Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Propuesta de buenas prácticas de ciberseguridad para el uso de chatbots en el sector privado costarricense

Jiménez Otoya, Cristian Rodolfo

Ramírez Rodríguez, Óscar Andrés

Julio 2022

Declaratoria de derecho de autor

Se declara que el presente proyecto de investigación fue realizado por los autores Cristian Rodolfo Jiménez Otoya y Óscar Andrés Ramírez Rodríguez, tomando como fundamento los diversos capítulos del trabajo en diferentes fuentes bibliográficas, literatura citada, las cuales poseen su respectiva referencia, respetando los derechos de autor de dichos trabajos. De igual manera se utilizó como referencia los datos recopilados, a través de los cuestionarios creados y las entrevistas realizadas, en las cuales se reflejan los comentarios de los profesionales entrevistados.

Se autoriza la reproducción total o parcial de este trabajo, para ser usados como referencia de trabajos futuros de tipo académico y científico, en este caso, se solicita incorporar la referencia de este trabajo respetando los derechos de los autores.

Agradecimientos

Queremos agradecer a todas las personas que han colaborado de diferentes maneras en el desarrollo de esta investigación:

Muy especialmente, agradecemos a nuestro profesor tutor Luis Naranjo Zeledón, por su invaluable orientación y recomendaciones durante todo el proceso de investigación y desarrollo del trabajo final de graduación, las cuales fueron claves para la exitosa culminación de este.

A los señores Gerardo Chaves, y a la señora Ivonne Chaves, expertos en el área investigada por sus aportes, diferentes recomendaciones y su disposición de colaborar en el proceso de revisión y entrevistas que hicieron posible este trabajo.

Al personal de la Universidad Cenfotec por su ayuda y facilitarnos los recursos necesarios para el cumplimiento del proyecto de investigación.

Agradecemos asimismo a nuestras familias por su apoyo y comprensión durante toda la Maestría y por la motivación para culminarla de manera exitosa.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad**, requisito para optar por el título de grado de **Maestría**, para los estudiantes: **Jiménez Otoya Cristian Rodolfo y Ramírez Rodríguez Oscar Andrés**

LUIS CARLOS NARANJO ZELEDON (FIRMA)
Firmado digitalmente por LUIS CARLOS NARANJO ZELEDON (FIRMA)
Fecha: 2022.07.30 11:54:33 -06'00'

Dr. Luis Naranjo Zeledón
Tutor

Alonso Ramírez
Digitally signed by Alonso Ramírez
Date: 2022.07.30 13:36:12 -06'00'

M. Sc. Luis A. Ramírez Jiménez
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2022.08.06 17:43:38 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 30 de julio de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°.

Índice de Contenido

Índice de Figuras

Índice de Tablas

Abstract

En la actualidad, múltiples organizaciones se ven beneficiadas gracias a los avances en la tecnología a nivel mundial. Grandes cantidades de tareas repetitivas han sido reemplazadas por procesos automatizados que permiten incrementar la productividad y el enfoque en objetivos de negocio. Se utiliza la inteligencia artificial (IA) y sus implementaciones, como lo sería la utilización de “bots” conversacionales que interactúan con usuarios internos o externos con una calidad tal como la que lo haría un ser humano; estos se conocen típicamente como chatbots. Sin embargo, toda solución tecnológica presenta retos y consideraciones que deben de ser tomados en cuenta a nivel de ciberseguridad para garantizar que las organizaciones que aprovechan sus beneficios no se vean afectadas por un riesgo no considerado. Se describe entonces, la tecnología chatbot, sus retos, consideraciones a nivel de ciberseguridad, la opinión experta de diferentes actores en la utilización de la tecnología e información sobre el estado de su uso en el sector privado costarricense, para generar una propuesta de buenas prácticas de ciberseguridad que pueda ser aplicada en el mismo sector.

Palabras Clave: chatbots, asistente virtual, ciberseguridad, inteligencia artificial, seguridad, privacidad, recomendaciones, buenas prácticas, amenazas, vulnerabilidades.

Capítulo 1. Introducción

1.1 Generalidades

Este es un trabajo de investigación aplicado, es decir, se desarrolla una propuesta que pueda ser aplicada por cualquier institución del sector privado costarricense, a partir de un instrumento de evaluación que les permita a los investigadores conocer el estado actual de las buenas prácticas de seguridad y encontrar los puntos de mejora.

Se concentra en el sector privado costarricense debido a qué es el sector reconocido como mayoritariamente productivo en el país, por lo que enriquecerá más el proceso de conocimiento y descubrimiento del estado actual de la solución y de los controles asociados a la tecnología que también retroalimentarán la propuesta.

1.2 Antecedentes del problema

Las organizaciones del sector privado costarricense han adoptado diferentes usos de la tecnología de inteligencia artificial (IA) con el objetivo de simplificar diferentes procesos de cara a la atención interna y externa de la empresa, así como la posible automatización de diferentes procesos que previamente eran realizados por seres humanos. Por ejemplo, la posibilidad de extracción de información, realización de configuraciones o consultas hacia sistemas y potencial disminución de tareas repetitivas en búsqueda de retornos de tiempo o de inversión al corto plazo, entre otros.

Esta evolución en el uso de la tecnología ha brindado diferentes opciones de tecnologías de IA, entre ellas los chatbots, que representan una solución atractiva al satisfacer muchas de las necesidades o mejoras que se mencionaron anteriormente como razón de uso de tecnología artificial. Sin embargo, el uso de estas tecnologías

en la ciberseguridad representa muchas veces una superficie de ataque con amenazas, riesgos y vulnerabilidades fuera de consideración o contemplación; por lo tanto, es importante que se realice un análisis que permita evaluar si las medidas que se han tomado de cara al uso son realmente las correctas o entregan un nivel de seguridad aceptable, con lo cual se permita identificar puntos de mejora y cómo estos se pueden aplicar.

1.3 Definición y descripción del problema

En esta investigación se busca comprender las medidas de seguridad tomadas por el sector privado costarricense en el uso de tecnologías de chatbots, determinando posibles amenazas, vulnerabilidades y riesgos de seguridad que podrían enfrentarse en caso de que las medidas tomadas no sean satisfactorias, no se hayan incluido controles de seguridad alrededor de ellas o no cubran al menos una base de lo que se sugiere como buenas prácticas y recomendaciones relacionadas. Esto permitirá crear la propuesta con los resultados del análisis de riesgos cualitativo basado en la información recopilada con anterioridad.

1.4 Justificación

Como resultado de la investigación se buscará recomendar la empleabilidad de las mejores prácticas de seguridad para la utilización de tecnologías de chatbots en el sector privado costarricense y reducir de esta manera las posibles vulnerabilidades o riesgos que el sector pueda enfrentar al considerar el uso de este tipo de tecnologías. Se quiere crear una mayor consciencia en cuanto a la utilización de estas, en donde el usuario evite la exposición de datos confidenciales, pérdida de información sensible, vulneración de sistemas, en la solución que se está utilizando o bien la plataforma donde esta se encuentra instalada.

1.5 Viabilidad

1.5.1 Punto de Vista Técnico

Los investigadores que llevarán a cabo la realización de los objetivos que en este documento se encierran, se desempeñan en el sector privado y cuentan con vasta experiencia en temas de ciberseguridad. Adicionalmente, poseen experiencia en diferentes áreas, incluida la específica de la investigación. Esto permite que el conocimiento relacionado con las buenas prácticas y recomendaciones de la industria se puedan utilizar como referencia para otorgar la propuesta relacionada con la utilización segura de las tecnologías de inteligencia artificial.

1.5.2 Punto de vista operativo

Al tener en cuenta que el tiempo disponible para la realización de la investigación es amplio, ya que actualmente se cuenta con dos investigadores y que la mayoría de los individuos envueltos en el sector privado costarricense que formarán parte de la investigación se encuentran activamente haciendo uso de tecnologías de chatbots, se pretende analizar, en primer lugar, la situación actual, efectuar el diagnóstico de la utilización de herramientas o soluciones pertinentes, así como comprender y proponer los posibles puntos a considerar o de adopción de mejores prácticas que sean pertinentes, esto para garantizar la utilización segura de estas. Por lo tanto, se considera que el tiempo y los recursos disponibles son adecuados y manejables para la investigación planteada.

1.5.3 Punto de vista económico

Para el cálculo referencial de ellos, se utilizó como referencia el sitio Glassdoor, en donde un analista de ciberseguridad tiene un salario promedio de $82066 base al año al momento de la realización de este trabajo, lo que equivale a $6838.83 por mes. Para la investigación se estima un total de 4 meses de trabajo, lo

que equivaldría a un total de $27355.33 por investigador, para un costo total de $54710.66.

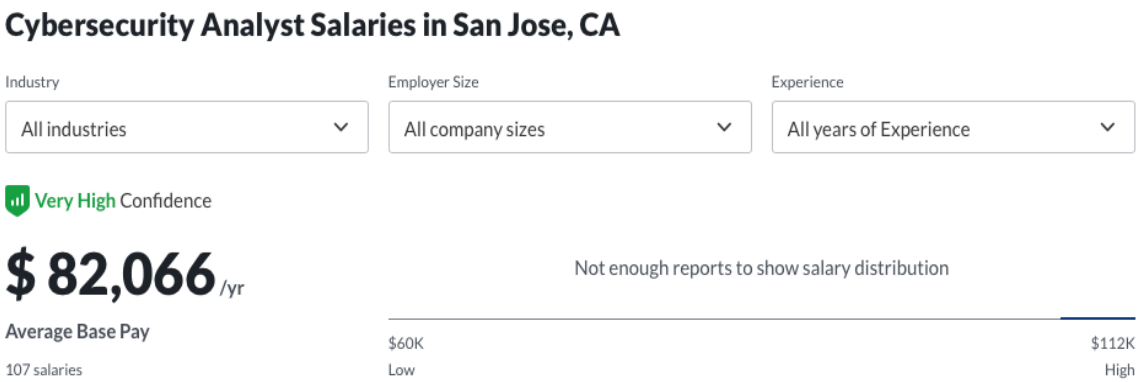

Figura 1: Salario analista de ciberseguridad.

Fuente: Glassdoor

1.6 Objetivos

Para la generación de este documento se ha utilizado la Taxonomía original de Benjamín Bloom del año 1956, debido a que se adapta a los requerimientos iniciales y posteriormente desarrollados alrededor de la investigación en cuestión, lo que permitió un desarrollo escalonado de la temática abordada.

1.6.1 Objetivo General

Proponer buenas prácticas de ciberseguridad mediante la elaboración de un análisis del uso de chatbots y sus riesgos para fomentar la utilización segura de esta tecnología en el sector privado costarricense.

1.6.2 Objetivos Específicos

1. Describir la tecnología de inteligencia artificial conversacional “chatbot”, definiendo sus elementos y su aplicabilidad en diferentes industrias para comprender su adopción y empleabilidad.

2. Explicar las posibles vulnerabilidades, riesgos y contramedidas de ciberseguridad asociados con los chatbots, informando sobre las posibles afectaciones y controles para poder identificar su superficie de ataque y disminuirla.
3. Efectuar una revisión de las prácticas empleadas en el uso y adopción mediante la aplicación de una entrevista a expertos en esta tecnología para obtener una base de recomendaciones a nivel técnico y de ciberseguridad.
4. Descubrir el estado de la implementación en producción y mecanismos de protección relacionados con los chatbots, mediante la aplicación de cuestionarios a empresas del sector para contrastar con respecto a las medidas sugeridas por los expertos y las que arrojará la investigación.

1.7 Alcances y limitaciones

1.7.1 Alcances

Se tomarán como referencia al menos cuatro instituciones del sector privado costarricense de diferentes verticales y tamaños que utilizan la tecnología chatbot para la realización de la investigación. Como resultado de la elaboración de la propuesta, se entrega un documento con la revisión del cumplimiento de cada uno de los objetivos propuestos, sujeto a la valoración de un panel de expertos del sector privado y de ciberseguridad, así como los resultados arrojados por el análisis de riesgo realizado.

1.7.2 Limitaciones

Dado que el objetivo de la investigación está relacionado con la entrega de una propuesta de buenas prácticas de ciberseguridad sobre la utilización de la tecnología de chatbot en el sector privado costarricense de forma segura, al

terminarlo no se realizará una implementación a nivel técnico, sin embargo, se analizarán en detalle los resultados obtenidos.

1.8 Marco de referencia organizacional y socioeconómico

La cuarta revolución industrial está profundamente relacionada con cambios que se han generado y se deben adoptar como consecuencia de los avances en tecnología, tales como robótica, inteligencia artificial, nanotecnología, entre otras. Estos cambios son disruptivos desde su concepción, producción y distribución por lo que las empresas deben de emplear nuevos modelos de homologación e integración con estas y las otras tecnologías que ya existen en sus ambientes.

Es especialmente interesante entender cómo las empresas hacen uso de estas tecnologías y toman ventaja de su valor. Existe un enfoque en la digitalización, la eliminación de tareas repetitivas, el aprovechamiento de los beneficios para poder simplificar y agilizar procesos que típicamente en la organización tienden a ser lentos, o como se mencionó previamente, repetitivos.

Precisamente la Revolución Industrial 4.0 es un nuevo enfoque para poder realizar los procesos productivos de una manera más organizada. Estos procesos serán realizados por sistemas ciber-físicos que llevan de la mano múltiples integraciones, así como automatizaciones que coordinan la elaboración de productos, tareas previamente pensadas, diseñadas y construidas con base en requerimientos y necesidades de negocio.

El nuevo enfoque permite llevar a cabo la coexistencia colaborativa a nivel de tarea entre humanos, sistemas o máquinas, lo que se conoce como “cobotización” y se puede ligar con los asistentes virtuales o chatbots. Estos toman tareas típicamente desarrolladas por humanos con una base de información y permiten brindar asistencia a través de diferentes canales en una interacción directa con un

humano que realiza las consultas o funge como cliente, o bien, la relación podría ser directamente con otro sistema integrado.

Costa Rica, como eje de la investigación, presenta las siguientes fortalezas y oportunidades consideradas estrategias de transformación digital hacia la Costa Rica del Bicentenario. Es particularmente interesante ver que se tienen muy buenas bases, como lo sería el nivel de alfabetización, además de considerar que los beneficios sociales se encuentran suficientemente desarrollados. Asimismo, en las empresas que en este caso son parte crucial de la investigación, se resalta el aspecto del crecimiento fuerte y sostenido desde el año 2010.

Indiscutiblemente, toda estrategia encierra oportunidades de mejora y, como tal, uno de los mayores retos que presenta el país es la disposición de tecnologías para la educación continua, así como la disponibilidad de canales digitales para la interacción entre el gobierno y otros actores.

	Fortalezas	Oportunidades
Ciudadanos	▪ Nivel adecuado de alfabetización ▪ Beneficios sociales bien desarrollados	▪ Disposición de tecnologías digitales para su educación continua ▪ Disponibilidad de canales digitales para interacción con el gobierno y otros actores
Empresas	▪ Crecimiento económico fuerte y sostenido desde 2010 ▪ Ampliación de exportaciones de productos y servicios en los últimos años	▪ Desarrollo de la industria 4.0 ▪ Mercado creciente para servicios digitales
Estado	▪ Voluntad política para la transformación digital ▪ Líder y referente en América Central	▪ Ventaja competitiva en la región ▪ Acceso a tecnologías que permiten mejorar la eficiencia del gobierno y la gobernanza
Tecnología	▪ Amplia penetración de telefonía móvil ▪ Precios de conectividad competitivos	▪ Desarrollo de 5G ▪ Disponibilidad de nuevas tecnologías, como inteligencia artificial, analítica de datos, grandes volúmenes de datos, para desarrollo de servicios innovadores.

Figura 2: Fortalezas y oportunidades de Costa Rica para el uso y adopción de servicios y productos digitales. Fuente: Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 - MICITT

Al considerar los puntos resaltados en la Figura 2, se identifican oportunidades que están entrelazadas indirecta o directamente y que, al lograr cumplir con una de ellas, como la disponibilidad de nuevas tecnologías, la inteligencia artificial, analítica de datos, etc., se podría al mismo tiempo ofrecer canales digitales adicionales para la interacción con el gobierno y otros actores.

De acuerdo con los índices de preparación de inteligencia artificial de los años 2020 y 2021, Costa Rica se ubica en la posición número 66 y 78 respectivamente, lo que evidencia una oportunidad de mejora en la adopción de tecnologías de IA. Para poder crear la tabla de posiciones, los reportes contemplan diferentes aspectos, entre ellos se consideran las capacidades y los aspectos habilitantes requeridos por los gobiernos para estar listos ante una implementación de inteligencia artificial (IA), pero no miden la implementación de esta. Al mismo tiempo, se mide el nivel de responsabilidad en el uso de este tipo de tecnologías, tomando como referencia parámetros de seguridad, confianza y transparencia (Oxford Insights, 2019 y 2020).

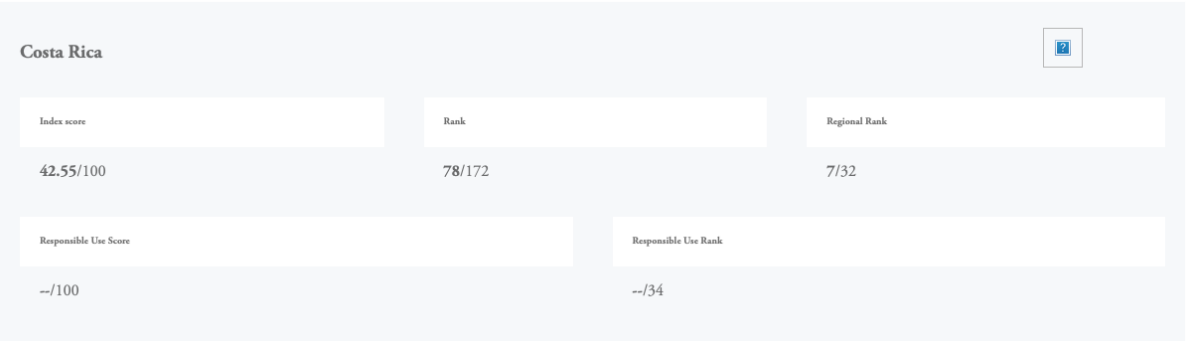

Figura 3: Ranking del Índice de preparación IA 2020, información y clasificación de Costa Rica. Fuente: Oxford Insights. https://www.oxfordinsights.com/government-ai-readiness-index-2020

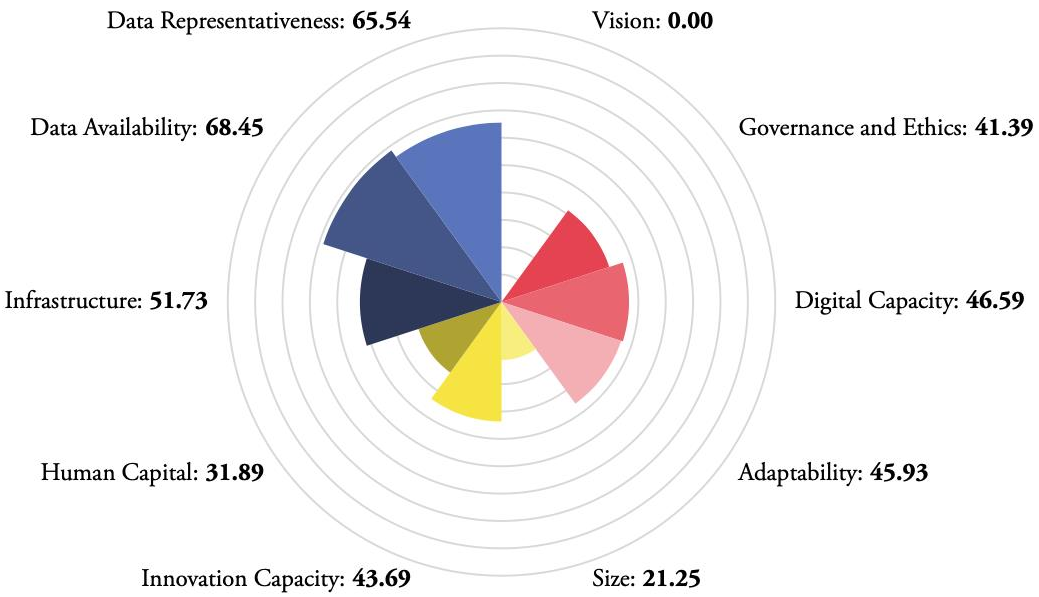

Figura 4: Ranking del Índice de preparación IA 2020, información y aspectos que fueron evaluados para otorgar la posición a Costa Rica. Fuente: Oxford Insights. https://www.oxfordinsights.com/government-ai-readiness-index-2020

Adicionalmente, el reporte del "Índice de Inteligencia Artificial" menciona en su información más destacada un incremento importante de un 34,5% de publicaciones relacionadas al área de la inteligencia artificial. Además, se recalca el acelerado progreso con el que ha avanzado el procesamiento del lenguaje natural (NLP, por sus siglas en inglés), lo que resulta en capacidades del lenguaje mejoradas significativamente para los sistemas de IA (Zhang et al., 2021).

Finalmente, se calcula que en Costa Rica el 86,69% de la mano de obra del país proviene del sector privado. En su mayoría, esto es clasificado como micro, pequeño, mediano o grande. Esto también contempla tanto empresas como trabajadores independientes (INEC, 2021).

Título
Total País
Cruce
de Sector Institucional
por Período
por Trimestre

Sector Institucional	Período	Trimestre			
Público		1er. Trimestre	2do. Trimestre	3er. Trimestre	4to. Trimestre
	2020	13,69	16,69	14,70	14,76
	2021	13,31	-	-	-
Privado		1er. Trimestre	2do. Trimestre	3er. Trimestre	4to. Trimestre
	2020	86,31	83,31	85,30	85,24
	2021	86,69	-	-	-

Figura 5: Indicadores de empleo por sector Institucional del país. Fuente: Sistema de Consultas INEC Costa Rica. https://www.inec.cr/sistema-de-consultas

1.9 Estado de la cuestión

1.9.1 Planificación de la revisión

Se hace una búsqueda de documentación con el objetivo de conocer el desarrollo académico que existe, las posibles áreas débiles que se puedan ampliar y así verificar que no se estén duplicando los estudios realizados en otras investigaciones.

1.9.1.1 Formulación de la pregunta

La formulación de la pregunta ayuda a delimitar los esfuerzos de búsqueda de información e investigación. El objetivo es encontrar respuestas que demuestren la contribución de este trabajo al campo de investigación y las relaciones entre ideas, teoría y aplicación práctica.

1.9.1.1.1 Foco de la pregunta

Se requiere para la presente investigación centralizar la búsqueda de documentos técnicos que especifiquen el uso de lineamientos y buenas prácticas de ciberseguridad en el marco del uso de tecnologías de inteligencia artificial de tipo conversacional, específicamente la llamada “chatbots” y ver la eficacia de los

controles que las empresas del sector privado costarricense han colocado alrededor de estas, para garantizar la protección de diferentes aspectos relacionados con la información.

1.9.1.1.2 Amplitud y calidad de la pregunta

Se establece en esta sección la pregunta de investigación que se desea responder de forma clara y concisa, basados en un problema a resolver. Se hace un listado de términos clave relevantes para la búsqueda de información y se consideran componentes clave como son la población específica, exposición y eventos de interés. Se definen medidas a utilizar para medir el efecto con base en la pregunta a responder y el diseño de los estudios.

1. **Problema**

Las tecnologías de inteligencia artificial de tipo chatbot han brindado a las organizaciones la posibilidad de realizar varios procesos de colaboración de forma óptima, simple, fluida, automatizada, integrada, entre otros beneficios. Como tal, esto ha permitido que diferentes sectores tomen ventaja de estas tecnologías, siendo el sector privado costarricense parte de estos y, por consecuencia, han logrado obtener múltiples ventajas, por ejemplo: aumento de su productividad en diferentes áreas, disminución del tiempo en la resolución de problemas, integración de sistemas, creación de asistentes virtuales, disminución de tareas repetitivas, por mencionar algunas.

