Laboratorio 1. Plan de la búsqueda sistemática

# Título (Mapeo sistemático de literatura)

Revisión sistemática de literatura sobre robo y secuestro de información a través de un ataque cibernético.

# Fase 1. Planificación del estudio

# Problema de investigación

Un ciberataque es cualquier tipo de actividad hostil que utiliza numerosos medios para robar, manipular o destruir datos, o sistemas de información y se dirige a sistemas de información computacional, infraestructuras, redes o dispositivos informáticos personales. (A Systematic Literature Review on the Cyber Security, pag 11).

A cada minuto se realiza un ataque cibernético a nivel mundial a empresas de cualquier tamaño, de los cuales un porcentaje de ataques logra pasar las barreras de seguridad; y cuando esto ocurre, repercute en ellas en costos asociados a la recuperación y la restauración de los sistemas, pueden llegar a ser tan significativos que incluso podrían llevar a la quiebra a su víctima, debido al tiempo de inactividad, la pérdida de ingresos y el daño reputacional a largo plazo.

El ransomware es un malware especializado que se distribuye para extorsionar a los objetivos y es uno de los casos de ciberataques más frecuentes y conocidos, (A Systematic Literature Review on the Cyber Security, pag 13) es un tipo de software que cifra los datos en la computadora de la víctima y exige un pago antes de que los datos puedan ser liberados (A Systematic Literature Review on the Cyber Security, pag 31).

En este estudio se va a realizar la caracterización de los ataques cibernéticos, y dentro de estos nos centraremos en el robo de información como parte de los ataques, para determinar el impacto que puede tener en las organizaciones víctimas de este problema.

# Preguntas de investigación

**P1** ¿Cuáles son las consecuencias más comunes en un ataque cibernético?

**P2** ¿Cuáles son los riesgos más comunes a los que se ven expuestas las empresas después de sufrir un ataque cibernético?

**P3** ¿Qué medidas se están tomando para mitigar los riesgos por robo de información en un ataque cibernético?

# Selección de fuentes

* + 1. Bases de datos seleccionadas para la búsqueda
       1. Scopus
       2. Web of sciencies
    2. Cadenas de búsqueda utilizadas

Tabla 1. Cadenas y ecuaciones de búsqueda

|  |  |
| --- | --- |
| **Cadena** | **Cadena de búsqueda** |
| A | ransomware AND cybersecurity AND cyber-attack |

# Criterios de inclusión y exclusión de estudios

**CI1**. Se incluirán estudios de ataques cibernéticos en los últimos 5 años (2019-2024).

**CI2.**Se incluyen estudios sobre aquellas empresas que les han secuestrado su información.

**CI3.** Se incluyen estudios que su área de estudio esté relacionada con la tecnología (ingeniería, ciencias de la computación, economía)

**CI4.** Se incluyen estudios en ingles

**CE1**.Se excluyen los estudios repetidos en las bases de datos científicas.

**CE2**.Se excluyen estudios de ataques cibernéticos que no se relacionan con robo de información. (Criterio manual)

**CE3**.Se excluyen estudios que no sean de tipo article and conference paper

# Selección de Estudios

1. En la Tabla 2 se resumen los resultados de las cadenas de búsqueda en las bases de datos seleccionadas así:

Tabla 2. Cantidad de estudios capturados por cadena de búsqueda sin ningún filtro.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Cadena** | Web of Science | Scopus | ACM | IEEE | Science  Direct |
| A |  | 156 |  |  |  |

Se realizó una búsqueda por cada cadena aplicando cada uno de los siguientes filtros:

1. Filtro 1 con sólo la cadena de búsqueda con el filtro de: Articule title, Abstract, Keywords.
2. Filtro 2: publicaciones de hasta 5 años (2019-2024) .
3. Filtro 3: publicaciones en las áreas de ingeniería, ciencias de la computación, economía, econometría y finanzas.
4. Filtro 4: publicaciones que sean Article y Conference paper.
5. Filtro 5: publicaciones que estén en inglés.
6. Filtro 6: publicaciones con las palabras claves. (Falta aplicar este filtro)

