visual, se logrará una presentación de los hallazgos de forma clara, concisa y efectiva, lo que facilitará la interpretación de los resultados y fomentará una discusión significativa.

Cronograma - Plan de Trabajo

Actividad	Duración estimada en días	Responsable	Fecha de inicio	Fecha de finalización	Descripción
Revisión bibliográfica	14	Alumno (Investigador)	3-abr	16-abr	Realizar una exhaustiva revisión bibliográfica para recopilar información relevante y actualizada acerca del tema de investigación.
Definición de objetivos	7	Alumno (Investigador)	17-abr	23-abr	Definir de manera precisa los objetivos específicos del trabajo final.
Diseño de la metodología	14	Alumno (Investigador)	24-abr	6-may	Seleccionar la metodología de investigación más adecuada para llevar a cabo el estudio.
Recolección de datos	21	Alumno (Investigador)	7-may	27-may	Recopilar los datos necesarios de manera rigurosa y sistemática para realizar un análisis exhaustivo y una evaluación adecuada del tema en cuestión.
Análisis de datos	14	Alumno (Investigador)	28-may	10-jun	Aplicar técnicas y herramientas estadísticas pertinentes para procesar y analizar de manera precisa los datos recopilados, con el

					fin de obtener resultados significativos y fundamentados.
Análisis de factibilidad	7	Alumno (Investigador)	11-jun	17-jun	Realizar una evaluación minuciosa de los resultados obtenidos, examinando su validez y relevancia en relación con los objetivos del estudio. Determinar la viabilidad y pertinencia de implementar las conclusiones y recomendaciones derivadas de la investigación.
Elaboración del informe final	7	Alumno (Investigador)	18-jun	24-jun	Redactar el informe final que incluya los hallazgos, conclusiones y recomendaciones basadas en el análisis realizado.
Revisión y corrección del informe final	7	Alumno (Investigador)	25-jun	1-jul	Realizar una revisión exhaustiva del informe final para garantizar su coherencia, precisión y claridad mediante la corrección de posibles errores o inconsistencias.
Presentación y defensa del informe	1	Alumno (Investigador)	2-jul	2-jul	Preparar y realizar la presentación del trabajo final ante el comité evaluador

Diagrama de Gantt



Para identificar el camino crítico, debemos examinar las dependencias entre las actividades y determinar cuáles deben completarse antes de que otras puedan comenzar, ya que tienen una dependencia directa y consecutiva.

En este proyecto, todas las actividades son críticas e importantes, en el sentido de que cualquier retraso, en cualquiera de ellas, afectaría directamente la finalización del proyecto en su totalidad.

Condiciones institucionales

Para implementar el fortalecimiento de la seguridad de la información en los organismos gubernamentales, se pueden requerir convenios con instituciones públicas que proporcionen los recursos necesarios para dicha implementación. A continuación, se detallan algunos elementos que podrían ser objeto de los convenios:

1. Estructura organizativa: La estructura organizativa de la institución es un aspecto relevante a considerar al redactar posibles convenios relacionados con la seguridad de la información. La distribución de responsabilidades y roles dentro de la organización puede influir en la forma en que se establecen los acuerdos y en las obligaciones de cada parte.
2. Políticas y procedimientos existentes: Al elaborar un convenio, es esencial tener en cuenta las políticas y procedimientos existentes en la institución, ya que estos servirán como base para establecer los requisitos de seguridad y las obligaciones de las partes involucradas.
3. Marco regulatorio y normativo: Las leyes, regulaciones y estándares aplicables a la institución en materia de seguridad de la información. Esto puede incluir leyes de

protección de datos, normas de cumplimiento específicas de la industria y estándares internacionales de seguridad de la información.

4. Acceso a laboratorios especializados: Para el desarrollo de pruebas, investigaciones y análisis de seguridad de la información. Es por ello que, será necesario establecer un convenio que defina los términos y condiciones para su uso. Dichos términos deben contemplar aspectos como los horarios de acceso, la disponibilidad de equipos necesarios, así como las responsabilidades compartidas en cuanto al mantenimiento y la seguridad de dichos laboratorios.

5. Uso de herramientas y software: Es posible que se requiera el uso de herramientas y software especializados para llevar a cabo análisis de vulnerabilidades, monitoreo de redes, detección de intrusiones, entre otros. Se requerirá establecer un convenio que precise los permisos de uso de dichas herramientas, así como los términos de licencia que apliquen. De esta manera, se asegurará el cumplimiento de los requisitos legales y de propiedad intelectual asociados a estas herramientas y software.