Sin embargo, para el uso de estas, no se han tomado medidas de seguridad adecuadas debido al poco tiempo de existencia de estas tecnologías y a la falta de concientización en las organizaciones sobre modelos de protección, por lo tanto, la presente investigación se enfoca en los estudios que se han realizado en la aplicación de medidas de seguridad en el uso de tecnologías de chatbots.

2. Pregunta

Con la anterior definición del problema, se formula la siguiente pregunta de investigación:

¿Cuáles investigaciones se han llevado a cabo en el área de ciberseguridad para determinar las medidas de seguridad necesarias en el uso de tecnologías de inteligencia artificial de tipo chatbot?

3. Palabras clave y sinónimos

Se hace un listado de palabras clave que se van a utilizar para la búsqueda e identificación de documentos y trabajos relacionados con la investigación. Algunas de estas palabras están en el idioma inglés, ya que hay un grueso de publicaciones en ese idioma, estas se muestran en la Tabla 1.

Tabla 1: Listado de palabras.

Palabra	Equivalente en inglés
Inteligencia artificial	Artificial Intelligence
Ciberseguridad	Cyber security
Bots	Bots
Chatbots	Chatbots
Riesgo	Risk
Vulnerabilidades	Vulnerabilities
Buenas prácticas	Best practices

Fuente: Elaboración propia.

4. Intervención

Observar los resultados de cómo las organizaciones han adaptado sus medidas de seguridad en el uso de tecnologías de inteligencia artificial de tipo chatbot. Extraer los artículos y documentos de mayor relevancia para la investigación y analizar los resultados obtenidos.

5. Control

Al iniciar la investigación, no se cuenta con una colección de estudios realizados en el área. Se inicia con una búsqueda a partir de las palabras clave identificadas.

6. **Efectos**

Se espera tener documentación suficiente con las búsquedas realizadas para entender cuáles medidas de seguridad son necesarias en el uso de tecnologías de inteligencia artificial de tipo chatbot e identificar el impacto a nivel de ciberseguridad que han sufrido las organizaciones como consecuencia de la falta de medidas.

7. **Medida de salida**

Para la documentación encontrada se realiza una revisión de la calidad de esta en sitios web especializados para este propósito.

8. **Población**

La población de esta investigación serán los usuarios de tecnología de chatbots del sector privado costarricense.

9. **Aplicación**

Este tipo de investigación puede resultar de utilidad para aquellas personas que deban utilizar tecnología de chatbot de forma segura.

10. **Diseño experimental**

Durante el diseño experimental se hace un análisis y clasificación de los estudios obtenidos con base en la calidad del contenido y la relevancia para la investigación. Así, se busca garantizar suficiente documentación de confianza para la investigación, con la finalidad de evitar tener un rango amplio de estudios que puedan generar resultados no respaldados.

1.9.1.2 Selección de fuentes

Se especifican en esta sección las fuentes para la identificación de estudios primarios que se utilizarán para la investigación.

1.9.1.2.1 Definición del criterio de selección de fuentes

Se han tomado en cuenta para la selección de fuentes, en general, varios aspectos como la popularidad entre investigadores y el respaldo teórico con que cuenta la fuente De igual manera, se toma en consideración varios aspectos como la popularidad entre investigadores y el respaldo teórico con que cuenta la fuente. También se consideran fuentes que cuenten con gran variedad de documentación y con relevancia vigente.

1.9.1.2.2 Lenguaje de estudio

Con el objetivo de encontrar un mayor número de publicaciones relevantes, se ha definido el lenguaje de búsqueda tanto en español como en inglés.

1.9.1.2.3 Identificación de fuentes

En este apartado se describe la selección de fuentes para el desarrollo de la investigación.

1. Método de selección de fuentes:

El método de selección de fuentes se basa en el respaldo con el que cuenta la fuente en el área de tecnología con respecto a la publicación de estudios y documentos investigativos.

2. Cadena de búsqueda:

Las cadenas de búsqueda utilizadas para encontrar las publicaciones relevantes a la investigación tienen combinación de “AND”.

- intitle: "chatbots" + "security"
- intitle: "artificial intelligence" + "cybersecurity"
- intitle: "artificial intelligence" + “chatbots” + "cybersecurity"
- intitle: "artificial intelligence" + "chatbots" + "cybersecurity" + "vulnerabilities"

- intitle: "conversational artificial intelligence" + "chatbots" + "cybersecurity" + "vulnerabilities"

3. Lista de fuentes:

Google Scholar

1.9.1.2.4 Selección de fuentes después de la evaluación

Se tomarán en cuenta las fuentes que coincidan con los criterios de búsqueda.

1.9.1.2.5 Comprobación de las fuentes

Se buscan los sitios donde han sido publicadas las fuentes para determinar su validez.

1.9.1.3 Selección de los estudios

Una vez seleccionadas las fuentes, se definen los estudios que sean relevantes para la investigación.

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios

Se tomarán en cuenta los estudios que hayan coincidido con las búsquedas de las palabras clave cuando se encuentren dentro del área de investigación y con una publicación no mayor a 5 años de antigüedad.

1.9.1.3.2 Definición de tipos de estudios

Se evaluarán los estudios relacionados al área de investigación cuyo enfoque esté dirigido al tema de ciberseguridad.

1.9.1.3.3 Procedimiento para la selección de los estudios

1. Utilizar la opción de búsqueda avanzada o búsqueda general disponible en las fuentes seleccionadas.
2. Aplicar las cadenas de búsqueda definidas utilizando las palabras clave.
3. Filtrar el rango de fechas para considerar únicamente estudios publicados dentro de los últimos 5 años.

4. Evaluar los resultados obtenidos y aplicar los criterios de selección con base en el Abstract y palabras clave del artículo.
5. Extraer y documentar la información relevante para la investigación.

1.9.2 Ejecución de la revisión

En la Tabla 2 se muestra la información recolectada a partir de los criterios de búsqueda definidos en la sección anterior.

Tabla 2: Índice de estudios recolectados.

#	Título del artículo	Autores	Año	Palabras clave	Enlace
1	Interrogating Virtual Agents: In Quest of Security Vulnerabilities	Josip Bozic Franz Wotawa	2020	chatbot, vulnerability, Cross-Site Scripting (XSS), security, privacy	https://link.springer.com/chapter/10.1007/978-3-030-64881-7_2
2	Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation	Alex S Wilner	2018	Cybersecurity, Internet of Things, Artificial Intelligence, Misinformation	https://journals.sagepub.com/doi/abs/10.1177/0020702018782496
3	Artificial Intelligence and Personal Data: International and National Framework	Aliyev, A. Ibrahim, Rzayeva G. Aydin, & Ibrahimova A. Nazim	2021	Artificial Intelligence, data, human, Human Rights, privacy, robot	http://phrg.padovauniversitypress.it/2021/1/4
4	Artificial Intelligence In Emerging Markets - Opportunities, Trends, and Emerging Business Models	Tonci Bakovic, Margarete Biallas, Alejandro Caballero, Maria Lopez Conde, Peter Cook, Prajakta Diwan, George Vivien	2021	Artificial Intelligence, opportunities, trends, innovation	https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/artificial+intelligence+in+emerging+markets

#	Título del artículo	Autores	Año	Palabras clave	Enlace
		Houngbonon, Hassan Kaleem, Baloko Makala, Sumit Manchanda, Rebecca Menes, Peter Mockel, Xiaomin Mou, Monique Mrazek, Gordon Myers, Kiril Nejkov, Marina Niforos, Felicity O'Neill, Ahmed Nauraiz Rana, Friedemann Roy, Ommid Saberi, Sabine Schlorke, Maud Schmitt, William Sonneborn, Davide Strusani, Ian Twinn			
5	Attacking Artificial Intelligence - AI's Security Vulnerability and What Policymakers Can Do About It	Marcus Comiter	2019	Artificial Intelligence, vulnerabilities, cybersecurity, security	https://www.belfercenter.org/publication/AttackingAI
6	Artificial Intelligence Index Report 2021	Daniel Zhang, Saurabh Mishra, Erik Brynjolfsson, John Etchemendy, Deep Ganguli,	2021	Artificial intelligent, report, data, global	https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf

#	Título del artículo	Autores	Año	Palabras clave	Enlace
		Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Niebles, Michael Sellitto, Yoav Shoham, Jack Clark, Raymond Perrault			
7	Development and Refinement of a chatbot for Cybersecurity Support	Bulin Shaqiri	2021	Chatbot, Cybersecurity	https://files.ifi.uzh.ch/CSG/staff/franco/extern/theses/BA-B-Shaqiri.pdf

Fuente: Elaboración propia

1.9.2.1 Evaluación de la calidad de los estudios

Se presume la calidad de los artículos mencionados a partir de la cantidad de filtros utilizados, así como del criterio experto del tutor.

- Artículo #1: *Interrogating Virtual Agents: In Quest of Security Vulnerabilities*

  Conferencia: *IFIP International Conference on Testing Software and Systems (ICTS) 2020*.

Para este primer artículo logramos observar que es en relación con una conferencia en su edición número 32, por lo que representa una conferencia establecida. Donde investigadores, desarrolladores, *testers* y usuarios se reúnen con el fin de presentar y discutir las innovaciones, experiencias y desafíos recientes en el tema de pruebas de software y sistemas y la medición de la calidad del software.

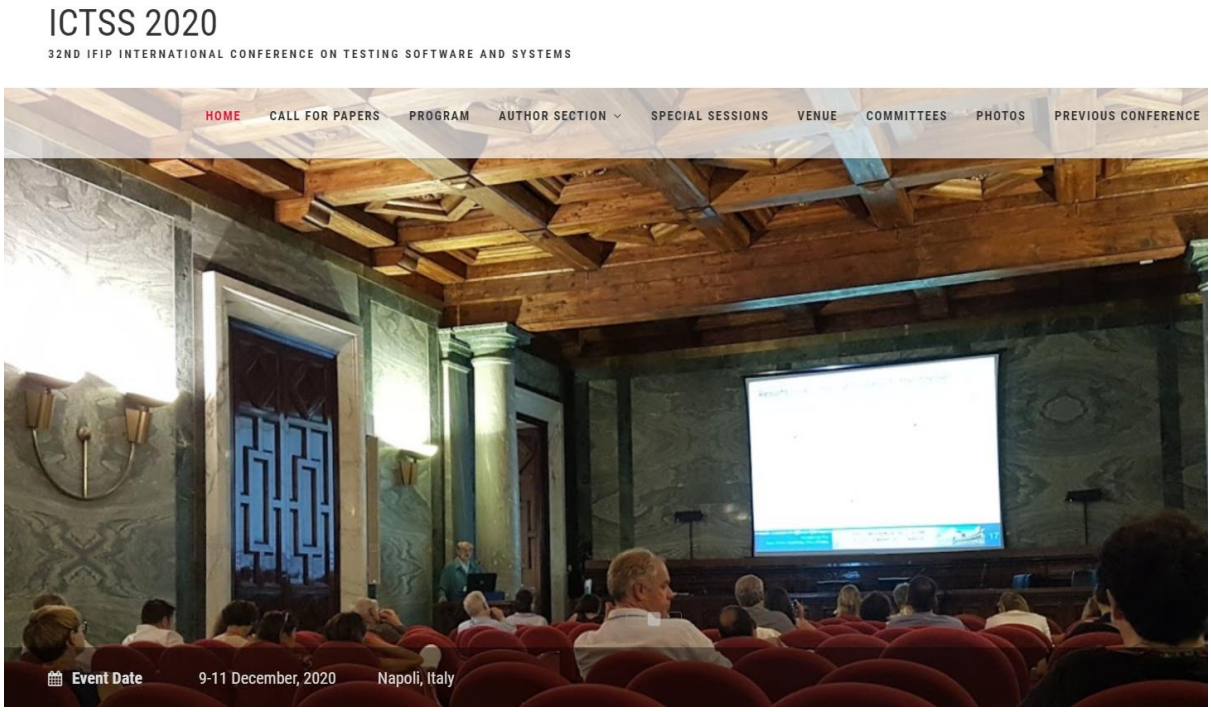

Figura 6: Página web IFIP - ICTS 2020. Fuente: http://home.ing.unisannio.it/ictss2020/

- Artículo 3: *Artificial Intelligence and Personal Data: International and National Framework*

  Universidad: Universidad Padova Italia

Según el *QS World University Rankings* 2022, la Università di Padova (Universidad de Padova, Italia), se encuentra de número 242 de 1300 universidades a nivel mundial. Por lo que se considera una fuente confiable.

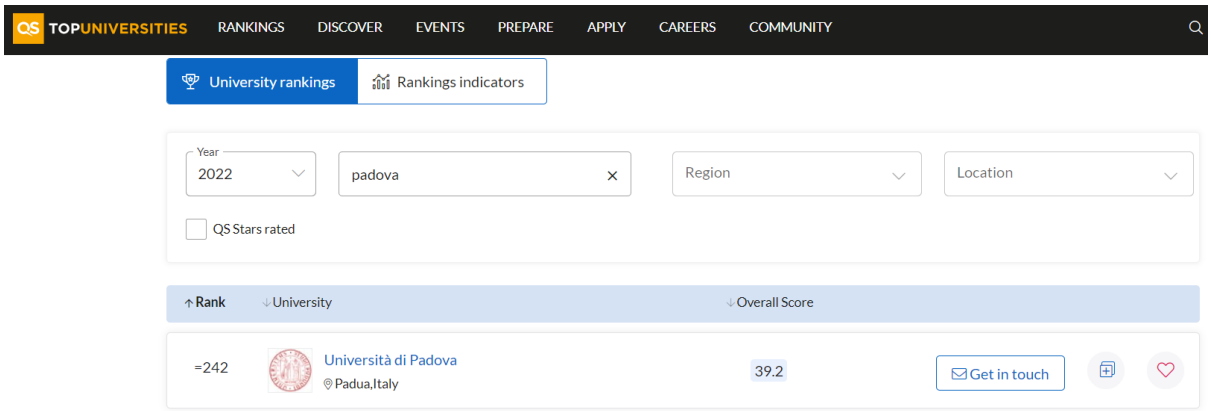

Figura 7: Ranking Università di Padova. Fuente: https://www.topuniversities.com/university-rankings/world-university-rankings/2022

Adicionalmente, para los siguientes artículos se presume de igual manera la calidad de estos, debido al criterio experto del tutor, el cual nos facilitó una lista de artículos en el área de Inteligencia Artificial, de los cuales seleccionamos e incluimos los que son relevantes al tema especificado de chatbots.

- Artículo 4: *Artificial Intelligence In Emerging Markets - Opportunities, Trends, and Emerging Business Models*

  Journal: International Finance Corporation (IFC) Publications

  Se considera de valor incluir esta revisión, al ser un reporte publicado por parte del International Finance Corporation (IFC), ya que esta es la mayor institución de desarrollo mundial centrada en el sector privado en los países en desarrollo; siendo a su vez, parte del World Bank Group.

- Artículo 5: Attacking Artificial Intelligence - AI's Security Vulnerability and What Policymakers Can Do About It

Universidad: Harvard Kennedy School

Según el QS World University Rankings 2022, esta universidad se encuentra en la posición #5, por lo que fundamenta la confiabilidad de la fuente.

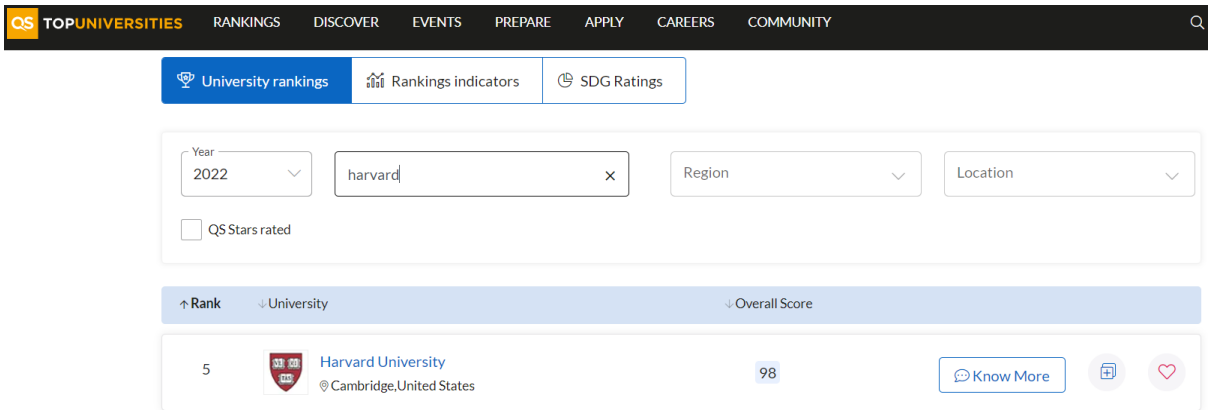

Figura 8: Ranking Harvard Kennedy School. Fuente: https://www.topuniversities.com/university-rankings/world-university-rankings/2022

- Artículo 6: Artificial Intelligence Index Report 2021

Universidad: Stanford University

Según el QS World University Rankings 2022, esta universidad se encuentra en la posición #3.

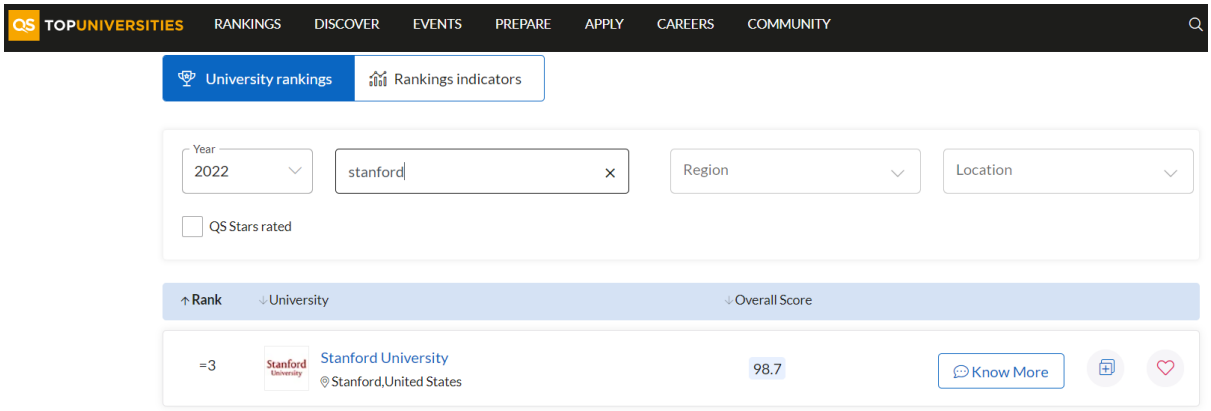

Figura 9: Ranking Stanford University. Fuente: https://www.topuniversities.com/university-rankings/world-university-rankings/2022

- Artículo 7: Development and Refinement of a chatbot for Cybersecurity Support

  Universidad: Universidad de Zurich

  Esta es una tesis de bachillerato presentada por un estudiante de la Universidad de Zurich, la cual Según el QS World University Rankings 2022, esta universidad se encuentra en la posición #70.

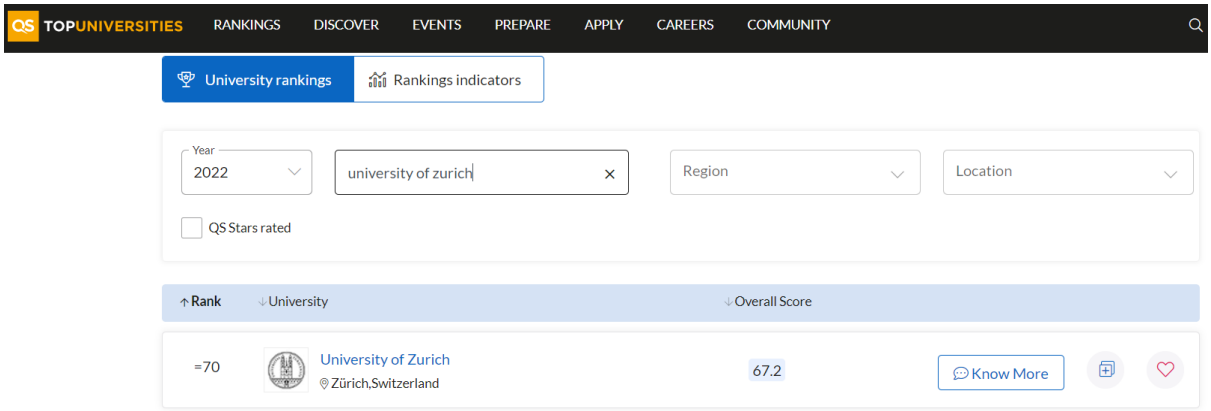

Figura 10: Figura 10: Ranking University of Zurich. Fuente: https://www.topuniversities.com/university-rankings/world-university-rankings/2022

1.9.2.2 Revisión de la selección

La selección de estudios primarios se realiza tras llevar a cabo una revisión de los Abstract y contenido incluido en cada artículo.

Tabla 3: *Extracción fuente 1.*

Repositorio	**Springer Link**
Título	Interrogating Virtual Agents: In Quest of Security Vulnerabilities
Publicación	Springer Link, IFIP International Conference on Testing Software and Systems (ICTSS) 2020
Autores	Josip Bozic, Franz Wotawa
Referencia	Bozic, J., & Wotawa, F. (diciembre de 2020). Interrogating Virtual Agents: In Quest of Security Vulnerabilities. In IFIP International Conference on Testing Software and Systems (pp. 20-34). Springer, Cham. https://doi.org/10.1007/978-3-030-64881-7_2
Descripción	
Área	Chatbots, sus vulnerabilidades en ciberseguridad y cómo bajo un escenario de pruebas son probados.
Resumen	Los chatbots, es decir, los sistemas que se comunican en lenguaje

Repositorio	Springer Link
	natural han adquirido una importancia creciente en los últimos años. Estos agentes virtuales brindan servicios o productos específicos a los clientes las 24 horas, los 7 días de la semana. Los chatbots proporcionan una interfaz simple e intuitiva, es decir, procesamiento de lenguaje natural, lo que los hace cada vez más atractivos para diversas aplicaciones. De hecho, los chatbots se utilizan como sustitutos de tareas repetitivas o consultas de los usuarios que pueden automatizarse. Sin embargo, estas ventajas siempre van acompañadas de preocupaciones, por ejemplo, si se puede garantizar la seguridad y la privacidad. Estas preocupaciones se vuelven cada vez más importantes porque, a diferencia de las solicitudes simples, los chatbots más sofisticados pueden utilizar servicios personalizados para los usuarios. En tales casos, se procesan e intercambian datos confidenciales del usuario. Por tanto, estos sistemas se convierten en objetivos naturales de ciberataques con consecuencias imprevistas. Por esta razón, garantizar la seguridad de la información de los chatbots es un desafío importante en la práctica. En este documento, contribuimos a este desafío e introducimos un enfoque de prueba de seguridad automatizado para chatbots. El marco presentado puede generar y ejecutar pruebas para detectar debilidades intrínsecas del software que conducen a la vulnerabilidad Cross-Site Scripting (XSS). Suponemos que se activa una vulnerabilidad cuando se obtiene información crítica del agente virtual o se bloquea, independientemente de su propósito. Discutimos los fundamentos básicos subyacentes y demostramos el enfoque de prueba utilizando varios chatbots del mundo real.
Aspectos a destacar	
	El tema abarca la importancia de considerar las posibles vulnerabilidades de una implementación de chatbots que no considere controles de ciberseguridad.