Tabla 3**.** Cantidad de estudios capturados por cadena de búsqueda al aplicarlos filtros.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Cadena** | **Cadena de búsqueda** | **Filtro No 1** | **Filtro No 2** | **Filtro No 3** | **Filtro No 4** | **Filtro No 5** | **Filtro No 6** |
| A | ransomware AND cybersecurity AND cyber-attack | 156 | 150 | 134 | 121 | 121 |  |

**Fig. 2.** Gráfico de filtros aplicados

Diagrama

Descripción generada automáticamente

# Fase 2. Ejecución del estudio

Explique el proceso que se llevó a cabo para conseguir los estudios seleccionados. Este proceso puede ser explicado utilizando tablas, diagramas de flujo, esquemas, entre otros.

Utilice una tabla como la Tabla 4 para mostrar la cantidad de estudios capturados, filtrados y seleccionados de acuerdo con el plan del estudio realizado. Es decir, utilizando los criterios de inclusión y exclusión y posterior a los diferentes filtros ejecutados.

Tabla 4. Número de estudios según la base datos consultada

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Web of Science | Scopus | ACM | IEEE | Science  Direct |
| Estudios capturados |  | 156 |  |  |  |
| Estudios seleccionados |  | 121 |  |  |  |

También puede utilizar un esquema donde muestre tanto el proceso con la cantidad de estudios filtrados. Tenga en cuenta que debe quedar claro el proceso de selección realizado y la cantidad de estudios capturados y seleccionados.

**Tarea 1.** Se espera que en esta sección incluya una tabla como la Tabla 5 que relacione los estudios filtrados, que es la primera parte del Laboratorio 2. Esta tabla puede ser construida en Excel para su fácil gestión.

Tabla 5. Relación de estudios seleccionados.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nro** | **Titulo Artículo** | **Año** | **Autores** |
| 1 |  |  | En esta columna incluir la referencia del artículo para poder generar la bibliografía. |
| 2 |  |  | (Deterding et al., 2011) |
| 3 |  |  |  |

# Red bibliométrica

Utilizando las cadenas de búsqueda más refinadas y los estudios capturados en las bases de datos seleccionadas, se debe construir la red bibliométrica utilizando la herramienta VOSViewer para conseguir visualizaciones relevantes para el trabajo propuesto.

Dentro de las visualizaciones de la herramienta pueden incluirse la visualización de la red, la visualización de la superposición, y la densidad visualización. La función de zoom y desplazamiento que permite explorar un mapa con detalles completos, lo cual es esencial cuando se trabaja con mapas grandes que contienen miles de estudios.

Construya las diferentes visualizaciones y muéstrelas en esta sección utilizando el formato de figura.

Incluya en esta sección los gráficos relacionados con tendencias de años, campos de investigación, entre otros relevantes (según su criterio), para darle contexto a estos resultados preliminares generados en esta etapa de la RSL.

**Tarea 2.** En esta sección se deben incluir tanto los gráficos como el análisis conceptual de cada uno de los gráficos generados donde se evidencie el análisis crítico de los hallazgos más relevantes de las visualizaciones.

Referencias

Incluir las referencias de los artículos seleccionados en formato APA (Haciendo uso del gestor bibliográfico Mendeley).

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining gamification. *Proceedings of the 15th*. http://dl.acm.org/citation.cfm?id=2181040

Aspectos adicionales de interés para la presentación del laboratorio

* 1. Tablas

**Table 1.** Nombre de la tabla ubicado en la parte superior

|  |  |  |
| --- | --- | --- |
| Heading level | Example | Font size and style |
| Title (centered) | **Lecture Notes …** | 14 point, bold |
| 1st-level heading | **1 Introduction** | 12 point, bold |
| 2nd-level heading | **2.1 Printing Area** | 10 point, bold |
| 3rd-level heading | **Headings.** Text follows … | 10 point, bold |
| 4th-level heading | *Remark.* Text follows … | 10 point, italic |

* 1. Figuras

j0157763

**Fig. 1.** Nombre de la figura ubicado en la parte inferior