6. Intercambio de información y datos: Con el fin de garantizar la seguridad y confidencialidad de estos datos, el convenio correspondiente deberá definir claramente los tipos de datos que serán intercambiados, los protocolos de seguridad a seguir para su transferencia y almacenamiento, así como los acuerdos de confidencialidad y protección de la información. De esta manera, se asegurará el cumplimiento de las normativas vigentes y se establecerán los mecanismos adecuados para preservar la integridad y privacidad de los datos involucrados.

7. Capacitación y formación: Se requerirá brindar capacitación y formación en seguridad de la información a los empleados de los organismos gubernamentales. El convenio deberá especificar los contenidos de los cursos, los recursos necesarios para su implementación y los compromisos de ambas partes para facilitar la participación de los empleados en dichas actividades.

8. Colaboración en investigaciones y proyectos conjuntos: En el contexto del fortalecimiento de la seguridad de la información, resulta importante establecer colaboraciones en investigaciones y proyectos con otras instituciones públicas. Con el fin de establecer una base sólida para estas colaboraciones, el convenio correspondiente deberá definir de manera precisa los objetivos comunes, las responsabilidades asignadas

a cada institución, los recursos que serán compartidos, así como los derechos de propiedad intelectual asociados a los resultados obtenidos.

Anexo: Coherencia y viabilidad del proyecto

La autoevaluación de coherencia y viabilidad del proyecto ha sido fundamental para identificar áreas de mejora y desafíos que pueden surgir durante su implementación. Dicha evaluación debe ser considerada como un proceso continuo a lo largo del proyecto, ya que permitirá ir adaptándose a las circunstancias cambiantes y asegurar su éxito.

Se ha concluido que el enfoque del proyecto es coherente con el objetivo de fortalecer la seguridad de la información en los organismos gubernamentales frente a los ciberataques. No obstante, se han identificado oportunidades para mejorar la planificación de actividades, asignar responsabilidades de manera más eficiente y considerar de manera más detallada las condiciones institucionales y posibles desafíos.

- Mejora en la planificación de actividades: Sería oportuno examinar y perfeccionar el cronograma y los plazos asignados a cada actividad con el fin de asegurar una distribución adecuada del tiempo y los recursos disponibles.
- Asignación de responsabilidades: Resulta primordial definir roles y tareas específicas de forma más detallada, lo que permitirá favorecer una coordinación más efectiva entre las personas involucradas en el proyecto, evitando posibles confusiones y garantizando un avance fluido del proyecto.
- Desafíos de seguridad de la información: Dado que el objetivo principal es fortalecer la seguridad de la información, es importante reconocer y abordar los posibles desafíos relacionados con la protección de datos sensibles. Esto incluye la identificación de vulnerabilidades existentes, la adopción de medidas de seguridad adecuadas y la implementación de políticas y procedimientos sólidos.
- Consideración de condiciones institucionales: Es fundamental tener en cuenta las condiciones institucionales requeridas para llevar a cabo el proyecto, tales como los acuerdos con otras entidades gubernamentales, los permisos para acceder a laboratorios, herramientas, equipos o datos.

Referencias

- Alconada Mon, Hugo. (2023, 06 de Abril). Hackearon al Poder Judicial de Chaco y piden un rescate por la información. LA NACION. https://www.lanacion.com.ar/politica/hackearon-al-poder-judicial-de-chaco-y-piden-un-rescate-por-la-informacion-nid08022022/#:~:text=El%20ataque%20afect%C3%B3%20la%20plataforma,judicial%2D%20hasta%20el%20lunes%20pr%C3%B3ximo
- Argentina.gob.ar. (2021). El Renaper detectó el uso indebido de una clave otorgada a un organismo público y formalizó una denuncia penal. Recuperado de https://www.argentina.gob.ar/noticias/el-renaper-detecto-el-uso-indebido-de-una-clave-otorgada-un-organismo-publico-y-formalizo
- D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," Journal of Management Information Systems.
- Forbesargentina. (2023). El error humano: la puerta de entrada de los cibercriminales a los sistemas de las empresas. Recuperado de https://www.forbesargentina.com/columnistas/el-error-humano-puerta-entrada-cibercriminales-sistemas-empresas-n28820
- Gobierno de la Nación Argentina. (2022, 25 de Marzo). Elaboran modelo de política de seguridad de la información para organismos públicos. Recuperado de https://www.argentina.gob.ar/noticias/elaboran-modelo-de-politica-de-seguridad-de-la-informacion-para-organismos-publicos
- IBM. (2023). IBM Security X-Force Threat Intelligence Index 2023. https://www.ibm.com/downloads/cas/KGVA4AZW
- INDEC. (Año 2020). POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/340000-344999/344363/res181.pdf
- Infobae. (2023, 06 de Abril) Hackearon el sitio web del Poder Judicial de Córdoba. INFOBAE. https://www.infobae.com/sociedad/policiales/2022/08/14/hackearon-el-sitio-web-del-poder-judicial-de-cordoba/