Fuente: Elaboración propia

Tabla 4: *Extracción fuente 2.*

Repositorio	Sage Journals
Título	Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation
Publicación	Sage Journals, Vol 73, Issue 2, 2018
Autores	Alex S. Wilner
Referencia	Wilner, A. S. (2018). Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. International Journal: Canada's Journal of Global Policy Analysis, 73(2), 308–316. https://doi.org/10.1177/0020702018782496
Descripción	
Área	Inteligencia Artificial, cómo esto se relaciona con el manejo de datos y la ciberseguridad
Resumen	El futuro de la ciberseguridad está cambiando. La inteligencia

	artificial desafía las nociones existentes de seguridad, derechos humanos y gobernanza. Las campañas de desinformación digital aprovechan las fabricaciones y las falsedades para obtener beneficios políticos y geoestratégicos. Y el Internet de las cosas, un panorama digital en el que miles de millones de objetos inalámbricos, desde frigoríficos inteligentes hasta automóviles inteligentes, están conectados entre sí, proporciona nuevos medios para distribuir y realizar ciberataques. A medida que los desarrollos tecnológicos modifiquen la forma en que pensamos sobre la ciberseguridad, también ampliarán la forma en que los gobiernos y las sociedades tendrán que aprender a responder. Este resumen de políticas analiza el panorama emergente de la seguridad cibernética en Canadá y en el extranjero, con la intención de informar el debate público y el discurso sobre los desafíos y oportunidades cibernéticos emergentes.
Aspectos a destacar	
	El tema abarca la importancia de considerar las posibles vulnerabilidades de una implementación de chatbots que no considere controles de ciberseguridad.

Fuente: Elaboración propia

Tabla 5: *Extracción fuente 3.*

Repositorio	Padova University Press, PHRG Peace Human Rights Governance
Título	Artificial Intelligence and Personal Data: International and National Framework
Publicación	Padova University Press, PHRG Peace Human Rights Governance - Volume 5, Issue 1, March 2021
Autores	Aliyev, A. Ibrahim, Rzayeva G. Aydin, & Ibrahimova A. Nazim
Referencia	Aliyev, A. I. (2021). Artificial Intelligence and Personal Data: International and National Framework. Peace Human Rights Governance. http://phrg.padovauniversitypress.it/2021/1/4
Descripción	
Área	Inteligencia Artificial, Datos, Humanos, Derechos Humanos, Robots, Privacidad
Resumen	En los últimos años, varias cuestiones relacionadas con el rápido desarrollo de las tecnologías de la información y la comunicación, con los sistemas de inteligencia artificial derivados de los procesos de digitalización, son difíciles de responder en la literatura teórica. El dinamismo actual y el reducido número de estudios hacen necesario analizar muchos puntos importantes de este ámbito. Especialmente, debido a las cambiantes tendencias de desarrollo de los derechos humanos en la sociedad electrónica, algunas relaciones siguen sin estar reguladas. Aunque la aplicación de sistemas de inteligencia artificial se caracteriza por aspectos positivos, por un lado, por otro lado, genera diversos problemas prácticos. La ubicación de toda la información personal en los sistemas de información, como resultado de la integración de estos sistemas, se enfrenta a la

Repositorio	Padova University Press, PHRG Peace Human Rights Governance
	amenaza de "¿qué pasa si los problemas de privacidad se revelan a todos?". Los sistemas de inteligencia artificial diseñados para servir a las personas, a menudo "interfieren" con su privacidad. Elon Reeve Musk, un conocido empresario tecnológico, afirma: "La inteligencia artificial es más peligrosa que las armas nucleares". El objetivo principal de escribir este artículo es ayudar a resolver los problemas que se enfrentan en relación con los problemas mencionados anteriormente. En nuestro artículo, hemos hecho varias sugerencias: dar un concepto legal a los sistemas de inteligencia artificial; edición de normas relacionadas con derechos digitales, incremento de la cibercultura para garantizar la ciberseguridad, etc. Así, por rápido que sea la digitalización, la automatización, el desarrollo científico y tecnológico, no implica el uso ilimitado de sistemas de inteligencia artificial. En cualquier caso, se deben orientar los derechos humanos, se debe tomar como base un "enfoque moral" y se debe garantizar la inviolabilidad de la privacidad.
Aspectos a destacar	
	Este tema y publicación tocan a profundidad características relacionadas con la privacidad de los seres humanos cuando se utilizan tecnologías de inteligencia artificial y como la ciberseguridad puede ayudar a mantener esa privacidad.

Fuente: Elaboración propia

Tabla 6: *Extracción fuente 4.*

Repositorio	**International Finance Corporation (IFC) | World Bank Group**
Título	Artificial Intelligence in Emerging Markets - Opportunities, Trends, and Emerging Business Models
Publicación	International Finance Corporation (IFC) Publications, Second and Expanded Edition, March 2021
Autores	Tonci Bakovic, Margarete Biallas, Alejandro Caballero, Maria Lopez Conde, Peter Cook, Prajakta Diwan, George Vivien Houngbonon, Hassan Kaleem, Baloko Makala, Sumit Manchanda, Rebecca Menes, Peter Mockel, Xiaomin Mou, Monique Mrazek, Gordon Myers, Kiril Nejkov, Marina Niforos, Felicity O'Neill, Ahmed Nauraiz Rana, Friedemann Roy, Ommid Saberi, Sabine Schlorke, Maud Schmitt, William Sonneborn, Davide Strusani, Ian Twinn
Referencia	Bakovic, T., Biallas, M., Caballero, A., Lopez Conde, M., Cook, P., Diwan, P., Vivien Houngbonon, G., Kaleem, H., Makala, B., Manchanda, S., Menes, R., Mockel P., Mou, X., Mrazek, M., Myers, G., Nejkov, K., Niforos, M., O'Neil, F., Rana, A. N.,... Twinn, Ian (marzo de 2021), Artificial Intelligence In Emerging Markets - Opportunities, Trends, and Emerging Business Models. https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/artificial+intelligence+in+emerging+markets
Descripción	
Área	Inteligencia Artificial, sus oportunidades, tendencias y modelos de

	negocio emergentes
Resumen	La inteligencia artificial está cambiando los negocios y la sociedad de forma inimaginable. Aun así, no se ha alcanzado todo su potencial, ya que la manera de realizar diversas actividades (búsqueda/recopilación de información, fabricación de productos, por mencionar un par) se encuentra en constante evolución. En los mercados emergentes, la IA ofrece reducción de costos y barreras de entrada para emprendedores y empresas, creando así, modelos comerciales innovadores con la posibilidad de superar a las tecnologías tradicionales. Se explota el rol de la IA tanto en mercados emergentes como en países en desarrollo, a través y dentro de sectores clave específicos; como transporte, hogares inteligentes (smart homes), energía, agroindustria, salud, financiero, manufactura.
Aspectos a destacar	
	De manera general, se destaca a los chatbots entre las aplicaciones de la inteligencia artificial más populares y usadas. De igual manera, se reconoce el riesgo económico y de inclusión social que trae consigo este tipo de tecnologías disruptivas. Mención de chatbots y su impacto como factor diferenciador y revolucionario en el sector financiero y de salud.

Fuente: Elaboración propia

Tabla 7: *Extracción fuente 5.*

Repositorio	**Harvard Kennedy School - Belfer Center for Science and International Affairs**
Título	Attacking Artificial Intelligence - AI's Security Vulnerability and What Policymakers Can Do About It
Publicación	Belfer Center for Science and International Affairs Paper, Harvard Kennedy School, agosto de 2019.
Autores	Marcus Comiter
Referencia	Comiter, M. (agosto de 2019), Attacking Artificial Intelligence - AI's Security Vulnerability and What Policymakers Can Do About It. Belfer Center for Science and International Affairs Paper, Harvard Kennedy School. https://www.belfercenter.org/publication/AttackingAI
Descripción	
Área	Inteligencia Artificial, ciberseguridad y sus vulnerabilidades
Resumen	Se habla de un nuevo tipo de ataque de ciberseguridad llamado "Ataque de Inteligencia Artificial". Al adoptar e incluir cada vez más sistemas de IA en componentes críticos en nuestro diario vivir y sociedad, representan una vulnerabilidad emergente y sistemática con el potencial de tener efectos significativos en la seguridad de un país. Por lo que también se resalta son fundamentalmente diferencias de ciber ataques tradicionales. Menciona partes críticas de la sociedad que son directamente vulnerables a estos ataques: filtradores de contenido, las fuerzas armadas / milicia, cumplimiento de leyes, tareas tradicionalmente basadas en el ser humano reemplazadas por IA y la sociedad civil.

Repositorio	Harvard Kennedy School - Belfer Center for Science and International Affairs
Aspectos a destacar	
	Propone creación de programas de “Cumplimiento de Seguridad de IA” para proteger contra ataques de IA, con la finalidad de reducir el riesgo de estos ataques y mitigación del impacto en caso de ataques exitosos. Los chatbots caben en la categoría de “tareas tradicionalmente basadas en el ser humano reemplazadas por IA”, pues se busca realizar tareas como la atención de clientes.

Fuente: Elaboración propia

Tabla 8: *Extracción fuente 6.*

Repositorio	Stanford University - Human-Centered Artificial Intelligence, Artificial Intelligence (HAI)
Título	Artificial Intelligence Index Report 2021
Publicación	Human-Centered Artificial Intelligence, Artificial Intelligence (HAI) Annual report, Stanford University
Autores	Daniel Zhang, Saurabh Mishra, Erik Brynjolfsson, John Etchemendy, Deep Ganguli, Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Niebles, Michael Sellitto, Yoav Shoham, Jack Clark, Raymond Perrault
Referencia	Zhang, D., Mishra, S, Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J. C., Sellitto, M., Shoham, Y., Clark, J., & Perrault, R. (marzo de 2021). The AI Index 2021 Annual Report. AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA. https://aiindex.stanford.edu/ai-index-report-2021/
Descripción	
Área	Inteligencia Artificial, reporte
Resumen	El Informe de índice de IA rastrea, recopila, destila y visualiza datos relacionados con la inteligencia artificial. Pretende proporcionar datos imparciales, rigurosamente examinados y de origen mundial para que los responsables de la creación de políticas, los investigadores, los ejecutivos, los periodistas y el público en general desarrollen intuiciones sobre el complejo campo de la IA.
Aspectos a destacar	
	Más del 60% de las organizaciones encuestadas en el 2020 consideran los riesgos de ciberseguridad como los más relevantes con la adopción de IA, manteniéndose en la misma posición en comparación al 2019. Se recalca el incremento de inversión en IA en las universidades top del mundo, así como en publicaciones académicas relevantes al tema. Se destaca también, la rapidez en la que el Procesamiento del Lenguaje Natural ha progresado, el cual está ligado a chatbots. Expertos indican en el informe que el Procesamiento del Lenguaje Natural será la tendencia que defina la IA en el 2021. Más del 50% de las organizaciones encuestadas indican que han

Repositorio	Stanford University - Human-Centered Artificial Intelligence, Artificial Intelligence (HAI)
	incorporado y adoptado IA en al menos una función de negocio en comparación al 2019. Se habla de la existencia y el esfuerzo de adopción y/o creación de políticas para IA con tal de maximizar el uso de estas tecnologías y sus implicaciones.

Fuente: Elaboración propia

Tabla 9: *Extracción fuente 7.*

Repositorio	Zurich Open Repository and Archive (ZORA), University of Zurich
Título	Development and Refinement of a chatbot for Cybersecurity Support
Publicación	Bachelor's Thesis, Department of Informatics (IFI), University of Zurich, February 04, 2021
Autores	Bulin Shaqiri
Referencia	Bulin Shaqiri (2021). Development and Refinement of a chatbot for Cybersecurity Support. https://files.ifi.uzh.ch/CSG/staff/franco/extern/theses/BA-B-Shaqiri.pdf
Descripción	
Área	Chatbot, Inteligencia Artificial, Ciberseguridad, Soporte
Resumen	La ciberseguridad recibe cada vez más la atención que merece. A más tardar, ahora que la pandemia Covid-19 se ha apoderado de todo el mundo y los empleados se ven obligados a trabajar desde casa siempre que sea posible, creando así nuevas vulnerabilidades para que las exploten los ciberdelincuentes, la importancia de la ciberseguridad es aún más evidente. En los últimos años, sin embargo, las inversiones como tales han ido en aumento, y la gran mayoría se ha movido hacia la seguridad como servicio y, por lo tanto, ha contratado protección fuera del sitio de varios proveedores. Junto con los sistemas de recomendación, se puede gestionar el gran volumen de alternativas de solución, pero aún se requiere experiencia para especificar correctamente los requisitos. Por lo tanto, los usuarios finales no pueden ingresar sus demandas de una manera simple y rápida. Si bien otros campos han explorado los agentes conversacionales (es decir, los chatbots) como posibles soluciones, incluidos algunos enfoques en ciberseguridad, todavía no se ha realizado ningún trabajo que haya utilizado dichos agentes conversacionales para mejorar la gestión de la ciberseguridad. En este sentido, el objetivo general de esta tesis es proporcionar un prototipo que permita a los usuarios finales enviar sus solicitudes de soporte de ciberseguridad, con el agente conversacional respondiendo luego con respuestas precisas, de modo que se pueda utilizar la información perspicaz extraída de la conversación. por los usuarios finales durante el proceso de toma de decisiones de ciberseguridad.
Aspectos a destacar	

Repositorio	Zurich Open Repository and Archive (ZORA), University of Zurich
	Chatbot para soporte de atención a eventos de ciberseguridad

Fuente: Elaboración propia

1.9.3 Análisis de resultados

A partir de los estudios recolectados en la sección anterior podemos determinar que las tecnologías de inteligencia artificial (IA) se han vuelto muy populares y útiles, llegando a sustituir completamente algunas tareas e inclusive trabajos que típicamente se han desempeñado por humanos y que prácticamente son utilizadas en todas las áreas de estudio de la actualidad. Esto ha permitido que muchas organizaciones utilicen diferentes tipos de ofrecimiento de esta tecnología, como las de chatbot, al ser estas consideradas las de uso más popular; típicamente este tipo de tecnología es implementado para poder cumplir con funciones o tareas de asistentes virtuales por lo que deben de manejar diferentes clasificaciones de información, como lo serían información personal, credenciales, información sensible o confidencial, entre otras.

Es importante tomar en cuenta que esta tecnología también tiene la capacidad de extraer y manipular información por medio de tareas automatizadas, por lo que la gestión no es solo a través de un usuario propiamente, sino que puede ser el resultado de la ejecución de un proceso ligado a otro sistema. Por lo tanto, se puede comprender que existe una necesidad evidente de análisis con respecto a sus vulnerabilidades, amenazas, riesgos, y buenas prácticas en ciberseguridad, ya que de lo contrario con un mal uso de estas tecnologías (o sin los controles de ciberseguridad que permitan reducir el riesgo asociado), se podrían ver comprometidos, lo que daría paso a un impacto o amenaza superior debido a la

pérdida de información, interrupción de sistemas, manipulación de información, entre otros.

Es por tanto importante entender qué diferentes tipos de ataques podrían afectar este tipo de tecnologías de forma directa o indirecta. Al comprender los posibles derivados de los riesgos, que a su vez encierran las amenazas y vulnerabilidades posibles, se podrá identificar maneras de prevenir, detectar y mitigar las incidencias, así como también la posibilidad de crear la documentación relevante que permita aprender de experiencias existentes y, a partir de esto, crear el análisis cualitativo que posteriormente permitirá crear la propuesta como eje central de la investigación.

Bajo el enfoque en el sector privado costarricense, se considera y demuestra que es el sector con mayor producción de empleo y economía en el país, por lo que, en caso de una eventualidad o incidencia, podría ser el que tendría una mayor afectación derivada de un ataque a las soluciones de chatbot. Este enfoque permite delimitar la investigación e identificar el nivel de madurez en la implementación segura de esas tecnologías y la creación de la propuesta de buenas prácticas en caso de que se encuentren puntos de mejora.

Capítulo 2. Marco Conceptual

Se generó la nube de conceptos que se muestra en la Figura 11, con el objetivo de identificar los conceptos más relevantes de la investigación. En la Figura 12 se muestra la relación entre los conceptos primordiales de la investigación que permite generar el marco conceptual de esta.

Figura 11: Nube de palabras generada utilizando el sitio. Fuente: Elaboración propia. Elaborado usando el sitio https://tagcrowd.com

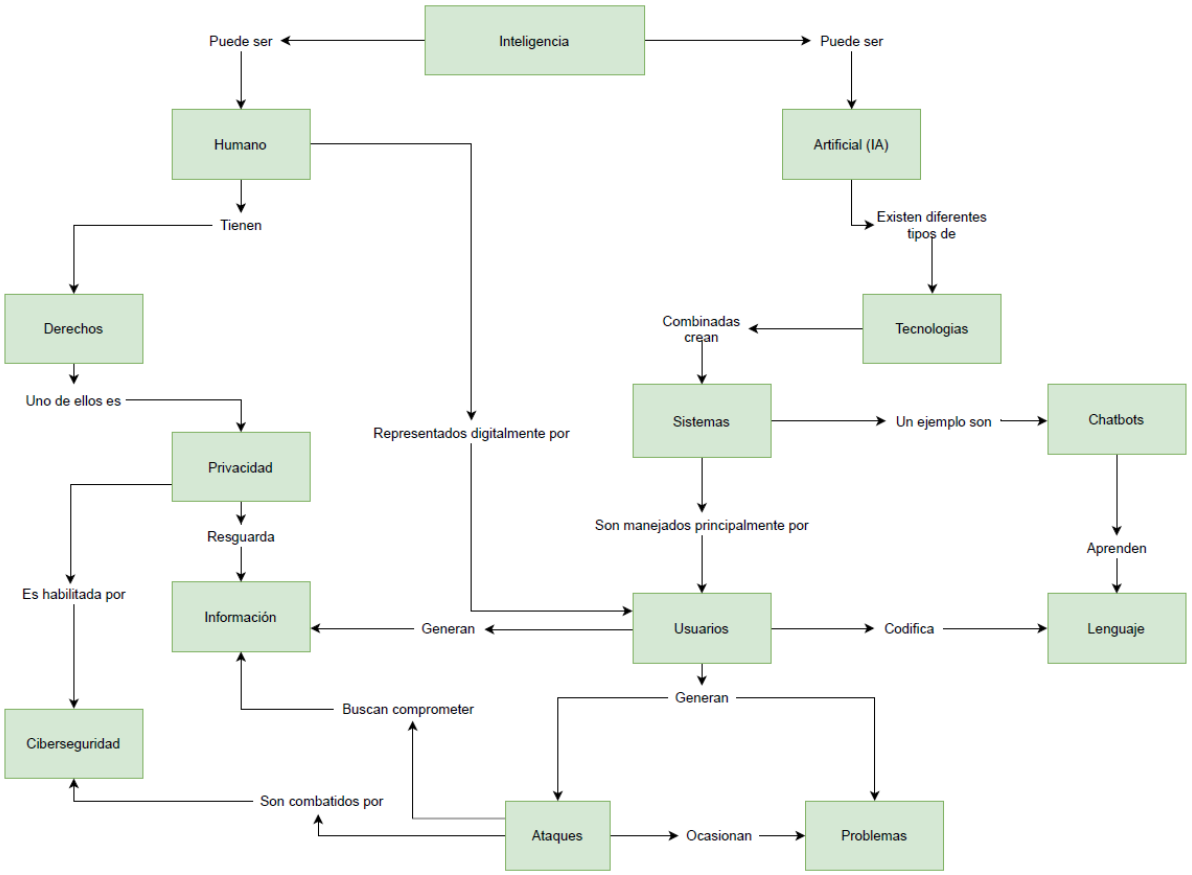

Figura 12: Mapa conceptual. Fuente: Elaboración propia. Elaborado usando el sitio https://app.diagrams.net

Se presenta, a continuación, la definición de los conceptos mayoritariamente mencionados y de mayor relevancia para la investigación. Se debe destacar que, con el fin de brindar un mejor contexto del tema en cuestión, el orden en el que se presentan los conceptos va desde un ámbito general hacía aspectos más específicos necesarios para comprender los diversos elementos asociados al tema.

2.1 Definición de conceptos

Las siguientes definiciones fueron tomadas desde diferentes sitios especializados en la temática de la investigación. Fueron consideradas a partir de su importancia y relevancia para el entendimiento y el contexto de la investigación.

- Inteligencia: capacidad de entender y pensar acerca de las cosas, y de obtener y usar conocimiento. (Macmillan dictionary, s.f.)
- Inteligencia Artificial: IBM (2020) la define: "Es la ciencia y la ingeniería de la fabricación de máquinas inteligentes, especialmente programas informáticos inteligentes. Está relacionada con la tarea similar de usar computadoras para entender la inteligencia humana, pero la IA no tiene que limitarse a métodos que son biológicamente observables"
- Derechos: los derechos dominan la comprensión moderna de qué acciones son permisibles y que instituciones son justas. Estructuran la forma de los gobiernos, el contenido de las leyes y la forma de la moralidad tal como muchos la ven ahora. Aceptar un conjunto de derechos es aprobar una distribución de libertad y autoridad, y, por ende, respaldar una cierta visión de lo que se puede, se debe y no se debe hacer. (Stanford Encyclopedia of Philosophy, 2005)
- Privacidad: el estado de ser libre de intrusión o perturbación en la vida o los asuntos privados de uno. (Collins Dictionary, s.f.)

- Información: el término se usa para denotar cualquier cantidad de datos, código o texto que se almacena, envía, recibe o manipula en cualquier medio. (Stanford Encyclopedia of Philosophy, 2012)
- Tecnologías: La tecnología o ingeniería como práctica se ocupa de la creación de artefactos y, cada vez más importante, de servicios basados en artefactos. El proceso de diseño, el proceso estructurado que conduce hacia ese objetivo, forma el núcleo de la práctica de la tecnología. (Stanford Encyclopedia of Philosophy, 2009)
- Sistemas: conjunto de elementos organizados que cumplen determinada función. (Cambridge, s.f.).
- Lenguaje: cualquier sistema de signos que permite componer e interpretar mensajes (Cambridge, s.f.).
- Usuarios: persona que utiliza un servicio (Cambridge, s.f.).
- Ataques: acción violenta que causa daño a alguien o algo (Cambridge, s.f.).
- Problemas: cuestión difícil que se intenta resolver o explicar (Cambridge, s.f.).
- Ciberseguridad: Según la International Telecommunications Unit (ITU), ciberseguridad es definida como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber-entorno.

2.2 Chatbots y sus consideraciones

Un chatbot es como se conocen a los robots de chat, un programa que simula la conversación humana, o chat, a través de la inteligencia artificial, permitiendo a los humanos interactuar con recursos digitales tal cual como lo harían con una persona

real (Oracle, s.f.). Estos son utilzados comúnmente en diferentes industrias para múltiples propósitos.

Microsoft (s.f) describe que los chatbots utilizan inteligencia artificial (IA) y procesamiento de lenguaje natural (NLP) que permite desarrollar múltiples actividades, entre ellas, el apoyar a los usuarios a interactuar con servicios web o aplicaciones a través de texto, gráficos o voz. Los chatbots pueden comprender el lenguaje humano natural, simular una conversación humana, ejecutar tareas sencillas y automatizadas. Los chatbots se utilizan en una variedad de canales, como aplicaciones de mensajería, aplicaciones móviles, sitios web y aplicaciones habilitadas para voz.

El foco de la investigación será específicamente sobre chatbots conversacionales y como estos permiten habilitar los beneficios previamente mencionados. Este tipo será analizado para entender sus riesgos y amenazas, lo que posteriormente permitirá crear la propuesta de utilización segura. Se definirá a continuación en qué consisten y su aplicabilidad en diferentes sectores.

2.2.1 ¿Por qué utilizarlos?

> Entre las grandes potencias en tecnología, una de las principales menciona: Los chatbots se utilizan para ayudar a los humanos a interactuar con la tecnología y automatizar tareas. Las mejoras en IA, aprendizaje automático, ciencia de datos y procesamiento de lenguaje natural han permitido la proliferación de chatbots al facilitar la creación de bots conversacionales para una variedad de aplicaciones que benefician a las empresas, sus clientes y sus empleados. (Microsoft, s.f.)

Muchas empresas los usan para que actúen como agentes virtuales que pueden manejar problemas de servicio al cliente y apoyar a los colaboradores. De

igual forma, ayudan también a las empresas a acelerar el ciclo de ventas, generar más clientes potenciales y mejorar la lealtad de los clientes.

A medida que las organizaciones invierten en tecnologías cada vez más complicadas y crean múltiples interfaces de mensajería, los chatbots se están convirtiendo rápidamente en un puente necesario entre clientes, colaboradores y las enormes cantidades de información, sistemas y aplicaciones con las que interactúan.

2.2.2 Procesamiento del lenguaje natural

Es el proceso de comprender, analizar y responder al habla humana. Se refiere a todo el proceso de principio a fin de cómo los chatbots usan la inteligencia artificial para comprender grandes cantidades de datos del lenguaje natural.

2.2.3 ¿Cómo funcionan los chatbots?

Cualquier aplicación con la que los usuarios interactúan de una forma conversacional, usando texto, gráficos o voz. A pesar de los diferentes tipos, todos funcionan de la misma manera. Puede considerarse como una aplicación que tiene una interfase conversacional. En la Figura 13 se muestra el funcionamiento de estos de manera general.

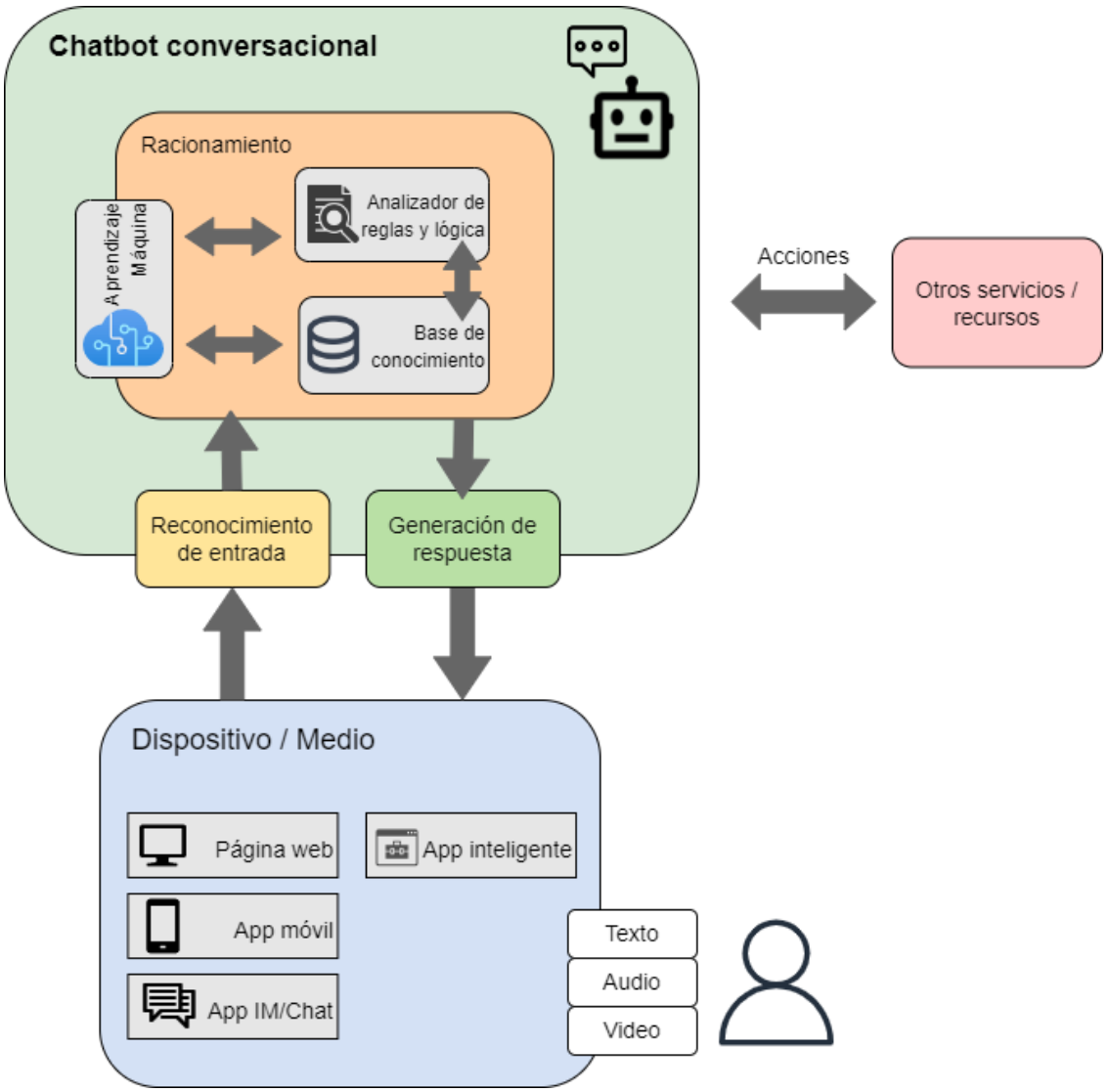

Figura 13: Funcionamiento de los chatbots. Fuente: Elaboración propia. Elaborado usando el sitio draw.io

El usuario ingresa un mensaje en texto u oral a un chatbot a través de un medio, el cual puede ser una página web, una aplicación móvil, de mensajes o de chat o una aplicación inteligente. Este mensaje puede ser una pregunta o un comando.

El chatbot recibe el contenido del mensaje y captura información relacionada, como el medio por el cual llegó el mensaje. Luego el chatbot utiliza procesamiento

de lenguaje natural (NLP) para determinar el propósito del mensaje e identificar las intenciones relevantes.

El chatbot determina una respuesta apropiada y la devuelve a través del mismo medio. Este proceso continúa los mismos pasos anteriores a medida que continúa la conversación hasta que se responda la pregunta de un usuario, se resuelva su problema o hasta que la solicitud sea transferida a un agente humano.

2.2.4 Chatbots Conversacionales basados en texto

Son un tipo de chatbot más complejo e interactivo que utiliza el procesamiento del lenguaje natural para proporcionar interacciones más personalizadas. Estos usan IA para conversaciones, procesamiento de lenguaje natural y acceso a bases de datos de conocimiento y otra información para detectar matices en las preguntas y respuestas de los usuarios, al tiempo que brindan respuestas dinámicas y relevantes de la misma manera que lo haría un ser humano.

Los chatbots, comúnmente conocidos como asistentes virtuales o asistentes digitales, también utilizan inteligencia predictiva y analítica para la personalización en función del perfil y de los comportamientos anteriores de cada usuario. Con el tiempo, estos pueden aprender las preferencias de un usuario y usar ese aprendizaje para hacer recomendaciones y anticipar necesidades.

Estos son utilizados por empresas de comercio electrónico, servicios en línea, plataformas sociales, empresas con software avanzado como servicio (SaaS) y negocios de empresa a empresa (B2B) que brindan soluciones comerciales.

Típicamente mantienen una arquitectura de interacción en el trasfondo. A continuación, se describen los módulos típicos que la componen:

- Módulo de cliente: Es la parte con la que el usuario podrá interactuar, así como las aplicaciones que el chatbot puede controlar.
- Módulo de comunicación: Es la infraestructura que transmite los mensajes de usuario desde el módulo de cliente hasta el módulo de generación de respuesta o módulo de base de datos.
- Módulo de generación de respuesta: Es el programa responsable por el entendimiento del mensaje de entrada y la generación de una respuesta apropiada para el usuario.
- Módulo de bases de datos: Es el lugar donde todos los datos relevantes a la conversación son almacenados.

2.2.5 Aplicación en diferentes industrias

- Recursos humanos:

  Ayudar con tareas del área, como generación de informes, respuestas frecuentes a consultas de usuarios de sistemas de recursos humanos o servicios propios.
- Finanzas y Contabilidad:

  Ayudar en la preparación de informes de gastos, abrir solicitudes de pedidos, actualizar y rastrear detalles de proveedores.
- Marketing:

  Envío de ofertas dirigidas a clientes leales, realizar un seguimiento de la satisfacción del cliente y crear experiencias personalizadas para la retención de clientes.
- Ventas:

Ofrecer apoyo e información a los clientes potenciales, proporcionar cotizaciones y comenzar una conversación proactiva, además de liberar tiempo para que el vendedor se centre en las ventas estrechas.

2.2.6 Beneficios y limitaciones

Los beneficios y limitaciones de los chatbots radican en la IA y los datos que los impulsan.

La IA es excelente para automatizar procesos repetitivos y mundanos. Cuando se integra en un chatbot para este tipo de tareas, esto suele funcionar bien. Sin embargo, si se realiza una solicitud a un chatbot que excede sus capacidades o complica aún más su tarea, este puede bloquearse, con consecuencias negativas para la empresa y el cliente. Hay preguntas y problemas que los chatbots simplemente no pueden responder o resolver, como problemas de servicio complejos que involucran una gran cantidad de variables.

Los desarrolladores pueden sortear estas limitaciones agregando una alternativa a su aplicación de chatbot para enrutar al usuario a otro recurso (como un agente en vivo) o solicitar al cliente otra pregunta o problema. Algunos chatbots pueden moverse sin problemas a través de la transición entre chatbots, agentes en vivo y viceversa. A medida que la tecnología y las implementaciones de IA continúan evolucionando, los chatbots y los asistentes digitales se integrarán de manera más fluida en nuestras experiencias cotidianas.

Todos los chatbots usan datos, accesibles desde una variedad de fuentes. Siempre que los datos sean de alta calidad y estén desarrollados correctamente, los datos serán un habilitador para este. Sin embargo, si la calidad de los datos es deficiente, limitará la funcionalidad de la herramienta; e, incluso, si la calidad es buena, pero el entrenamiento de aprendizaje máquina del chatbot no se modela

correctamente o no se supervisa, este puede tener un rendimiento deficiente o no deseado.

En otras palabras, su chatbot es tan bueno como la IA y los datos que integra.

2.2.7 Vulnerabilidades, amenazas, riesgos de seguridad y contramedidas aplicables en la tecnología chatbot

Se debe de considerar, en primer lugar, los términos asociados a la ciberseguridad que se analizarán de acuerdo con los diferentes elementos de los chatbots. Por esto, se empieza por definir los conceptos de amenaza, vulnerabilidad, riesgo y explotación:

- La **amenaza** a la seguridad se define como el riesgo de que una organización y sus sistemas puedan verse comprometidos (Hasal, M., Nowaková, J., Saghair, K. A., Abdulla, H., Snášel, V., & Ogiela, L., 2021).
- Una **vulnerabilidad** de sistema es una debilidad que un atacante puede explotar para violar los límites de privilegios (es decir, realizar acciones no autorizadas) en un sistema informático. etcétera. Un sistema es vulnerable cuando tiene código “débil”, no se encuentra con los parches de seguridad recomendados y actualizados, no se encuentra protegido de la manera adecuada, etc (Hasal, M., Nowaková, J., Saghair, K. A., Abdulla, H., Snášel, V., & Ogiela, L., 2021).
- Un **riesgo** de ciberseguridad es la medida en que una entidad se ve amenazada por una circunstancia o evento potencial (NIST, s.f.).
- Un ***exploit*** es un código que aprovecha una vulnerabilidad de software o una falencia de seguridad (Trend Micro, s.f.).

El incremento en el uso de los asistentes personales permite corroborar la creciente popularidad de los chatbots. Sin embargo, es importante no solo tomar en cuenta las innovaciones alrededor de la tecnología o cómo esta simplifica el día a día de las personas, sino también aquellas posibles vulnerabilidades o riesgos existentes y cómo los atacantes podrían aprovecharlas.

En esta sección se pretende describir vulnerabilidades o riesgos relacionados con la tecnología. Se define la seguridad de los chatbots y se referencia algunos antecedentes sobre el estado del arte en el campo. Para esto se tomará en cuenta la arquitectura típica de chatbot, la cual fue descrita en la sección 2.2.4 Chatbots Conversacionales basados en texto.

Se considera el siguiente escenario: la interacción entre un usuario y la herramienta.

Primero, un usuario inicia sesión en la plataforma asociada donde está alojado el chatbot, esta podría ser una aplicación en su teléfono móvil, un sitio web u otro dispositivo con la capacidad de acceso considerado como “inteligente”, de esta manera se representan las interfaces del lado del cliente con las que el usuario interactúa y genera mensajes. Otra función importante del lado del cliente incluye la autenticación del usuario.

Cuando se envía un mensaje, el módulo de comunicación es responsable de transportar los textos del lado del cliente al módulo que genera la respuesta. Aquí, los desarrolladores se centran en cifrar y autenticar las comunicaciones mediante protocolos seguros como HTTPS. Este módulo también es responsable de monitorear el tráfico en busca de actividad sospechosa, como un ataque DDoS inminente.

Una vez que se llega al lado del servidor, el chatbot debe interpretar el mensaje y generar una respuesta. La interpretación del mensaje implica algoritmos de procesamiento de lenguaje natural (NLP) que se utilizarán para analizar oraciones en campos útiles. Para generar el mensaje apropiado el modelo aprende a asignar una oración de entrada a la oración de salida más apropiada o a la respuesta óptima.

Una vez que el módulo generador de respuesta ha generado la respuesta, el módulo de comunicación la retransmite al módulo cliente. Al mismo tiempo, el módulo de base de datos almacena información relacionada con la interacción actual del chatbot. Las preferencias del usuario también se pueden almacenar aquí, por ejemplo, a cuál tema de conversación responde más activamente el usuario actual.

Con base en la información anterior se pueden considerar riesgos o vulnerabilidades asociados a cada uno de los módulos que son parte de la solución.

2.2.7.1 Módulo del cliente

- Ataque de activación no intencional →

  En una situación ideal, el usuario tiene control total sobre los datos recopilados por el asistente personal. Sin embargo, las cosas pueden salir mal de varias maneras. En ocasiones, las frases de activación que utilizan estos asistentes personales pueden confundirse con otras palabras en una conversación informal. Un atacante podría utilizar palabras claves que permitan obtener información personal o bien que detonen acciones que exploten y violenten la privacidad de los usuarios o de la información que el propio chatbot maneja.

  - **Contramedida:**

Se han desarrollado herramientas que permiten diferenciar de las conversaciones generadas por bots o personas. Por ejemplo, Xiaoice de Microsoft, utiliza un clasificador humano-a-bot de bots para determinar si un humano está hablando con el chatbot. De lo contrario, Xiaoice puede captar conversaciones que el usuario está teniendo con otras personas.

- Autenticación y autorización →

  La confirmación de la identidad del usuario (autenticación) no siempre es necesaria, por ejemplo, cuando el usuario solicita ayuda (tomando como referencia el acceso a un sitio de compras) generalmente no se precisa de una autenticación, el sistema no requiere tampoco el acceso a los datos del usuario.

  Sin embargo, la situación es diferente cuando se requiere trabajar con los datos del usuario, como cuando se chatea con un chatbot bancario sobre el saldo de una cuenta. En ese caso, la autenticación y autorización son necesarias para validar al usuario con credenciales adecuadas y seguras. En caso de que no se realicen los procesos de autenticación y autorización, el usuario podría estar solicitando información que no le corresponde o violentando la privacidad de datos de otros usuarios existentes e inclusive de los propios sistemas.

  - **Contramedida:**

    La protección de los datos y la comunicación de un usuario está garantizada por la autenticación de dos factores. Por ejemplo, se le pide al usuario que se verifique mediante la autenticación de credenciales de la cuenta a través de un correo electrónico o un

mensaje de texto. También existen esquemas de autenticación de múltiples factores que se usan durante el inicio de sesión y la conversación con un chatbot.

En resumen, la autorización garantiza que la persona adecuada tenga acceso mediante el privilegio mínimo a los datos y servicios correctos, y la autorización es necesaria cuando un chatbot gestiona los datos de un usuario.

El almacenamiento y el intercambio de datos personales a través de Internet nunca serán considerados 100% seguros. Al interactuar con los chatbots, una capa de seguridad de autenticación personal (escaneo personal), confirma la verificación del usuario por parte de los bots. El escaneo personal también garantiza que, en el caso de interactuar con un chatbot malicioso, la información del usuario no sea utilizada por atacantes.

- Chatbots Maliciosos →

Los chatbots maliciosos que operan en aplicaciones de mensajería instantánea multiplataforma (Viber, WhatsApp, etc.) pueden contactar al usuario y hacerse pasar, por ejemplo, por un chatbot de pedido de pizza. Tal situación se denomina *Smishing*.

Desde el momento en que el usuario responde al atacante, el chatbot continúa la conversación. El objetivo es similar al de otros esquemas de *phishing* para robar datos personales. Recibir mensajes de personas o servicios desconocidos es una buena indicación de que probablemente se trata de *phishing*.

- **Contramedida:**

La autenticación para aplicaciones de usuario protege los datos del usuario y del dispositivo contra el uso indebido o malicioso; en caso de que el usuario perdiera su teléfono o computadora, o simplemente los dejara desbloqueados involuntaria o voluntariamente. Si una ventana de chatbot se encuentra abierta, un atacante podría simplemente pedirle al chatbot información confidencial. Aquí, se necesitan tokens temporales que garanticen la interacción con recursos legítimos y que se puedan autenticar mutuamente.
De esta manera se puede evitar tanto la suplantación de identidad de un chatbot que busca obtener información del usuario o bien la suplantación del usuario solicitando información sensitiva o confidencial que maneja el propio chatbot.

- Control de Acceso Quebrantado →

El control de acceso aplica una política tal que los usuarios no pueden actuar fuera de sus permisos previstos. Las fallas generalmente conducen a la divulgación, modificación o destrucción de información no autorizada de todos los datos o al desempeño de una función comercial fuera de los límites del usuario.

- **Contramedida:**

  El control de acceso solamente será efectivo en el código del servidor confiable o API sin dependencia de servidor (*serverless*), donde el actor malicioso no tendrá el alcance para modificar la verificación de control de acceso o los metadatos. Implementar mecanismos de control de acceso una vez y reutilice en las otras aplicaciones del ambiente.

Los controles de acceso al modelo deben imponer la propiedad de los registros en lugar de aceptar que el usuario pueda crear, leer, actualizar o eliminar cualquier registro.

Registrar fallas de control de acceso y avisar a los administradores cuando corresponda, como, por ejemplo, en caso de múltiples intentos fallidos.

Establecer una tasa límite para la API y el acceso al controlador para minimizar el daño de las herramientas de ataque automatizado.

- Inyección →

Se considera que una aplicación es vulnerable a un ataque de este tipo en las siguientes circunstancias:

- La aplicación no valida, filtra ni desinfecta los datos proporcionados por el usuario.
- Las consultas dinámicas o las llamadas no parametrizadas sin escape consciente del contexto se utilizan directamente en el intérprete.

Para efectos del módulo de cliente, si no se validan correctamente las entradas que ingresan los usuarios, se puede caer en una condición de riesgo, lo mismo si se realiza una consulta que no tiene una manera adecuada de manejarse.

- **Contramedida:**
  - Prevenir la inyección requiere mantener los datos separados de los comandos y consultas.
  - Utilizar API seguras, que evite el uso del intérprete por completo, lo que proporciona una interfaz parametrizada.

- Utilizar una validación de entrada positiva del lado del servidor. Esta no es una defensa completa, ya que muchas aplicaciones requieren caracteres especiales, como áreas de texto o API para aplicaciones móviles.

2.2.7.2 Módulo de comunicación

- Ataques de Hombre en el Medio (MitM Attacks)

Estos ataques pueden interceptar mensajes entre el Cliente A y el Cliente B y reemplazarlos con los mensajes maliciosos del adversario. Estos ataques pueden incitar a la violencia al incitar a los usuarios, cambiar las políticas de opinión a través de ataques de ingeniería social o enviar spam a ambos clientes.

El principal desafío detrás de estos ataques es desarrollar una revisión confiable de los mensajes originales. La herramienta Honeybot, los sistemas trampas o honeypots para bots, habilita un “hombre en el medio” mediante la interacción con un intermediario que hace que la conversación sea natural al involucrar a los usuarios en el tema antes de realizar cambios en el mensaje. Por ejemplo, Honeybot podría hacer algunas preguntas como "¿Cuál es tu película favorita?" y una vez que la conversación está completamente desarrollada, el Honeybot puede lanzar ataques de spam insertando enlaces maliciosos. Parecería natural, ya que los usuarios compartieron enlaces a sus películas favoritas, pero Honeybot también podrían eliminar e insertar sus propias publicaciones.

Detectar estos ataques puede ser un desafío. En el caso de que exista un agente sofisticado que actúe como un hombre en el medio, la conversación puede parecer muy natural. En estos casos, lo más apropiado sería aplicar

protocolos de cifrado y autenticación para proporcionar tráfico entre el módulo cliente y la retroalimentación del módulo de generaciones de respuesta. A pesar de los riesgos, muchos chatbots todavía no aplican estas mejores prácticas.

- **Contramedida:**

  Detectar estos ataques puede ser desafiante. En los casos en que existe un agente sofisticado que actúa como un hombre en medio de la conversación, esta puede resultar o parecer muy natural.

  En estos escenarios, y, en general para la prevención de este tipo de ataques, lo mejor es adoptar protocolos de cifrado y autenticación para asegurar el tráfico entre el módulo del cliente y el módulo de respuesta.

- Ataques Distribuidos de Denegación de Servicio (DDoS)

  Los ataques DDoS tienen como objetivo evitar que el chatbot interactúe con los usuarios inundando el servidor con solicitudes. Para las empresas que confían en los chatbots para atender a sus clientes, el tiempo de inactividad puede tener un costo grave.

  Para llevar a cabo un ataque de este tipo, los atacantes normalmente necesitan recopilar una gran cantidad de recursos informáticos, generalmente infectando computadoras con un *malware* y obligándolas a unirse a una red maliciosa llamada botnet.

  Hay varias formas en que los atacantes informáticos pueden lanzar ataques de DDoS. Un método simple es obstruir la red con información sin sentido: tráfico que busca ralentizar significativamente el tiempo de respuesta del servidor. Otro método es generar paquetes falsos que contengan la

misma dirección IP para los campos de origen y destino. También, le piden al agente de diálogo que genere una respuesta muy larga y detallada para algunos tipos de solicitudes; por ejemplo, un atacante podría pedirle al módulo de generación de respuestas que le cuente una historia.

Si varias computadoras maliciosas hacen esta misma solicitud y engañan al servidor para que envíe todas estas respuestas a un usuario desprevenido, el tráfico resultante impedirá por completo todos los canales. Si se tarda mucho tiempo para encontrar una solución a este problema, esto afectará a cualquier aplicación que requiera una conexión de red, aún más si esta es compartida.

- **Contramedida:**

  Estos ataques no son exclusivos para las herramientas de chatbots, ya que apuntan a múltiples servicios disponibles en internet.

  Una técnica consiste en medir las propiedades estadísticas de los paquetes enviados a través de la red para que los administradores puedan usar esta información para guiar sus sistemas de detección de amenazas. Por ejemplo, se puede capturar la distribución de las direcciones IP de origen y compararla con la distribución anterior. Si la coincidencia es alta, seguramente el tráfico actual es legítimo. Si no, puede que alguien esté intentando realizar un ataque DDoS.

2.2.7.3 Módulo de generación de respuesta

- Ataques fuera del dominio

Considere un chatbot que está muy bien entrenado en algunos temas, pero carece de conocimiento autorizado sobre otros temas. Un adversario podría encontrar sistemáticamente estos puntos débiles en el chatbot

mediante ataques de fuerza bruta o incluso desarrollando una "red neuronal de sondeo". Esta podría estimar la confianza que el modelo de diálogo tiene en su respuesta.