- International Organization for Standardization (ISO/IEC 27001). 2005 “Information technology — Security techniques — Information security management systems – Requirements”.
- ISOTools Excellence. (2023, 06 de Abril). ISO 27001 ¿En qué se basa la política de seguridad de la información?. https://www.pmg-ssi.com/2018/12/iso-27001-en-que-se-basa-la-politica-de-seguridad-de-la-informacion/
- La Nación. 2020. “Confirman un ciberataque al sitio oficial Argentina.gob.ar el lunes”. Recuperado de https://www.lanacion.com.ar/tecnologia/confirman-cibertaque-al-sitio-oficial-argentinagobar-lunes-nid2505601/
- La Nación. 2021. “Sigue la preocupación por la difusión online de los datos de argentinos del Registro Nacional de las Personas”. Recuperado de https://www.lanacion.com.ar/tecnologia/sigue-la-preocupacion-por-la-difusion-online-de-los-datos-de-argentinos-del-registro-nacional-de-las-nid22102021/
- La Nación. 2022. “Globant es la nueva víctima del grupo LAPSUS$: filtraron 70 GB de datos y claves maestras de sus servicios”. Recuperado de https://www.lanacion.com.ar/tecnologia/globant-es-la-nueva-victima-del-grupo-lapsus-filtraron-70-gb-de-datos-y-claves-maestras-de-sus-nid30032022/
- La Nación. 2022. “Hackearon al Poder Judicial de Chaco y piden un rescate por la información”. Recuperado de https://www.lanacion.com.ar/politica/hackearon-al-poder-judicial-de-chaco-y-piden-un-rescate-por-la-informacion-nid08022022/
- OSI. (2018). ¿Sabías que el 95% de las incidencias en ciberseguridad se deben a errores humanos? Recuperado de https://www.osi.es/es/actualidad/blog/2018/12/05/sabias-que
- Ponemon Institute & HP. (2015). 2015 Cost of Cyber Crime Study: Global. Recuperado de https://www.slideshare.net/TheInternetofThings/2015-cost-of-data-breach-study-50952854
- Puntoapunto. (2018). Un 60% de empresas argentinas sufrió incidentes de seguridad informática. https://puntoapunto.com.ar/un-60-de-empresas-argentinas-sufrio-incidentes-de-seguridad-informatica/
- Rosario3. (2022). ¿Por qué la Argentina no está preparada para un ciberataque?

- https://www.rosario3.com/tecnologia/Por-que-la-Argentina-no-esta-preparada-para-un-ciberataque--20221104-0021.html

- TN. (2021). Registraron más de 900 millones de intentos de ciberataques en Argentina durante 2020. https://tn.com.ar/tecno/2021/02/25/registraron-mas-de-900-millones-de-intentos-de-ciberataques-en-argentina-durante-2020/

- Universidad Nacional de Córdoba. "Política de Seguridad de la Información para la Universidad Nacional de Córdoba". https://www.unc.edu.ar/sites/default/files/PoliticadeSeguridad08.pdf

Bibliografía

- Busaniche, Beatriz. (2021, 27 de Enero). Datos personales en riesgo: ¿el Estado está haciendo sus deberes?. INFOBAE. Recuperado de https://www.infobae.com/opinion/2021/01/27/datos-personales-en-riesgo-el-estado-esta-haciendo-sus-deberes/#:~:text=La%20administraci%C3%B3n%20p%C3%BAblica%20tiene%20m%C3%A1xima,es%20propiedad%20de%20cada%20ciudadano&text=La%20gesti%C3%B3n%20p%C3%BAblica%20demanda%20grandes%20vol%C3%BAmenes%20de%20informaci%C3%B3n.

- Gobierno de la Provincia de Buenos Aires. (sin fecha de publicación). Manual de Seguridad de la Información. Recuperado de https://buenosaires.gob.ar/jefedegobierno/sindicatura-general/manual-de-control-interno-y-auditoria-gubernamental-de-la-ciuda-2

- GORDON, HERNANDEZ, MALIK. (Año 2016). "Official (ISC)2 Guide to the CISSP CBK"

- IBM. (2021, 14 de Abril). Política y objetivos de seguridad. IBM. Recuperado de https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

- International Organization for Standardization (ISO/IEC 27001). 2005. Information technology — Security techniques — Information security management systems – Requirements.

- Tipton, H. F., & Krause, M. (Eds.). (2008). Information Security Management Handbook (Vol. 6th Edition). CRC Press.

- Schneier, B. (2000). Secrets and lies: Digital security in a networked world. Wiley.
- Schneier, B. (2002). The art of deception: Controlling the human element of security. Wiley.
- Schneier, B. (2005). The art of intrusion: The real stories behind the exploits of hackers, intruders and deceivers. Wiley.