Este tipo de ataque se le conoce como un ataque "fuera de dominio". Si los atacantes informáticos pueden explotar los ataques fuera del dominio con éxito, se podría causar un daño importante, ya que el comportamiento del chatbot para estos casos extremos puede ser muy impredecible.

Por ejemplo, si un adversario descubre que un chatbot de servicio al cliente diseñado para la reserva de vuelos no puede manejar bien los alquileres de automóviles, entonces los actores maliciosos podrían engañar a los usuarios para que divulguen información personal para alquilar un automóvil solo para que los atacantes roben su información.

- **Contramedida:**

  Para lograr una defensa adecuada contra los ataques fuera de dominio, debe de existir una manera para el que el chatbot pueda manejar su propio nivel de confianza sobre una respuesta.

  Para ejemplificar, un detector podría entrenarse para que clasifique ciertos tipos de solicitudes con respecto a si estas pertenecen al dominio o fuera del dominio. Sin embargo, el desafío es generar los datos de entrenamiento como un manual que se pueda usar como “etiquetado” para la clasificación o categorización, lo cual requiere de mucho tiempo y podría ser costoso.

  También, es posible abordar el tema generando automáticamente una manera en la que se pueda alterar de forma nativa como las redes neuronales del bot pueden cuantificar

incertidumbre y de esta manera mejorar la capacidad del modelo para determinar puntos de entrenamiento en el espacio de entrada y que permita diferenciar el tipo de consulta.

- Muestras de texto contradictorio

Los actores maliciosos pueden atacar directamente el módulo de generación de respuesta mediante la elaboración de mensajes de entrada inteligentes. Estos mensajes pueden hacer que el chatbot responda con información falsa, maliciosa o que utilice lenguaje ofensivo. Los ataques dirigidos a los sistemas de diálogo suelen elaborar una oración de entrada que puede romper el chatbot.

- **Contramedida:**

Para lidiar con este tipo de ataque se podría crear un agente encargado de predecir la oración de entrada correcta que va a desencadenar la correspondiente sentencia de salida. Después de este entrenamiento, el agente puede ser capaz de producir una sentencia de entrada que llevará al modelo de diálogo que podría utilizar el agresor como sentencia de salida.

Emplear un detector de “discurso de odio”, por esto, se puede entender como cualquier lenguaje negativo que fomente la animosidad entre usuarios. Cualquier oración que contenga palabras que inciten al odio serán filtradas automáticamente.

En la práctica, sin embargo, los detectores no son perfectos y tienen vulnerabilidades bien conocidas. Por ejemplo, no es necesario utilizar lenguaje soez explícito para elaborar un mensaje de odio, la

concordancia simple de palabras clave es insuficiente y nunca exhaustiva.

- Ataques a los modelos de lenguaje

El estado actual de los sistemas de procesamiento de lenguajes naturales (NLP) requiere el uso de modelos de lenguaje previamente entrenados. Recientemente, estos excelentes modelos han logrado hazañas impresionantes en áreas como la traducción automática neuronal, la clasificación de emociones y la detección de toxicidad. Esta ubicuidad hace que sea aún más importante que estos modelos de lenguaje sean lo suficientemente seguros para el uso directo de los chatbots.

Una de las formas en que los atacantes pueden explotar la confianza actual de la comunidad de chatbots en los modelos de lenguaje es generar modelos de NLP que pueden hacer que el sistema se comporte mal de otras formas muy específicas. Estos modelos de lenguaje maliciosos pueden terminar en el chatbot durante el desarrollo, dependiendo de si el programador se toma, o no, el tiempo de estudiar cada modelo.

Este es un ataque muy sofisticado debido al modelo de lenguaje. Sin embargo, este comportamiento podría considerarse sospechoso y disparar detonadores basados en análisis de modelo. Por ejemplo, dadas oraciones de entrada, el chatbot podría responder con lenguaje ofensivo.

- **Contramedida:**

La solución más simple contra estos ataques es adoptar las mejores prácticas en el desarrollo de chatbot. Antes de integrar cualquier modelo de lenguaje, se debe de llevar a cabo extensos procedimientos de verificación en ambientes de pre y postproducción. Adicionalmente,

se debe de garantizar que el modelo lingüístico ha sido difundido por una organización legítima y que futuras actualizaciones de este modelo de lenguaje tienen que ser verificadas.

Otro enfoque más sofisticado sería desarrollar una autodefensa en el algoritmo. Por ejemplo, que el algoritmo sea capaz de buscar palabras desencadenantes que puedan manipular al chatbot en el uso de lenguaje ofensivo. Una vez que esas palabras se detectan, el chatbot puede entrenarse de nuevo para limpiar esos factores que desencadenaron los mensajes no deseados o inclusive el modelo de lenguaje podría descartarse por completo.

- Ataque de ingeniería de retroalimentación

Estos ataques aprovechan las respuestas y la capacidad del módulo de generación para aprender de los usuarios. Muchos de los chatbots están diseñados de tal manera que puedan mantener conversaciones más atractivas con los usuarios a medida que pasa el tiempo porque pueden aprender las preferencias del usuario cuando se trata de temas de conversación. Sin embargo, un atacante podría aprovechar esto generando retroalimentación que induciría al chatbot en la dirección equivocada, como en la generación de discursos de odio.

Hay dos formas principales en que los chatbots están diseñados para mejorar a partir de la interacción del usuario:

1. **A través del reaprendizaje** - Su objetivo es volver a entrenar los sistemas de NLP de tal manera que las consultas normales se pueden responder como de costumbre, pero las oraciones de entrada con ciertas palabras desencadenantes provocarán un comportamiento

sospechoso. El desafío clave aquí es garantizar que estos factores desencadenantes no alerten al usuario ante cualquier actividad sospechosa.

2. **A través de aprendizaje reforzado** - Esencialmente se asume que el atacante tiene acceso completo al chatbot, de esta manera ellos pueden agregar una perturbación que será propagada en el ambiente. Esta perturbación selectiva puede empujar al agente hacia el aprendizaje de una política de elección del hacker.

- **Contramedida:**

  Es posible prevenirlos mediante la adopción de una variedad de soluciones, por ejemplo: en lugar de volver a entrenar al bot directamente en los mensajes, los desarrolladores pueden separar el módulo de generación de respuesta y los ejemplos de entrenamiento que se encuentran en el módulo de base de datos con una capa de abstracción que actuará como filtro.

  Para prevenir ataques contra un agente de aprendizaje por refuerzo, los desarrolladores deben tener en cuenta que en la práctica hay limitaciones en cuanto a la duración en la que un atacante puede perturbar las respuestas recibidas por el agente de diálogo. Si el contexto cambia o el agente es traído abajo para recibir actualizaciones, el atacante fallará en llevar a cabo su ataque.

2.2.7.4 Módulo de bases de datos

- Ataques de inyección SQL →

  Una vulnerabilidad clave en muchas aplicaciones que usan SQL como almacén de datos es un ataque de inyección. Estos ataques se basan en

entradas cuidadosamente diseñadas para obligar a la base de datos a funcionar y realizar operaciones no deseadas, como modificar información o devolver información sensible.

- **Contramedida:**

  El motivo principal de esta vulnerabilidad es la falta de validación de entrada. Por lo tanto, cualquier solución adecuada para estos ataques requieren como mínimo que el desarrollador invierta suficiente tiempo de limpieza y validación de datos.

  Si se busca optar por soluciones más sofisticadas, se pueden utilizar técnicas de análisis estáticos, dinámicos o algoritmos de aprendizaje automático. Por ejemplo, existe un algoritmo llamado WAVES, que busca en la aplicación cualquier lugar donde puede ocurrir un ataque de inyección y luego construye entradas inadecuadas basadas en patrones de ataques conocidos. Antes de implementar la aplicación, los desarrolladores del chatbot deben hacer que sea capaz de resistir los ataques generados por WAVES.

- Otras contramedidas →
  - **Firewalls de bases de datos**:

    Los firewalls pueden denegar tráfico por defecto, el único tráfico que se debe de permitir tiene que ser explícitamente permitido y desde aplicaciones o servicios que necesiten tener acceso a los datos en las bases de datos.

  - **Firewalls de Aplicaciones Web (WAF):**

    Se debe de implementar firewalls de aplicaciones web, ya que estos permiten analizar las consultas o las entradas realizadas, como las

generadas en un ataque de inyección de SQL que apuntarían hacia la aplicación web para filtrar información o borrar datos.

- **Fortalecimiento de Base de Datos**:

  Es importante verificar que la base de datos es aún soportada por el fabricante y que se esté ejecutando la última versión con todos los parches de seguridad instalados para remover vulnerabilidades conocidas. Adicionalmente, se debe de desinstalar o deshabilitar cualquier característica innecesaria o que no se esté utilizando.

  También, se debe de gestionar el cambio de contraseñas de cualquier cuenta y evitar los parámetros por defectos, o bien, deshabilitar por completo cuentas que no están siendo utilizadas.

  Finalmente, se recomienda garantizar que todos los controles de seguridad que hacen parte de la base de datos estén habilitados, si existe una razón específica para que alguna medida se encuentre deshabilitada, esta se debe de documentar e informar.

2.2.7.5 Amenazas generales

Existe una variedad de amenazas que podrían afectar la funcionalidad y correcta operación del chatbot o de alguno de sus módulos a nivel general. A continuación, se mencionan múltiples amenazas que tienen en común este tipo de afectación:

- Ransomware

  Como su nombre lo indica, el ransomware es un tipo de software malicioso que busca cifrar los archivos de la víctima y amenaza con exponer la información, para evitar esto, la organización o víctima afectada debe realizar el pago de una recompensa.

- *Malware*

  El *malware* es un tipo de software diseñado y codificado con la intención de generar daño o afectaciones a cualquier dispositivo o servidor dentro de un ambiente.

- *Phishing*

  El *phishing* se concibe como el acto malicioso de buscar información sensible de personas aparentando ser una entidad o institución legítima. Usualmente las personas pueden solicitar detalles de información sensible en este tipo de amenaza, como, por ejemplo: información personal, información bancaria, datos de tarjetas de crédito, entre otros.

- *Whaling*

  El *whaling* es similar al *phishing*, pero en este caso se busca información sensible de empleados experimentados de la organización o con altos cargos.

2.2.7.6 Contramedidas generales

Existen contramedidas establecidas como frecuentes prácticas para la protección de los chatbots. A continuación, se van a describir algunas de ellas:

- Asegurar el tráfico de la red →

  Es importante asegurar los datos generados por medio de los diferentes módulos y, a su vez, cómo este alcanza al usuario que realiza las consultas. Razón por la que se deben tomar en consideración protocolos criptográficos que permitan evitar el acceso a información por medio de un tercero no autorizado, así como la manipulación de información.

  Es importante entonces implementar cifrados de extremo a extremo y garantizar que la comunicación solamente se está dando a través de medios

seguros. Algunos de los ejemplos de estos protocolos considerados seguros son HTTPS y TLS.

- Mensajes auto destructibles

  Es posible eliminar cualquier tipo de información sensible conforme ya no es necesaria. Esto puede ser después de que el intercambio de mensajes acaba, o bien, después de un tiempo establecido. La información que podría ser eliminada por este tipo de mensajes hace referencia a las siguientes clasificaciones: información personal, identificadores, PINs, contraseñas, preguntas de seguridad y sus respuestas, entre otros.

- Minimizar la información valiosa

  Con esta contramedida se pretende asegurar que no se esté almacenando información confidencial que no debería de estar en la base de datos. Se debe de garantizar que aquellos datos retenidos, por temas de cumplimiento con regulaciones u otros propósitos, se muevan a un almacenamiento más seguro y adecuado, que sea menos susceptible a amenazas.

- Educación

  Las organizaciones o empresas deben de incentivar el uso adecuado de las herramientas que proveen a sus usuarios o clientes y de esta manera motivar la correcta utilización de las herramientas, así como limitar la exposición a amenazas. Sin embargo, un mal uso de las herramientas de chatbots podría llevar a una puerta trasera y al acceso de información inadecuada. Por lo que una organización o empresa debe asegurarse de que sus desarrolladores entiendan la relevancia de la seguridad del chatbot.

- Autenticación del Conector del Bot

Se deben de implementar mecanismos que permitan realizar la autenticación del conector o conectores utilizados en la arquitectura del chatbot. Existen kits de desarrollo de software (SDKs) que permiten automatizar la autenticación básica de bot a canal para la organización.

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

La investigación es clasificada como de tipo evaluativa, ya que se van a comparar aspectos presentes en las organizaciones tomando como base el uso de la tecnología de chatbot y las consideraciones que han tomado las organizaciones a nivel de ciberseguridad para garantizar la utilización segura de esas tecnologías. De igual manera, no se cuenta con un cliente particular, sino que se elegirá una muestra derivada del sector privado con la garantía de uso de tecnologías de chatbot en su ambiente.

3.2 Alcance Investigativo

En este caso, la investigación contempla dos tipos de alcance investigativo, los cuales son detallados a continuación:

- Exploratorio: Dado que la exploración, el estudio y la investigación sobre la aplicabilidad y las buenas prácticas de ciberseguridad sobre el uso de la tecnología de chatbots no es tan basto, también se busca examinar este tema. Se plantean múltiples cuestionamientos relacionados con los aspectos de seguridad que se deben de colocar o manejar en las organizaciones de cara al uso o interacción con estos de forma segura. Adicionalmente, actualmente en el país existen pocos esfuerzos evaluativos con respecto a ello.

- Descriptivo: Con esta investigación se pretende comprender las medidas de ciberseguridad aplicadas en las organizaciones del sector privado costarricense con respecto al uso de las tecnologías de chatbot. Como tal, se pretende también entender el contexto sobre el cual fueron tomadas las medidas y, poder exponer así, limitaciones que impiden a las organizaciones adoptar una ciberseguridad adecuada.

3.3 Enfoque

Para realizar a cabo esta investigación, se utilizará un enfoque cualitativo, recalcando aquellas características propias de las tecnologías de chatbots: tareas que típicamente puede lograr un usuario o un sistema a través de la interacción con estas tecnologías, información que es puesta a disposición de las herramientas para ser consultada, utilizada como mecanismo de respuesta y retroalimentación a quien interactúa como cliente y las características propias de los riesgos, amenazas y buenas prácticas de seguridad que ayuden a mitigar o reducir las dos primeras mencionadas.

La comprensión de estos diferentes elementos permitirá retroalimentar y robustecer la investigación, identificar el raciocinio detrás de la ejecución de controles a través de las conversaciones con los participantes del estudio para la recolección de la información que permitirá generar la propuesta resultante.

3.4 Diseño

Al tomar en consideración las diferentes características contempladas en los siguientes puntos mencionados previamente (Objetivos, Alcance investigativo y el Enfoque), se califica esta investigación como evaluativa, ya que pretende tomar como referencia la actual utilización de las tecnologías de inteligencia artificial, específicamente las de chatbots. Se busca realizar un análisis y una valoración de

los escenarios en los cuales esta tecnología es considerada para su empleabilidad, así como las condiciones relacionadas con ciberseguridad sobre las que se busca plasmar la seguridad del usuario final y de los datos que ellos manejan en sus interacciones, ya sea con seres humanos o bien con otros sistemas o procesos de la empresa del sector.

Esto permitirá a su vez identificar posibles riesgos, amenazas que puedan presentarse y crear una afectación. A partir de esto se busca realizar el análisis del estado actual que permita generar la propuesta final que contempla la enumeración de buenas prácticas y estrategias identificadas como oportunidades de mejora. Esta propuesta será entregada a las empresas correspondientes, por esta razón, se utilizará el Modelo Sensitivo o Respondiente de Robert Stake (1967), que consiste en dar respuesta a necesidades planteadas por audiencias que requieren la información. Su objetivo no solo consiste en recopilar información, sino comprender mejor el tema y resolver la necesidad inicialmente planteada.

3.5 Población y muestreo

Debido a que la investigación presenta un formato cualitativo y no se realizan mediciones de ninguna índole, no se tiene una referencia de población sobre la cual se estará recolectando un muestreo como tal. Dicho esto, se hace un acercamiento a expertos en el área y en la tecnología de chatbot y a empresas del sector privado que hagan uso de esta herramienta.

3.6 Instrumentos de recolección de datos

Barrantes (2002) describe la recolección de la información como un proceso en el cual se seleccionan y utilizan instrumentos para capturar los datos de la manera más exacta posible (medidas, valores, entre otros) y con ello alcanzar los objetivos propuestos.

3.6.1 Cuestionario

Con el fin de obtener la información relacionada sobre el uso de chatbots de forma segura, se utilizará un cuestionario predefinido (Tabla 10) que brinde la retroalimentación necesaria para poder efectuar el análisis de información correspondiente, esta encuesta será distribuida entre los participantes del sector y se dará un plazo para su realización.

Se usará la plataforma de Google Forms como medio para preparar y distribuir el cuestionario y, a la vez, tener acceso a las respuestas recibidas de manera centralizada, así como hacer uso de su forma de presentar las respuestas de manera visual, con gráficos

Descargo legal incluido en el cuestionario:

El presente cuestionario pretende recopilar información sobre el estado actual de la utilización, implementación y ejecución de los controles alrededor de la tecnología chatbot en el sector privado costarricense. La información obtenida a partir de las respuestas aquí recopiladas se mantendrá de forma anónima, sin ligamen para el individuo que la responde y el uso será única y exclusivamente con fines académicos para la retroalimentación en la generación de una propuesta de mejores prácticas en ciberseguridad para el mismo sector.

Tabla 10: Cuestionario a aplicar a empresas del sector privado que utilizan chatbots.

Preguntas	Opciones de respuesta	Resultado esperado
1. Indique en cuál industria del sector privado se desempeña.	( ) Financiero. ( ) Tecnología. ( ) Educación. ( ) Salud. ( ) Servicios. ( ) Transporte.	Recibir retroalimentación con el tipo de implementación más utilizado en las organizaciones, manejo de datos, controles de

Preguntas	Opciones de respuesta	Resultado esperado
	( ) Turismo. ( ) Mercadeo. ( ) Otro. Indique: _____	seguridad asociado y técnicas de validación de manejo de riesgos en industrias del sector privado costarricense.
2. ¿Qué tipo de implementación de chatbot posee su organización?	( ) Página web. ( ) App móvil. ( ) App IM/Chat. ( ) App inteligente. ( ) Otro. Indique: _____	
3. ¿El chatbot implementado en su organización fue desarrollado a lo interno o adquirido por medio de un tercero?	( ) Desarrollo interno. ( ) Tercero. ( ) Otros. Indique: _____	
3.1 Si se desarrolló interno: ¿Se contemplaron las buenas prácticas vigentes en la industria para el Ciclo de Vida de Desarrollo Seguro de Software (S-SDLC)?	( ) Sí. ( ) No.	
3.2 Si es de un tercero o contesta “Otros”: ¿Se consideró la seguridad como un aspecto importante de la evaluación de la solución?	( ) Sí. ( ) No.	
4. ¿Con qué tipo de servicios interactúa el chatbot de forma principal en su organización?	Indique: _____	
5. ¿La herramienta se está utilizando como parte de los procesos / funciones	( ) Sí. ( ) No.	

Preguntas	Opciones de respuesta	Resultado esperado
de ciberseguridad?		
6. En la implementación de chatbot existente, ¿se consideró el cifrado como un elemento indispensable para la comunicación y el manejo de datos en general?	( ) Sí. ( ) No.	
7. ¿La herramienta se utiliza para uso interno, externo o ambos?	( ) Interno. ( ) Externo. ( ) Ambos.	
8. ¿La información obtenida por medio del chatbot es utilizada como beneficio empresarial para la mejora de interacción, servicios o consumo con un tercero? Seleccione las que aplique.	( ) Mejora de interacción. ( ) Mejora de Servicios. ( ) Consumo de un tercero. ( ) Otro. Indique: _____	
9. ¿Existe actualmente en su organización algún documento o consentimiento informado que los usuarios deben aceptar al utilizar el chatbot?	( ) Sí. ( ) No.	
10. Indique cuales, de los siguientes controles de seguridad, se han implementado en su organización para la implementación segura de chatbots:	( ) Validación de entrada de información. ( ) Interacción segura con la BD. ( ) Autenticación de múltiples factores (MFA). ( ) Utilización de	

Preguntas	Opciones de respuesta	Resultado esperado
	certificados digitales. ( ) Almacenamiento seguro de la información recopilada. ( ) Cumplimiento con regulaciones nacionales. ( ) Cumplimiento con regulaciones internacionales. ( ) Buenas prácticas recomendadas por el fabricante. ( ) Manejo de errores y excepciones en el procesamiento de consultas y respuestas. ( ) Aplicaciones de parches de seguridad. ( ) Web Application Firewall (WAF). ( ) Load Balancer (LB). ( ) Next Generation Firewall (NGFW). ( ) Data Loss Prevention (DLP). ( ) Otro. Indique: _____	
11. ¿Cuáles de los siguientes mecanismos o técnicas utilizan en su organización para medir el nivel de riesgo de una solución chatbot?	( ) Pruebas de penetración (Pentesting). ( ) Análisis de vulnerabilidades. ( ) Ejecución en	

Preguntas	Opciones de respuesta	Resultado esperado
	ambientes controlados (Sandboxing). ( ) Entornos de preproducción y post producción. ( ) Pruebas de usabilidad. ( ) Pruebas de estrés. ( ) Otro. Indique: _____	
12. ¿Se está tomando en cuenta la privacidad de la información sensible de los usuarios en la utilización de chatbots?	( ) Sí. ( ) No.	
13. ¿Tienen los usuarios de su organización el derecho de solicitar la eliminación de sus datos personales de repositorios de almacenamiento utilizados por los chatbots, después de un periodo de tiempo?	( ) Sí. ( ) No.	
14. ¿La herramienta y los recursos de interacción propios de la misma (como el API) contienen características para control y manejo de tráfico a lo interno de la red?	( ) Sí. ( ) No.	

Fuente: Elaboración propia.

3.6.2 Entrevista

Este instrumento ayudará entender de forma más amplia, a través de preguntas abiertas, diferentes perspectivas sobre la motivación contemplada para emplear controles específicos, con el fin de proveer seguridad alrededor de chatbots. Esto nos permitirá enlazar con los resultados de los cuestionarios, para así poseer un panorama más diverso, enriqueciendo la propuesta.

De la misma manera, se utilizará este instrumento para obtener una opinión experta de actores enfocados en herramientas de asistentes virtuales o chatbots, con el propósito de obtener aportes que alimenten la propuesta final. En la Tabla 11, se señala una serie de preguntas dirigidas.

Tabla 11: *Entrevista a aplicar orientada a expertos.*

Preguntas	**Resultado esperado**
1. ¿Considera que en la actualidad las empresas están tomando las medidas de ciberseguridad adecuadas para la utilización de asistentes virtuales? Mencione algunas. 2. ¿Considera que es posible beneficiarse de las tecnologías de chatbots en la ciberseguridad? ¿Podría brindar ejemplos? 3. ¿Qué retos, en manejo seguro de datos, han encontrado cuando una organización desea implementar esta tecnología a nivel internacional? 4. ¿Considera que el uso de estas herramientas respeta y mantiene la privacidad de los usuarios y la información que ahí se comparte? ¿De qué manera? 5. ¿Tiene conocimiento de que en el país	Obtener retroalimentación con respecto al estado actual de la utilización de las herramientas, su relación con el manejo de datos de forma segura, los retos más importantes de ciberseguridad y recomendaciones de adopción e implementación con base en la experiencia y conocimiento de parte de los expertos.

Preguntas	Resultado esperado
existen regulaciones que velan por el cumplimiento del resguardo de la privacidad del usuario? Independiente de la respuesta, ¿qué elementos de la regulación considera importantes y por qué? 6. ¿Considera que, para la utilización de un chatbot, el usuario debe brindar de alguna manera un consentimiento informado? Resalte la importancia del porqué. a. ¿Se debe de contemplar, en este consentimiento informado, que la información recopilada a partir de un chatbot sea compartida con un tercero? b. ¿Se debe de contemplar que el usuario tenga el derecho de solicitar que se eliminen sus datos e información personal? 7. En su experiencia, ¿cuáles son los retos más importantes de ciberseguridad con respecto a los usuarios que utilizan este tipo de herramientas? 8. ¿Qué recomendaciones, para los procesos de adopción y educación en las organizaciones, daría para garantizar el cumplimiento de la política de uso adecuado?	

Fuente: Elaboración propia

3.7 Técnicas de análisis de información

Con el fin de poder evaluar de forma gráfica y analizar los datos recolectados a través de los cuestionarios realizados, se buscará efectuar un mapa conceptual

que contenga los diferentes elementos que son contemplados en la investigación y que son de interés para la evaluación correspondiente de oportunidades de mejora en el uso de tecnologías de chatbot de forma segura.

Adicionalmente, el mapa conceptual permitirá comprender y visualizar de mejor manera la información obtenida en relación con la utilización y los requerimientos previos a la adopción de estas tecnologías. Con esto, se buscará entender los problemas relacionados a la ciberseguridad que también nutrirán la propuesta de buenas prácticas.

En la Figura 14, se visualiza la manera en que se pretenden analizar los datos obtenidos:

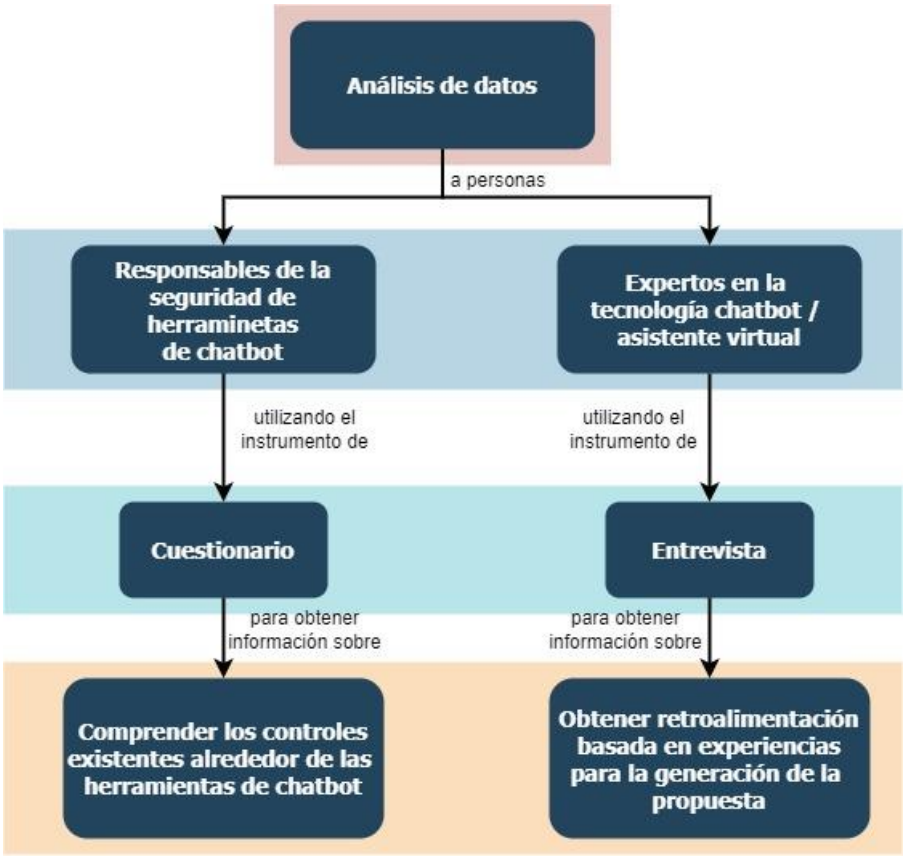

Figura 14: Mapa para el análisis de datos. Fuente: Elaboración propia. Elaborado usando el sitio draw.io

Capítulo 4. Análisis del Diagnóstico

4.1 Aplicación de entrevista y cuestionario

Como parte del proceso de análisis de la información y en conjunto con la información recopilada en el Capítulo 2, luego de aplicarse los instrumentos de recolección de información, se obtuvieron los siguientes resultados.

4.1.1 Aplicación de entrevistas a expertos en la tecnología de chatbot

Se realizó una entrevista a Ivonne Chaves Ríos, quien es arquitecta de soluciones con más de 12 años de experiencia en desarrollo de software, datos y nube. Además, ha sido ganadora en varios hackatones y speaker internacional reconocida en temas de tecnología. Actualmente trabaja como Business Program Manager & Technical Trainer – Data & Artificial Inteligence para la multinacional Microsoft.

En la Tabla 12, se presentan las respuestas obtenidas como parte de la entrevista.

Tabla 12: *Respuestas obtenidas en entrevista a Ivonne Chaves.*

Preguntas	**Respuestas**
1. ¿Considera que en la actualidad las empresas están tomando las medidas de ciberseguridad adecuadas para la utilización de asistentes virtuales? Mencione algunas.	Algunas sí, pero muchas no. Cuando las empresas están empezando a involucrar temas de Inteligencia Artificial, tratan de abarcar más de lo que pueden. No quieren solamente un chatbot para contestar preguntas frecuentes, sino además quieren llevarlo a ejecutar procesos de forma automatizada. Empiezan a correr antes de gatear. Y es donde empiezan a dejar muchos huecos. Las falencias normalmente vistas son: - Manejo de datos personales. - No se respetan normas como

Preguntas	Respuestas
	GDPR. En el área bancaria y de salud, si se ve mas preocupación pues no solo se rigen por las normas del país, sino también por normas e instituciones internacionales, como NIST. Recomendaciones para la ejecución y el uso de Inteligencia Artificial de forma responsable: 1. Que sea lo suficientemente inclusiva. 2. Transparente. 3. Accountability (quien lo hizo, quien lo tiene y por qué) 4. Privacidad y Seguridad 5. Reliability. 6. Sentimiento de seguridad al usar el bot. 7. Trato sin distinción al usuario. En caso de desarrollo, utilizar buenas prácticas de desarrollo desde el inicio.
2. ¿Considera que es posible beneficiarse de las tecnologías de chatbots en la ciberseguridad? ¿Podría brindar ejemplos?	Todo lo que realice o intervenga un ser humano y se pueda registrar procedimentalmente, se puede hacer a través de un chatbot. Por ejemplo, al llegar un correo que se cree malicioso, pero no hay total seguridad y existe la duda, es posible pasarlo a un chatbot o enviarle pantallazos, y este por debajo tiene un modelo de IA y este modelo “sustituye” la labor del personal de seguridad basándose en ciertas reglas que le han sido alimentadas; el proceso que seguiría la persona responsable del

Preguntas	Respuestas
	equipo de seguridad para revisar y verificar la situación. Al final el chatbot da una respuesta (basada en porcentajes) de que ese correo es 40% seguro. Basado en ese resultado, sería redirigirse a una política que indique como proceder basado en el porcentaje dado por la herramienta. Si es posible y ayudan, pero no es solamente el chatbot como tal, ya que este viene a ser como una interfase apoyada en Lenguaje Natural para ser lo más natural o humano posible. Lo importante es lo que está detrás de el: los modelos y la lógica; pues se va a tomar el input, procesarlo y dar un resultado. Tener el modelo correcto, entrenar el modelo correcto, capturar los insumos correctos y de la forma correcta. Tener conocimiento en UX, para poder tener la información correcta que le ayude al modelo usado a decir si algo es seguro o no.
3. ¿Qué retos, en manejo seguro de datos, han encontrado cuando una organización desea implementar esta tecnología a nivel internacional?	Adopción de estas tecnologías sin mostrar un descargo legal (disclaimer en inglés) al usuario final sobre el tipo de tratamiento y manejo que se le va a dar a los datos (si se va a usar para entrenar el modelo que se utiliza), donde va a estar esa data, la posibilidad del usuario de pedir no usar más la información brindada. tanto a usuarios propios de Costa Rica, como a usuarios internacionales. Es distinto acceder al Registro Nacional

Preguntas	Respuestas
	(en el caso de Costa Rica) y accedan a información pública a manejar datos personales como fecha de nacimiento, número de teléfono, nombre completo, como si fuera público.
4. ¿Considera que el uso de estas herramientas respeta y mantiene la privacidad de los usuarios y la información que ahí se comparte? ¿De qué manera?	Con base en la experiencia y herramientas utilizadas, si. Si la plataforma como tal ya presenta cumplimiento de distintas normativas (ISO, PCI), los bots que se utilicen dentro de estar plataformas heredan toda la robustez en la parte de seguridad y cumplimiento de normativas. Sin embargo, la seguridad es una responsabilidad compartida.
5. ¿Tiene conocimiento de que en el país existen regulaciones que velan por el cumplimiento del resguardo de la privacidad del usuario? Independiente de la respuesta, ¿qué elementos de la regulación considera importantes y por qué?	No específicamente de chatbots, pero todo aquello que apunte a una base de datos, debería estar registrada de forma correcta en la PROHAB y, por ende, manejarse con la sensibilidad debida. Esta la institución, está la ley. Hay regulaciones a través de reglamentos, pero no hay una actuación de forma reactiva tratando de regular la situación de muchas bases de datos o brindando algún tipo de lineamiento. El proceso de registro es un poco engorroso y las guías existentes son un poco ambiguas, no son muy claras. Hay regulaciones, pero no está la cultura. Mucho profesional no tiene conocimiento y no ha existido una buena divulgación.

Preguntas	Respuestas
	Elementos importantes de la regulación: Más allá de tener un ente rector, que la regulación tenga una estructura clara de los medios correctos donde poner las denuncias. Además, las implicaciones legales y promoción de la legislación como tal. Hacer entender la importancia de los datos, saber cuándo si dar los datos y si los damos saber que tratamiento van a tener esos datos.
6. ¿Considera que, para la utilización de un chatbot, el usuario debe brindar de alguna manera un consentimiento informado? Resalte la importancia del porqué.	Por supuesto.
a. ¿Se debe de contemplar, en este consentimiento informado, que la información recopilada a partir de un chatbot sea compartida con un tercero?	Definitivamente. Poniendo un ejemplo desde el punto de vista bancario, un banco “X” que es parte de un conglomerado “XYZ”, ellos se ven como uno solo, pero desde el punto de vista jurídico, el otro es un tercero. Si se comparten información o hacen algún tipo de *cross-sharing*, ya lo estarían utilizando como un tercero.
b. ¿Se debe de contemplar que el usuario tenga el derecho de solicitar que se eliminen sus datos e información personal?	Si, los datos son propiedad de cada uno y se debe tener la posibilidad de hacer esta solicitud en el momento que uno así lo desee.
7. En su experiencia, ¿cuáles son los retos más importantes de ciberseguridad con respecto a los usuarios que utilizan este tipo de herramientas?	La educación, pero en dos vías: 1. Del usuario final → no dimensiona y comparte información sensible como contraseñas. Deben entender que no hay que compartir esta información aun que se la soliciten sin importar el medio, en especial un chatbot porque piensan que “de por sí, es

Preguntas	Respuestas
	una maquina y ya la tenía”. 2. El desarrollador/programador del chatbot → tener la ética de no pedir esta información por este medio. Que los desarrolladores entiendan que no están programando algo transaccional, sino buscando que interactúe de la manera más natural con los clientes. Pedir solamente la información que se necesita, pero a la vez, evitar recibir información que no se debería y, de recibirla, tener la capacidad (algún modelo, algún servicio cognitivo) que notifique que se está compartiendo algo que no se debería compartir, como la contraseña.
8. ¿Qué recomendaciones, para los procesos de adopción y educación en las organizaciones, daría para garantizar el cumplimiento de la política de uso adecuado?	Mas allá de una política, debe de empezarse aún más atrás. Desde la escuela y colegio, hacer entender que es la ciberseguridad, por que debo de estar protegiendo mis datos, porque no debo de compartir algo tan básico como el PIN del celular (para desbloquearlo) con todo el mundo; para que cuando se sea más grande, ese impacto no sea tanto. A pesar de que los Centennials (Generación Z) ya vienen muy de la mano con la tecnología, son los más imprudentes a la hora de manejar sus datos, son sumamente confiados, a pesar de estar anuentes a los peligros que hay, lo cual se vuelve muy irónico.

Preguntas	Respuestas
	A nivel de empresas, donde se tiene una mezcla de estas generaciones, desde Baby Boomers hasta algunos Centennials inclusive, se debe tener una estrategia por cada una de estas generaciones. Además, estas políticas deben estar dirigidas según el sector y la información que va a estar tratando (según su puesto). Es diferente la información que recibe un cajero de un banco, a un cajero de un super mercado. En resumen, cultura para todos los niveles y tener presente la seguridad como un punto de suma importancia.

Fuente: Elaboración propia.

Se realizó una entrevista adicional a Gerardo Chaves, arquitecto de soluciones de software y colaborador de la empresa Cisco Systems con 28 años de experiencia en la industria.

En la Tabla 13, se presentan las respuestas obtenidas como parte de la entrevista.

Tabla 13: *Respuestas obtenidas en entrevista a Gerardo Chaves.*

Preguntas	Respuestas
1. ¿Considera que en la actualidad las empresas están tomando las medidas de ciberseguridad adecuadas para la utilización de asistentes virtuales? Mencione algunas.	Hasta ahora los que se han utilizado en servicios como la banca, telecomunicaciones, internet, me parece que sí, lo cual no es muy sorprendente pues lo hacen como una extensión de su página web. Soluciones como Whatsapp ofrecen sus propias opciones/soluciones de seguridad como el cifrado de extremo a extremo. Sin embargo, lo que se considera que no se está manejando de forma adecuada por las organizaciones es el manejo de PII. Como usuarios, no

Preguntas	Respuestas
	sabemos de qué manera está manejando las empresas los datos personales y el usuario común tiene la costumbre de compartir más información de la cuenta. Si se tiene embebido en la página web, se podría pensar que se están ejecutando los mismos controles que se encuentran en la página. Se deben de tener consideraciones con respecto al uso de NLP de terceros y el almacenamiento de información en ese tercero, garantizar que el NLP se tiene conocimiento de donde se almacena la información en sí. La interacción entre los diferentes módulos del chatbot tiene que ser completamente protegido, mediante cifrado y otras técnicas de seguridad. Se debe de implementar controles que restrinjan los elementos esperados y aceptados por el chatbot de forma que se limite la posibilidad de fallas o manejo inadecuado en la interacción por medio de la validación de contenido. Implementar el chatbot primeramente en un ambiente de sandbox, que permita realizar inspección de calidad de uso del mismo y su correcta operación. Garantizar el cumplimiento de regulaciones o políticas como PCI, GDPR, etc.
2. ¿Considera que es posible beneficiarse de las tecnologías de chatbots en la ciberseguridad? ¿Podría brindar ejemplos?	Podría beneficiarse en la utilización de características propias del chatbot, como, por ejemplo: ▪ La detección de la velocidad a la que escribe el usuario. ▪ Detectar si la identidad que está escribiendo es realmente una persona y descartar que sea una suplantación de identidad por medio de otro robot. A un chatbot no se le puede aplicar ingeniería social al mismo nivel que a un agente de servicios. Sin embargo, un agente puede detectar rápidamente un comportamiento sospechoso.
3. ¿Qué retos, en manejo seguro de datos, han encontrado cuando una	Cumplimiento de regulaciones o políticas, tomar en cuenta de dónde se

Preguntas	Respuestas
organización desea implementar esta tecnología a nivel internacional?	saca la información y donde se va a almacenar. Asegurarse de que los diferentes elementos de interacción del chatbot estén en un mismo lugar o al menos en un lugar donde su interacción sea permitida por las leyes o regulaciones involucradas.
4. ¿Considera que el uso de estas herramientas respeta y mantiene la privacidad de los usuarios y la información que ahí se comparte? ¿De qué manera?	No sabe, no le consta. Sin embargo, como usuario no existe confianza al 100%. Se le pasa información al chatbot para que resuelva de acuerdo con lo necesario y nada más. El usuario no sabe determinar que está hablando con un chatbot por lo que muchas veces brindan más información de la necesaria y personal. Eventualmente podrían existir agentes que busquen obtener información sensitiva de las personas.
5. ¿Tiene conocimiento de que en el país existen regulaciones que velan por el cumplimiento del resguardo de la privacidad del usuario? Independiente de la respuesta, ¿qué elementos de la regulación considera importantes y por qué?	Si, las regulaciones deberían de incluir a los chatbots en las mismas.
6. ¿Considera que, para la utilización de un chatbot, el usuario debe brindar de alguna manera un consentimiento informado? Resalte la importancia del porqué.	Si, para que el usuario sea consciente de que no debería compartir más de lo necesario.
a. ¿Se debe de contemplar, en este consentimiento informado, que la información recopilada a partir de un chatbot sea compartida con un tercero?	Si, se debería de pedir autorización al usuario y no tomarlo por sentado.
b. ¿Se debe de contemplar que el usuario tenga el derecho de solicitar que se eliminen sus datos e información personal?	Si, el usuario debería de poder solicitar la eliminación de información personal, es un principio adecuado.
7. En su experiencia, ¿cuáles son los retos más importantes de ciberseguridad con respecto a los usuarios que utilizan este tipo de	Ya esta pregunta fue contestada previamente en la #1.

Preguntas	Respuestas
herramientas?	
8. ¿Qué recomendaciones, para los procesos de adopción y educación en las organizaciones, daría para garantizar el cumplimiento de la política de uso adecuado?	El chatbot es una interfaz, las recomendaciones que existen actualmente con respecto al uso de páginas o herramientas web, no debería de inventarse una categoría 100% nueva. Las empresas deberían de tener el chatbot identificado a nivel de la red y el tráfico que el mismo genera. Limitar el tipo de chatbots que se pueden utilizar y solamente permitir la herramienta oficial de la empresa. Asegurar que los chatbots que entreguen contenido tengan filtros de grado de contenido. Se podría clasificar el contenido o la información de la empresa y que el chatbot aplique filtros de contenido de acuerdo con esto a la hora de entregar información. Se debe de limitar la información que se puede compartir con entidades externas en caso de que la herramienta sea también de uso externo. Utilizar soluciones de DLP y monitoreo de tráfico de salida. Se debe de implementar verificación de autenticación de múltiples factores para garantizar que es utilizado solo por individuos de la empresa.

Fuente: Elaboración propia.

4.1.2 Análisis de datos recopilados a partir de las entrevistas a expertos

En la presente sección se analizan las respuestas brindadas por parte de los expertos entrevistados. A partir de este análisis, se busca relacionar sus aportes con la información plasmada en la sección 2.2.7 Vulnerabilidades, amenazas, riesgos de seguridad y contramedidas aplicables en la tecnología chatbot, donde se discuten vulnerabilidades, riesgos y contramedidas, para que, de esta manera, se pueda

consolidar la información que retroalimenta la propuesta final de buenas prácticas en ciberseguridad.

Es de suma relevancia hacer notar que ambos expertos consideran los siguientes aspectos de extrema importancia:

- Protección y privacidad de datos.
- Cifrado de datos de extremo a extremo.
- Autenticación de usuarios.
- Consideración de regulaciones nacionales e internacionales a la hora de determinar los controles que se colocarán y el manejo adecuado de información.
- Se dan recomendaciones para la ejecución y uso de la tecnología de forma responsable que contemplan los siguientes aspectos:
    - Que sea lo suficientemente inclusiva.
    - Transparente.
    - Que guarde el registro de la toma de acciones y el no repudio.
    - Sentimiento de seguridad y confianza al usar el bot.
    - Trato igualitario al utilizar la solución.
    - Proveer un consentimiento informado al usuario para el manejo de su información a través de la herramienta.
    - Almacenamiento seguro de la información.
    - Eliminación de información sensible del usuario cuando este así lo requiera.

Ambos mencionan desconocer sobre la existencia de regulaciones o leyes orientadas a colocar medidas en la utilización de chatbots a nivel nacional.

Adicionalmente, resaltan la importancia de garantizar que el chatbot maneje información de forma limitada, que valide las consultas y las respuestas de una manera preestablecida que permita garantizar que el bot no distribuirá más información de la cuenta y que no será víctima de ingeniería social, que respete y maneje de forma adecuada la información personal de los usuarios garantizando la protección de estos.

Se recomienda también garantizar que el usuario final, consumidor del chatbot, no pueda diferenciar de que está hablando con un bot. Se sugiere utilizar mecanismos de autenticación mutua y de autenticación de múltiples factores entre los actores de la comunicación, así como la validación de que el lenguaje natural de procesamiento (NLP) utilizado provenga de una fuente confiable.

En la entrevista se realizó una pregunta orientada al descubrimiento y verificación sobre la posible implementación de este tipo de soluciones a nivel de ciberseguridad y cómo podría mejorar la detección de riesgos, vulnerabilidades, amenazas y explotaciones, por lo que sugieren aprovechar el chatbot para detectar la velocidad a la que escribe un usuario, y así detectar si quien escribe realmente es una persona o si existe una suplantación de identidad.

En adición, concuerdan en que todo en lo que intervenga un ser humano y se pueda registrar procedimentalmente, es posible realizarlo a través de un chatbot; para esto, plantean el siguiente ejemplo:

> Al llegar un correo que se cree malicioso, pero no hay total seguridad y existe la duda, es posible pasarlo a un chatbot o enviarle pantallazos, y este por debajo tiene un modelo de IA y este modelo “sustituye” la labor del personal de seguridad basándose en ciertas reglas que le han sido alimentadas; el proceso que seguiría la persona responsable del equipo de seguridad para

revisar y verificar la situación” (I. Chaves, comunicación personal, 31 de marzo del 2022)

En resumen, las medidas sugeridas y puntualizadas por los expertos van de la mano con los riesgos y las contramedidas indicadas en la sección 2.2.7 Vulnerabilidades, amenazas, riesgos de seguridad y contramedidas aplicables en la tecnología chatbot. Además, los entrevistados realizaron sugerencias adicionales con respecto al funcionamiento propio de la solución y del proceso de interacción con el ser humano.

4.1.3 Aplicación de cuestionario a gestores de la herramienta

Se envió el cuestionario a diferentes empresas de distintas industrias del sector privado y se brindó un tiempo prudencial para el llenado de este.

4.1.4 Análisis de resultados de la encuesta a gestores de la herramienta

Se analizan las respuestas obtenidas en cada uno de los cuestionarios y se realiza una reflexión al respecto para poder utilizarlas como referencias adicionales para la propuesta. Los gráficos usados a continuación, se obtienen por la facilidad de la herramienta de Google Forms y su manera amigable de presentar visualmente la información.

- Respuestas Pregunta 1.

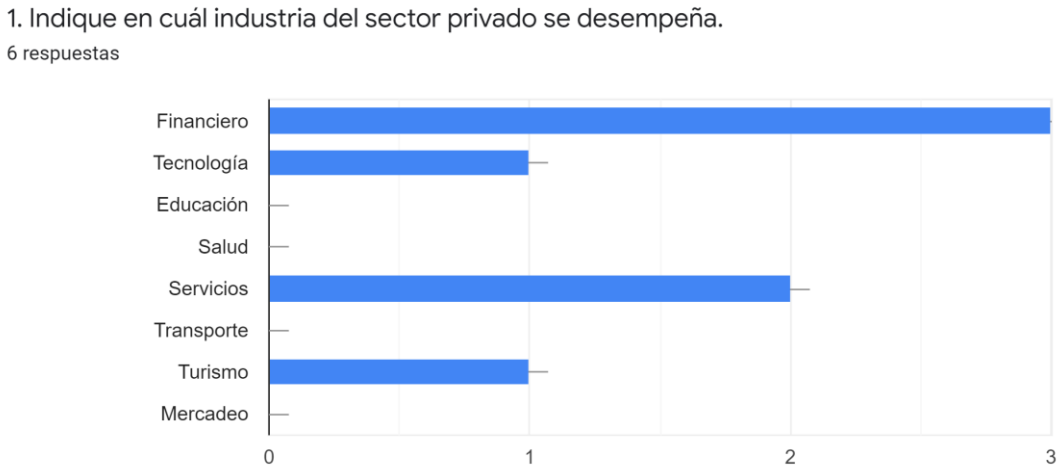

Figura 15: Respuestas pregunta 1 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Con respecto a la obtención de respuestas para el cuestionario, mayoritariamente se obtuvieron de empresas del sector financiero y en segundo lugar el sector de servicios. Esto permite observar una mayor adopción de este tipo de tecnología en empresas que buscan brindar servicio al cliente y atención mediante consultas frecuentes.

- Respuestas Pregunta 2

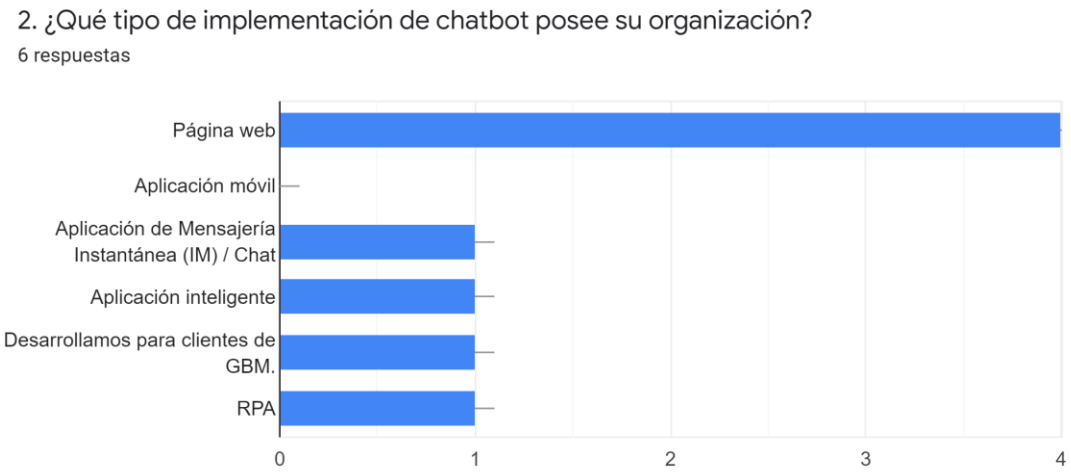

Figura 16: Respuestas pregunta 2 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Se muestra que el tipo de implementación predominante es mediante la utilización de una página o sitio web como punto de interacción. Adicionalmente, se corrobora la existencia de otros tipos de implementaciones, por ejemplo, a nivel de aplicaciones de mensajería, aplicaciones inteligentes y se evidencia que también existen desarrollos personalizados de acuerdo con los requerimientos específicos de quienes requieran servicios de este tipo de solución. Respuestas pregunta 3

Figura 17: Respuestas pregunta 3 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

A partir de los resultados, se evidencia una preferencia evidente con respecto a la adquisición por medio de un tercero con respecto a la posibilidad de un desarrollo interno, esto podría ser debido a que muchas empresas deciden delegar la responsabilidad del desarrollo del chatbot, ya sea por causa de una falencia de conocimiento o por otros motivos. Sin embargo, algunas empresas sí optan por el desarrollo propio de sus chatbots.

- Respuestas pregunta 3.1

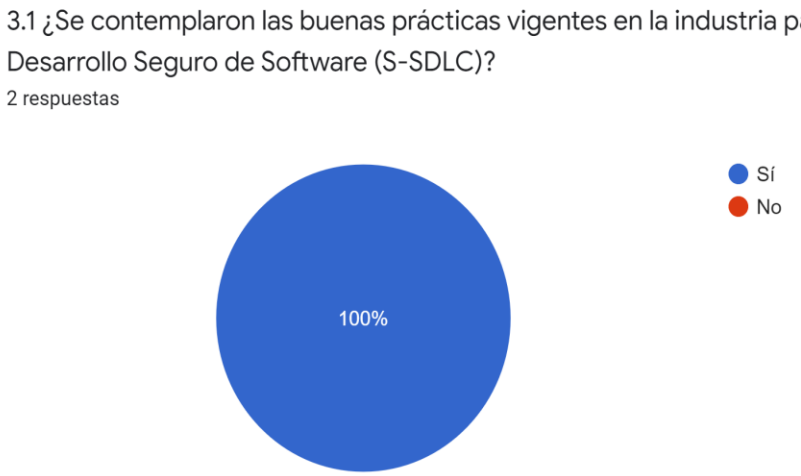

Figura 18: Respuestas pregunta 3.1 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Esta pregunta es únicamente para los que contestaron que el chatbot implementado en la empresa fue un desarrollo interno. Aquellas empresas que deciden desarrollar sus chatbots internamente confirman utilizar buenas prácticas relacionadas con el Ciclo de Vida de desarrollo seguro de software (S-SDLC).

- Respuestas pregunta 3.2

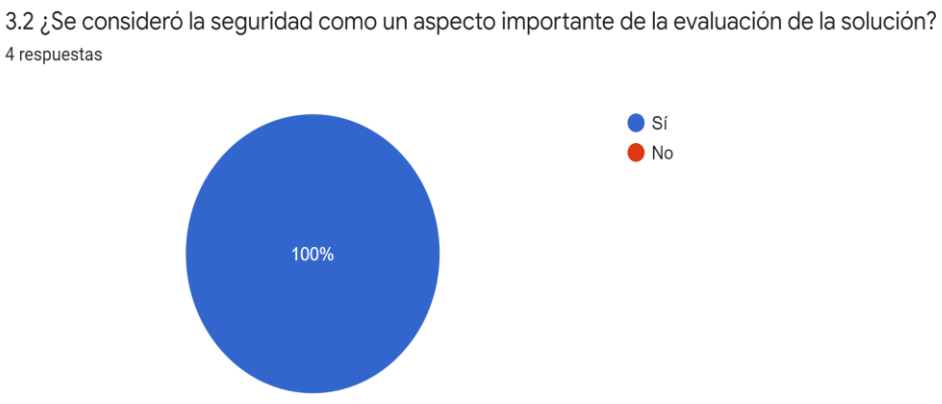

Figura 19: Respuestas pregunta 3.2 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Esta pregunta es únicamente para los que responden que el chatbot fue adquirido por medio de un tercero, Se indica que la seguridad sí fue considerada como un elemento importante del proceso de evaluación a la hora de seleccionar el tipo de despliegue que se llevaría a cabo.

- Respuestas pregunta 4

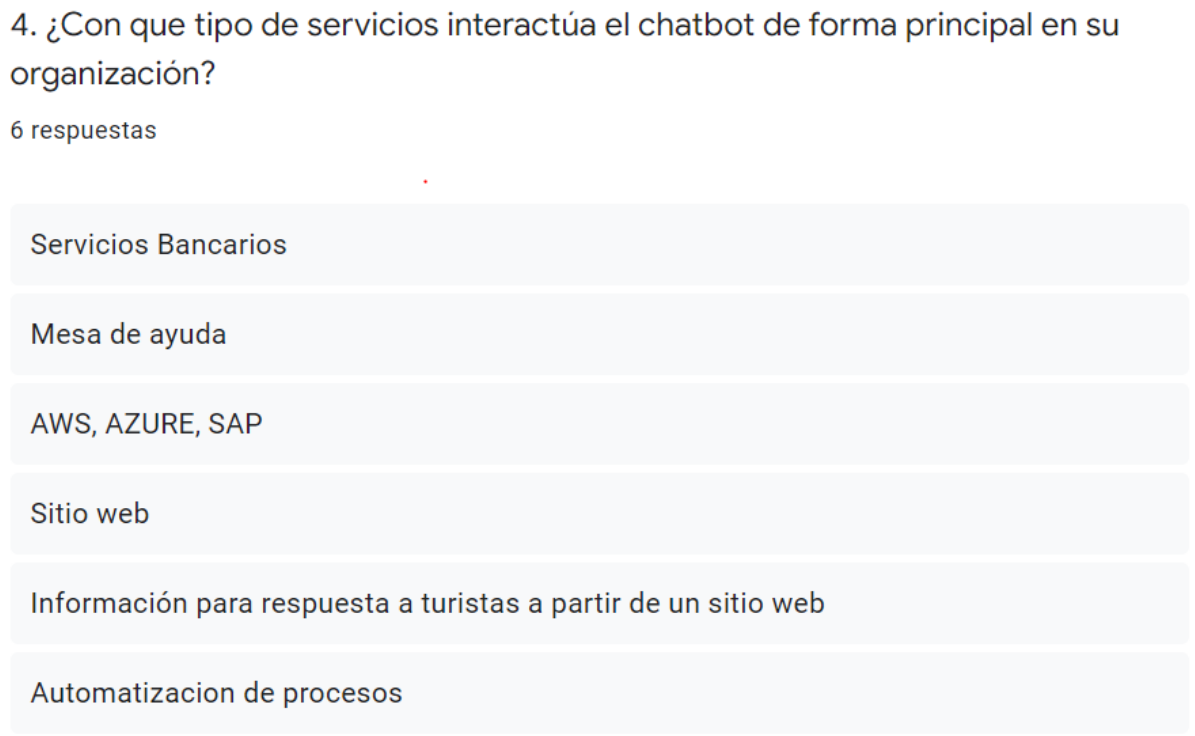

Figura 20: Respuestas pregunta 4 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Esta pregunta resalta que la utilización de los chatbots no va enfocada solamente a un tipo de casos de uso, sino que las organizaciones pueden aprovechar su versatilidad para aplicarlo en diferentes tareas, procesos y objetivos. Esto les permite facilitar sus procesos de negocio, atención al cliente, entrega de información y optimización de recursos. Se debe de considerar la superficie de ataque relacionada con la implementación de la solución, buscando la mejor manera

de resguardar de principio a fin el proceso de interacción, acceso a la información, almacenamiento de esta, entre otros.

- Respuestas pregunta 5

Figura 21: Respuestas pregunta 5 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Las respuestas a esta pregunta demuestran que existe una oportunidad de exploración en la utilización de este tipo de soluciones en ambientes de ciberseguridad para brindar apoyo en la respuesta con respecto a procesos u obtención de información que pueda disminuir tiempos de acción, por ejemplo: Tiempo promedio a detección (MTTD) y tiempo promedio a respuesta (MTTR).

- Respuestas pregunta 6

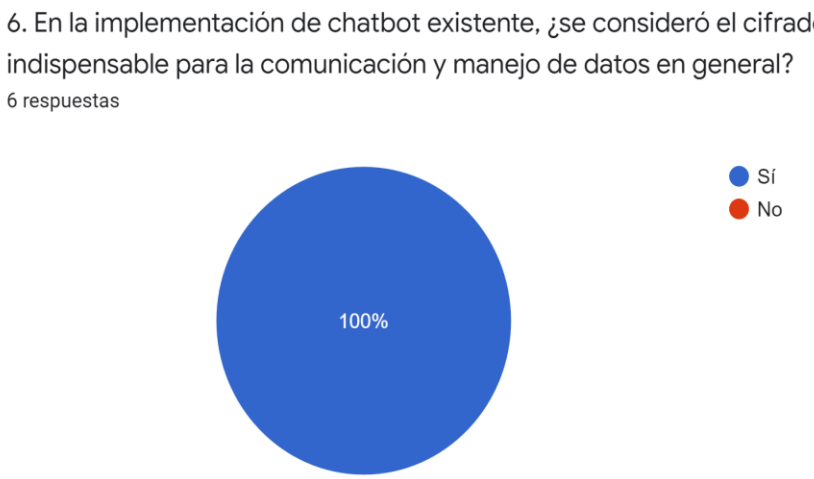

Figura 22: Respuestas pregunta 6 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Todos los involucrados consideran que el cifrado es un elemento indispensable para la protección y el resguardo de la información que va a manejar el chatbot.

- Respuestas pregunta 7

Figura 23: Respuestas pregunta 7 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Existe una mayor interacción desde los usuarios externos hacia el chatbot, sin embargo, se da también la implementación de ambos tipos de comunicación en una sola organización, lo que resalta la versatilidad de la tecnología. Por último, no se obtuvieron respuestas de interacción exclusivamente interna, por lo que se propondrá explorar estos casos de uso.

- Respuestas pregunta 8

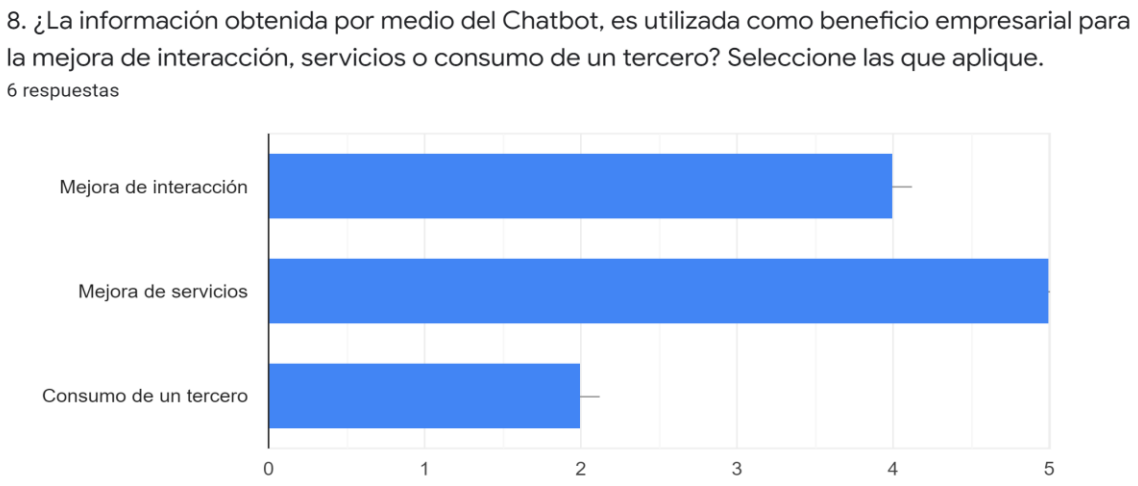

Figura 24: Respuestas pregunta 8 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Existe un mayor beneficio empresarial derivado de la utilización de esta solución para la mejora de la interacción y la mejora de servicios por parte de la empresa. Por otro lado, hay un aprovechamiento de esta para el consumo de un tercero, lo que puede plantear riesgos que deben de ser tomados en cuenta y que han sido analizados a lo largo de la investigación.

- Respuestas pregunta 9

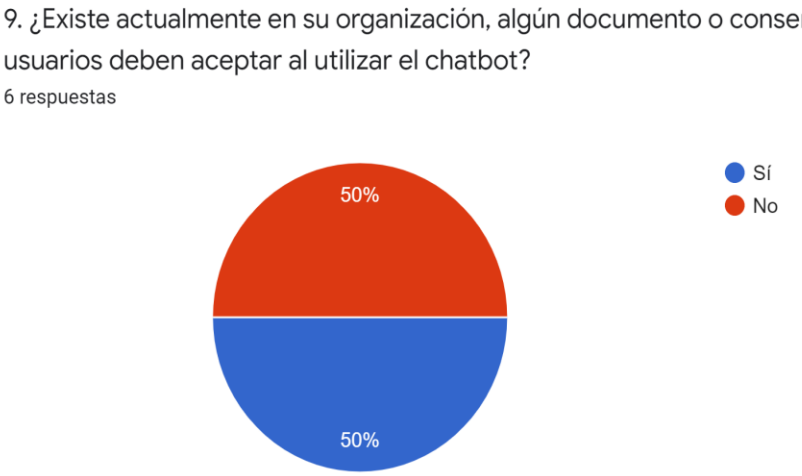

Figura 25: Respuestas pregunta 9 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Existe un balance en la implementación actual de un consentimiento informado que el usuario debe de aceptar previo a la utilización de la solución. Es importante recalcar e informar al usuario sobre el uso que se le dará a sus datos y cómo estos serán manejados.

- Respuestas pregunta 10

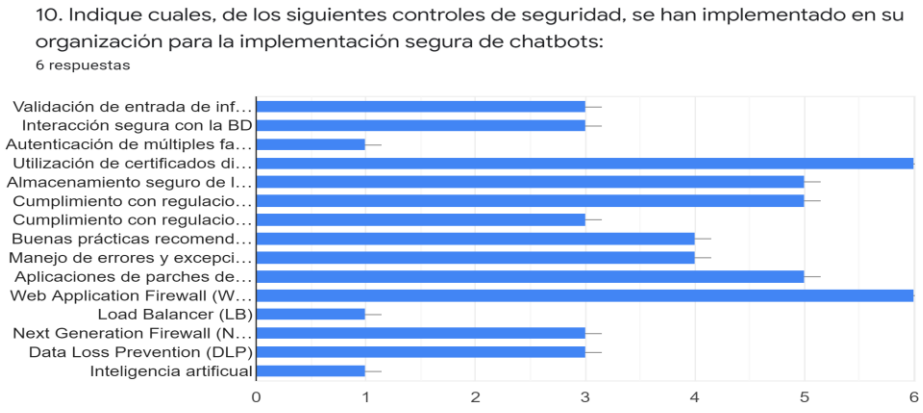

Figura 26: Respuestas pregunta 10 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Como se puede observar, se han implementado diversos controles de seguridad que buscan resguardar los diferentes elementos que hacen parte de la solución chatbot, sus procesos de interacción y el acceso a la información que estos manejan. Pero, estos controles no están implementados a un mismo nivel en cada sector, por lo que existe una oportunidad de mejora para otras de las organizaciones cuestionadas con el objetivo de estandarizar controles y brindar una defensa a profundidad como principio básico de las buenas prácticas de ciberseguridad.

Al considerar como base los resultados de la pregunta #1, y las respuestas brindadas, se interpreta que el sector financiero, que maneja información con un valor mayoritario en términos económicos (debido a la naturaleza de sus operaciones), indica colocar la mayor cantidad de controles alrededor de las soluciones de chatbot.

- Respuestas pregunta 11

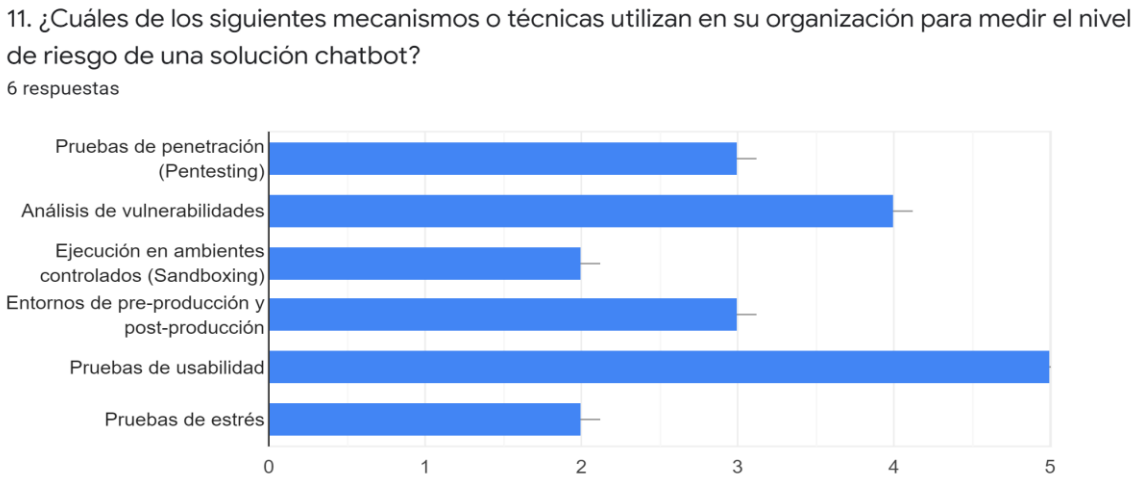

Figura 27: Respuestas pregunta 11 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Dentro de los mecanismos o técnicas para medir el nivel de riesgo y la calidad de los controles aplicados a nivel de ciberseguridad, predominan las pruebas de usabilidad, esto más que todo para garantizar la calidad de experiencia del usuario y evitar errores inesperados.

En segundo lugar, existe una preferencia por la realización de análisis de vulnerabilidades, pruebas de penetración, y entornos de pre/post producción, siendo los primeros mecanismos de verificación activa de controles mediante el intento de identificación de falencias en la ciberseguridad o de elementos que se puedan aprovechar por un actor malicioso para comprometer los activos. Los entornos de pre/post producción suelen estar relacionados con la correcta ejecución de los servicios de la solución y la garantía de que estos no van a derivar un problema en algún otro servicio, pero también son utilizados para la mejora en la validación de entradas, manejo de errores y excepciones.

Se evidencia que es necesario contemplar a un mayor nivel de detalle los límites y las situaciones en donde por una cantidad de solicitudes superior a las que las capacidades de recursos permiten se vea comprometida la disponibilidad de la herramienta y, por ende, todos los procesos asociados con esta.

Por último, el sector financiero, de nuevo, como en los resultados de la pregunta #10, es quien mayoritariamente hace uso y aprovechamiento de los mecanismos o técnicas para medir el riesgo de este tipo de tecnología y garantizar su disminución.

- Respuestas pregunta 12

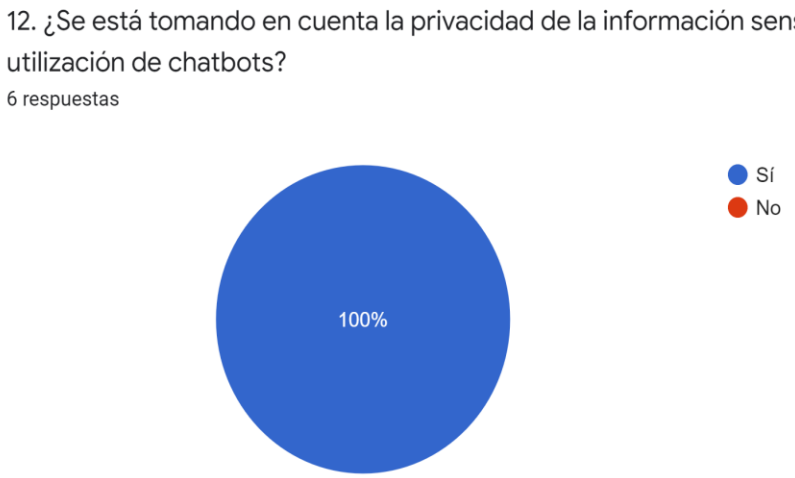

Figura 28: Respuestas pregunta 12 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

La totalidad de empresas consultadas indica que la privacidad de los usuarios que interactúan con la tecnología es tomada en cuenta en el manejo de información sensible.

- Respuestas pregunta 13

Figura 29: Respuestas pregunta 13 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

Algunas de las empresas indican que actualmente están brindando a los usuarios la posibilidad de eliminar los datos personales recopilados por ellos. Es

importante brindar esta opción para que el usuario pueda ser capaz de solicitar la eliminación de sus datos después de un tiempo que debería de establecerse en el consentimiento informado o en el momento en el que sus datos ya no sean requeridos.

Por tanto, para aquellas organizaciones que aún no lo han implementado, se recomienda hacerlo.

- Respuestas pregunta 14

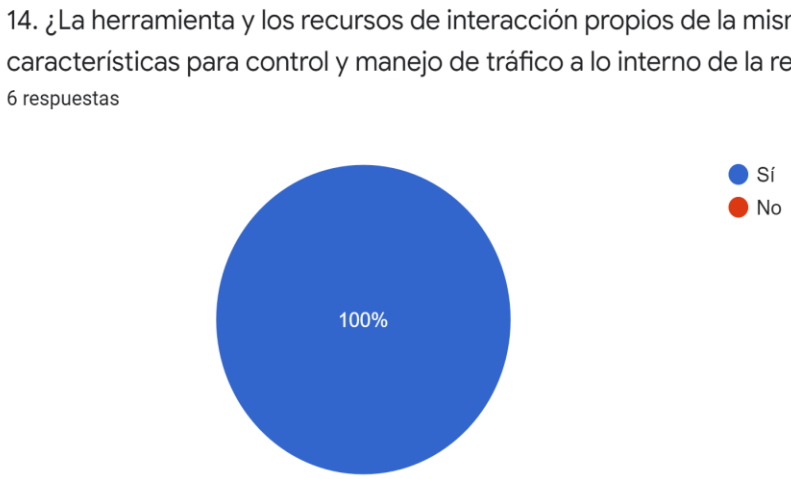

Figura 30: Respuestas pregunta 14 del cuestionario. Fuente: Elaboración propia. Datos procedentes de encuesta aplicada.

La totalidad de las empresas indican que utilizan un mecanismo de control y manejo de tráfico a lo interno de la red. Este punto es importante para poder realizar un seguimiento de las transacciones y comunicaciones realizadas por el chatbot, así como para poder colocar capas de protección a lo largo de la superficie de ataque cubierta por esta.

De acuerdo con lo analizado y la reflexión inicial de cada una de las preguntas, se obtiene como resultado de este cuestionario que existe una base

adecuada para el desarrollo, implementación, interacción, manejo de información y protección de datos. Sin embargo, hay oportunidades de mejora, tanto en la exploración de casos de uso, específicamente relacionados con la ciberseguridad, como en los modelos de implementación e interacción de la plataforma y en la aplicación de controles para poder cubrir de una manera más profunda y adecuada la superficie de ataque de los chatbots.

Adicionalmente, es importante valorar y considerar los mecanismos de validación para asegurar que estos controles estén trabajando de una manera adecuada mediante diferentes técnicas y actualizaciones.

Por último, pero no menos importante, se insta a las organizaciones a buscar la implementación de un proceso adecuado para la remoción de los datos sensibles de un usuario cuando ya no son requeridos, esto a través de una solicitud explícita a partir de lo estipulado en el consentimiento informado y que es recomendado tener.

En él, también debe de indicarse el periodo a partir del cual un usuario podría realizar tal solicitud. Adicionalmente, se deben de mantener las capacidades de seguridad que busquen resguardar al usuario, la información, los activos de la organización que ya se encuentran en ejecución y garantizar que se continúen aplicando las mejores prácticas de desarrollo de software seguro en aquellos escenarios donde aplique.

Capítulo 5. Propuesta de Solución

En este capítulo, se presenta la propuesta final de buenas prácticas de ciberseguridad en la utilización de chatbots para el sector privado costarricense, se resalta que la intención de este proyecto es cubrir una falencia de investigaciones y bases aplicadas a nivel nacional.

Adicionalmente, proveer una referencia sólida de medidas y controles de seguridad que permitan disminuir la superficie de ataque relacionada con la tecnología chatbot, para que, de esta manera, la tecnología pueda ser implementada y utilizada, contemplando la disminución de riesgo asociado, y así poder mantener los servicios e interacciones con el resguardo apropiado.

Para esto se utilizarán, principalmente, los resultados obtenidos en las secciones 2.2.7 Vulnerabilidades, amenazas, riesgos de seguridad y contramedidas aplicables en la tecnología chatbot, 4.1.2 Análisis de datos recopilados a partir de las entrevistas a expertos y 4.1.4 Análisis de resultados de la encuesta a gestores de la herramienta.

5.1 Buenas prácticas en ciberseguridad para el uso de chatbots

Los problemas de seguridad siempre están presentes con las nuevas tecnologías y traen consigo nuevas amenazas y vulnerabilidades. Aunque los chatbots son una tecnología emergente, los métodos de seguridad que los respaldan existen desde hace mucho tiempo y son muy efectivos.

Los chatbots son un desarrollo innovador de la era actual, y las tecnologías emergentes, como la inteligencia artificial, están cambiando la forma en que las empresas pueden interactuar con sus clientes, por lo que mantenerlos seguros debe de ser una revisión constante y una prioridad para las organizaciones.

A continuación, se describirán las recomendaciones de buenas prácticas de ciberseguridad a nivel de uso, implementación, vulnerabilidades, amenazas, contramedidas y verificación de estas con relación a la tecnología chatbot.

5.1.1 Generalidades sobre recomendaciones en el uso de chatbots y mejoras en la experiencia del usuario

Para un uso correcto de la solución de chatbots y mejorar en la interacción con el usuario, se debe de contemplar lo siguiente:

- Ser lo suficientemente inclusiva con el usuario. Las soluciones de IA deben empoderar e involucrar a todos las personas, asegurándose de ser intencionalmente inclusivo, tener un trato igualitario al interactuar y ser diverso al cubrir el espectro completo de comunidades. (Microsoft, s.f.)
- Ser lo más transparente posible. Esto quiere decir que estas soluciones deben ser comprensibles, lo cual también ayuda a los desarrolladores a resolver problemas relacionados con sus propios desarrollos.

  Parte de esta transparencia quiere decir que los encargados de crear soluciones deben ser abiertos de cómo y por qué están utilizando la inteligencia artificial, pero también ser abiertos con la limitación de sus sistemas. Por otro lado, las personas deben ser capaces de entender el comportamiento de las soluciones de inteligencia artificial. (Microsoft, s.f.)
- Guardar el registro de la toma de acciones y el no repudio.
- Transmitir un sentimiento de seguridad y confianza al utilizarse. (Microsoft, s.f.)
- Proveer de un consentimiento informado al usuario para su entendimiento con respecto al manejo de su información.
- Brindar la opción de eliminar datos sensibles cuando el usuario lo requiera y estos ya no sean necesarios.
- Considerar regulaciones nacionales e internacionales sobre el manejo de datos.

Adicionalmente, se plantean los siguientes puntos:

- Considerar si realmente el chatbot es necesario: identificar el problema que se busca resolver, determinar si se puede automatizar un proceso, si se pueden cubrir las necesidades del usuario, o si se puede colocar un canal disponible y manejable para los usuarios.
- Ralentizar el proceso de respuestas para que el usuario no pierda confianza en la interacción por causa de respuestas que se obtengan excesivamente rápido. Debe de considerarse una pausa antes de brindar la respuesta a la consulta realizada.
- Delimitar el alcance que tendrá la solución con sus usuarios. Es importante no brindar acceso a más información o recursos que a los estrictamente necesarios.
- A los usuarios les gusta obtener respuestas y mantener una conversación concisa, por lo que respuestas muy elaboradas o extensas pueden llevar a la frustración y a la insatisfacción.
- Contemplar que sus usuarios no desean detectar que están hablando con un bot, lo que podría ser frustrante para ellos. Para esto, considerar los elementos, comportamiento típico de una conversación humana y cómo esto puede ser incorporado y aplicado en la interacción.
- Determinar el momento adecuado en el que el chatbot debe de transferir la conversación a un humano.
- Asegurarse de entrenar de forma adecuada al bot para utilizar ejemplos de conversaciones que tendrá.
- Observar a sus usuarios. Realizar pruebas de usabilidad que permitan garantizar la satisfacción de sus usuarios en el proceso de interacción.

- Validar que el lenguaje natural de procesamiento que utilizará provenga de una fuente confiable y verificar su desarrollador.
- Utilizar mensajes auto destructibles para eliminar información sensible conforme ya no sea necesaria, o bien, después de un tiempo establecido.
- Motivar la utilización correcta de las herramientas y limitar la exposición a amenazas.
- Utilizar el aprendizaje de máquina para predecir la oración de entrada que desencadenará una sentencia de salida. De esta manera se pueden prevenir ataques de ingeniería social aplicados a los chatbots y se establece el comportamiento esperado por estos.
- Educar al usuario en la identificación de posibles amenazas e intentos de estafa.

5.1.2 Mecanismos de ciberseguridad para la protección de chatbots

Se proponen, a continuación, algunos mecanismos de ciberseguridad que la organización debe de contemplar para la protección de la arquitectura utilizada y sus procesos relacionados. En la Figura 31 se muestra una representación general para su mejor visualización.

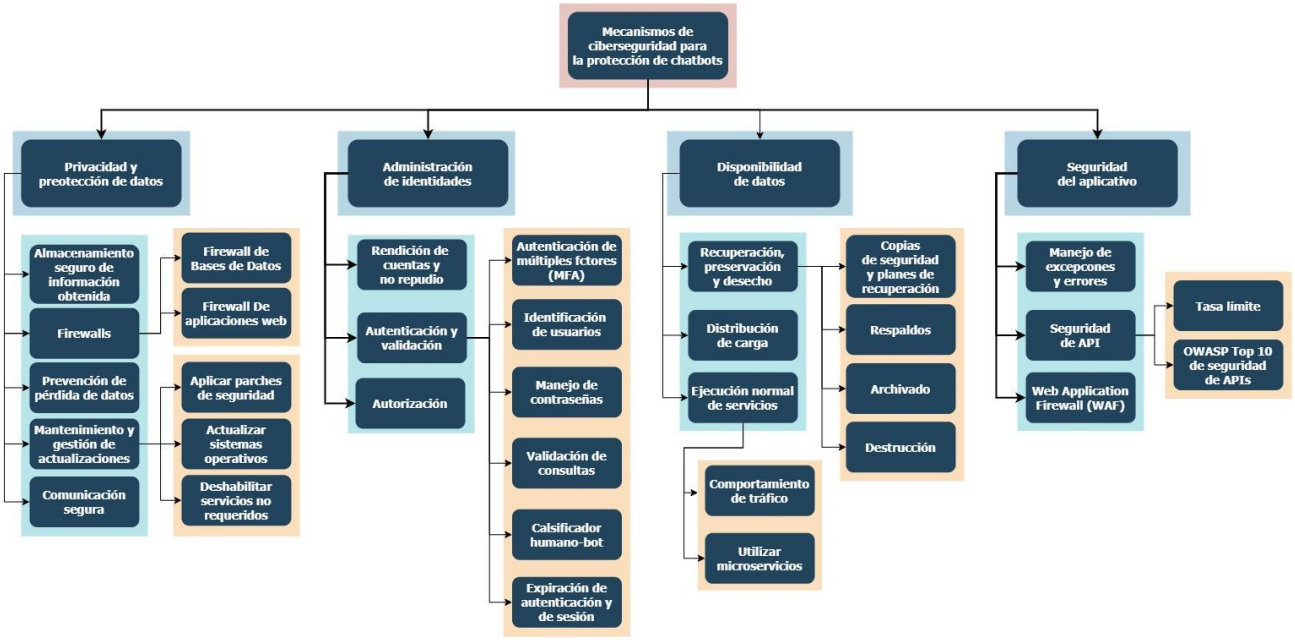

Figura 31: Mecanismos de ciberseguridad para la protección de chatbots. Fuente: Elaboración propia. Elaborado usando el sitio draw.io

5.1.2.1 Privacidad y protección de datos

La tecnología, en general, ha abierto nuevos caminos que pueden provocar la filtración de datos, los cuales pueden acabar en manos no deseadas. La privacidad es crucial, y mucho más al considerar la información que se cataloga como información de identificación personal (personally identifiable information, PII por sus siglas en inglés), como historial médico, número de cédula, preferencias, orientación o hábitos sexuales, origen étnico, datos biométricos, por mencionar algunos.

Por esta razón, es que se recomienda utilizar los siguientes ejemplos de controles y medidas para resguardar la privacidad y la protección de los datos.

<u>Cifrado</u>

Cifrar la comunicación de extremo a extremo. Utilizar métodos y algoritmos recomendados, para esto se debe de verificar periódicamente cuáles son estos algoritmos y garantizar dónde son necesarios, y que se tenga el soporte, la compatibilidad y la implementación adecuada de estos.

Almacenamiento seguro de información obtenida

Para esto, primero se debe de contemplar la clasificación correcta de la información para comprender su nivel de sensibilidad o criticidad, entender cuál será la ubicación y los tipos de dispositivos que serán permitidos para el almacenamiento y el uso de la información según la clasificación otorgada. Por último, se debe de considerar el cifrado de la información en reposo.

Firewalls

- **Implementar firewalls de bases de datos**. Para poder proteger la base de datos, la información allí almacenada y filtrar las consultas hacia o desde esta. Estos deben de implementarse en la red o directamente a nivel de la base de datos.
- **Firewalls de próxima generación para filtrar el tráfico de red.** Este tipo de firewalls son considerados de próxima generación, pues reúnen servicios que previamente eran ofrecidos por plataformas independientes. Servicios como sistemas de prevención y detección de intrusiones (IPS / IDS), inspección de archivos, filtrado de URLs, políticas de control de tráfico por identidad y descifrado de tráfico HTTPS o TLS, son ahora implementados a nivel de una sola plataforma. Esto permite brindar una protección más completa contra las amenazas que se puedan presentar sobre la red y que busquen comprometer las comunicaciones desde y hacia los diferentes elementos de la arquitectura a nivel de chatbot.

Comunicación segura

Utilizar protocolos de comunicación como HTTPS y TLS. Esta para que sea segura debe de realizar, por ejemplo: una verificación de integridad en la comunicación, es decir, que los datos no hayan sido alterados por un tercero;

también, autenticación de pares, ocultar la información a un tercero no deseado mediante la confidencialidad y el no repudio, que se refiere a la capacidad de omitir que una identidad pretenda prescindir de su responsabilidad en un proceso en el que sea involucrado en la comunicación.

Además, utilizar certificados digitales, para demostrar el aseguramiento de la comunicación con el servidor esperado, típicamente utilizados a nivel de comunicaciones sobre HTTPS, entre otros. Son un elemento crucial de la infraestructura de llaves públicas (PKI por sus siglas en inglés) y hasta la fecha dan garantía de ser un mecanismo ideal para los procesos de autenticación, integridad, confidencialidad y no repudio. Estos utilizan algoritmos robustos designados por los administradores e identifican los pares en la comunicación.

Prevención de pérdida de datos

En la búsqueda para resguardar la información sensible o privada de una organización, se deben considerar soluciones que permitan identificar este tipo de información con base en diferentes técnicas, como la detección de patrones, utilización de expresiones regulares e, inclusive, la detección de tipos de archivos; que permiten evitar la filtración de información hacia un tercero no autorizado que pueda usar esta información para otros fines no pretendidos.

Mantenimiento y gestión de actualizaciones

- **Aplicar parches de seguridad.** Es importante mantener los sistemas lo más actualizados posibles, al igual que los programas o aplicativos que forman parte de estos. Es necesario referirse a actualizaciones liberadas por parte de los desarrolladores o fabricantes para poder disminuir la superficie de ataque y poder contrarrestar vulnerabilidades descubiertas e implementar mejoras a nivel de sistema.

Actualizar sistemas operativos. Se debe de mantener el sistema lo más orientado a las recomendaciones propias de los fabricantes o desarrolladores. Esto para lograr la estabilidad, disponibilidad del sistema, y para evitar conflictos entre versiones o debilidades propias del sistema operativo, así como también para que este cuente con el respaldo del fabricante y el soporte para la resolución de problemas. Se deben de mantener los sistemas actualizados, ya que con ellos típicamente vienen parches de seguridad o mejoras a nivel de la seguridad propias del sistema que apoyarán en el proceso de resguardo de información y protección de los recursos que dependan del sistema operativo.

- **Deshabilitar servicios no requeridos.** Es recomendable realizar una determinación de los servicios, puertos de comunicación e interacciones entre sistemas que serán permitidas. De esta manera, se pueden identificar servicios, procesos, y comunicaciones anómalas que buscan comprometer y abusar del sistema o programa, lo cual puede ocasionar que se le dé un uso o acceso inadecuado que pueda derivar en una afectación mayor.
  Asimismo, esa base de conocimiento sobre lo que es “normal” puede apoyar en la detección de anomalías y procesos de respuesta ante una amenaza.

5.1.2.2 Administración de identidades

El manejo de identidades garantiza que solo las personas autorizadas tengan acceso a los recursos tecnológicos que necesitan para realizar sus funciones. Abarca políticas y tecnologías que incluyen procesos en la empresa para identificar, autenticar y autorizar correctamente a personas, grupos de personas o aplicaciones, al utilizar atributos que otorgan derechos de acceso y restricciones a los usuarios en función de su identidad.

Autenticación y validación

- **Autenticación de múltiples factores.** Verificar a los usuarios mediante autenticación de múltiples factores, requiriendo que los usuarios demuestren su identidad proporcionando al menos dos pruebas o factores al iniciar sesión. Algo que el usuario conoce, como nombre y contraseña; y algo que el usuario posee, como una clave de seguridad física.
- **Identificación de usuarios**. Los usuarios deben de estar correctamente identificados y no deben de utilizar una identidad genérica, por ejemplo, un usuario común para todos los accesos de los diferentes gestores, como el usuario “Administrador”.
- **Manejo de contraseñas.** Se deben de tener contraseñas robustas, definidas bajo una mínima aceptación que contemple la longitud mínima, combinaciones y caracteres aceptados. Adicionalmente, estipular el periodo durante el cual la contraseña será vigente. Esta política de contraseñas debe de ser actualizada y revisada periódicamente.
- **Validación de consultas.** Validar las consultas realizadas por ambas partes en el proceso de comunicación, para detectar un intento de suplantación de identidad y afectación a la contraparte. Se recomienda tener una base de consultas “regulares” o esperadas por la aplicación, para poder mapear una consulta directamente hacia una respuesta típica según la interpretación de la organización y así evitar cualquier tipo de filtro de información o comportamiento no deseado.
- **Clasificador humano-bot.** Utilizar un clasificador de humano a bot para determinar si realmente la comunicación se está dando con un humano. Estos clasificadores pueden poner a prueba características propias de la

comunicación realizada por un chatbot para determinar si la interacción se da con otra inteligencia artificial, o bien, con un ser humano. Para esto, se puede medir el tiempo de respuesta, consultas no genéricas, palabras clave, entre otros.

- **Expiración de autenticación y sesión.** Generar expiraciones de tiempo en la autenticación y la sesión. De esta manera se pueden evitar afectaciones a nivel de continuidad de la aplicación; por ejemplo, si un usuario no está realmente utilizando un canal de comunicación, este se pueda liberar para que otro usuario que realmente necesita el servicio pueda aprovecharlo.

Autorización

Utilizar los mecanismos para brindar la autorización correspondiente al chatbot y al usuario de forma adecuada. Referenciar el principio del privilegio mínimo, aplicar roles y políticas a los usuarios para definir permisos adecuados de acuerdo con la necesidad de saber del usuario y características mínimas para que pueda realizar sus tareas. Además, debe de haber una correcta identificación de roles y responsabilidades asociadas para cada tarea en la aplicación.

Evitar el uso de cuentas y usuarios privilegiados. Se debe de utilizar, en lugar de ellas, cuentas específicas e independientes que vayan de acuerdo con roles y responsabilidades requeridas para que la identidad pueda desempeñarse adecuadamente, mientras que las cuentas privilegiadas deben de ser resguardadas por los encargados de área.

Rendición de cuentas y no repudio

Asegurar que los controles guarden un registro de acciones y garanticen el no repudio. Esto permitirá determinar quién tomó qué acción, realizar un proceso de

auditoría adecuado, que el usuario no pueda negar haber tomado una acción y que se tenga un registro histórico sobre la administración y consumo de la aplicación.

Revisar y auditar de forma periódica la base de usuarios aún presentes en la organización y sus permisos. Todo esto para evitar que un usuario que ya no se encuentra desempeñando sus funciones tenga accesos o permisos que puedan derivar en una afectación.

5.1.2.3 Disponibilidad de datos

Esta es la característica o habilidad que asegura el acceso confiable y oportuno a los datos y los recursos que los respaldan por parte de personas autorizadas, con el fin de prevenir afectaciones que limiten la ejecución normal de servicios, el acceso a estos, la recuperación de información y su archivado, así como la distribución de cargas de forma adecuada para optimizar la experiencia del usuario.

<u>Ejecución normal de servicios</u>

- **Comportamiento de tráfico.** Medir las estadísticas de paquetes enviados a través de la red por la solución mediante una herramienta de analítica de red, para así poder tener una base de conocimiento y detectar una anomalía de forma oportuna. De esta manera se pueden evitar ataques que busquen inhabilitar los servicios que otorga la aplicación, conocidos como denegaciones de servicio (DoS, por sus siglas en inglés).
- **Utilizar microservicios**. Separar los componentes del chatbot para que una falla, compromiso o una afectación general, no se transforme en una limitante de la disponibilidad del servicio en su totalidad.

<u>Distribución de cargas</u>

Utilizar balanceadores de carga para evitar la saturación de recursos. Mediante este tipo de solución se distribuyen las solicitudes de acuerdo con la capacidad,

carga y otras condiciones, para que los elementos que actualmente manejan los recursos asociados a la solución puedan comportarse de una mejor manera. Adicionalmente, se evita el consumo desmedido, se mejora el manejo de peticiones y respuestas en cada uno de los elementos.

Recuperación, preservación y desecho

- **Copias de seguridad y planes de recuperación.** Las copias de seguridad y los planes de recuperación permiten tener la capacidad para restaurar las operaciones de forma parcial o total. Esto requiere de un planeamiento adecuado que contemple qué información será copiada, dónde y cómo debe de restablecerse.
- **Respaldos.** Los respaldos permiten recuperar información en caso de una afectación al ambiente productivo, lo que proporciona que los sistemas, la información o los programas vuelvan a su estado original, y dar así continuidad a los procesos y operaciones. Es importante que estos respaldos se almacenen en ubicaciones distintas de donde se encuentra la información, los sistemas o los programas productivos, así como colocar medidas equivalentes a las existentes para resguardarlos.
- **Archivado.** Archivar de manera segura la información que se debe conservar y los registros de actividad como garantía del cumplimento legal o normativo que se requiera. Típicamente, regulaciones internacionales con las que las organizaciones deben de cumplir solicitan el archivo de información por un periodo determinado. Por ende, realizar el archivado de información permite tener acceso a esta cuando se requiera y manejar un histórico que debe de ser resguardado de la misma manera que la información que aún no está siendo archivada.

- **Destrucción.** Destruir de manera segura la información, una vez terminada su vida útil. Es un mecanismo que permite garantizar que la información no va a ser accesada por un tercero no autorizado.

5.1.2.4 Seguridad del aplicativo

Sin importar si el chabot es un desarrollo propio o de un tercero, se debe verificar y garantizar que las mejores prácticas descritas en el ciclo de vida de desarrollo seguro de software (S-SDLC) están siendo contempladas. Este ciclo sigue varias etapas, como la definición de alcance (*Scope*), definición de la solución (*Definitions*), definición de antecedentes (*Background*) y modelos de capacidad de madurez (*Capability Maturity Models*).

Cada una de estas etapas define pasos y procesos que deben de ser tomados en cuenta para realizar el desarrollo seguro de cualquier solución de software, incluyendo chatbots.

Otras consideraciones de seguridad que se deben de contemplar como parte del desarrollo de un chatbot son las siguientes:

Manejo de excepciones y errores

Realizar una verificación con respecto al manejo de errores y excepciones a nivel de la herramienta según su tipo de implementación. Esta medida permite identificar un evento no esperado, invalidado o no permitido según la designación del administrador de la solución, y así evitar brindar información, respuestas o que la solución cree un comportamiento que podría generar una afectación en el proceso esperado.

Seguridad de API

- **Tasas límite**. Establecer una tasa límite para la API y el acceso al controlador. Ambos son un componente esencial de la seguridad de las

aplicaciones, ya que los ataques DoS pueden abrumar un servidor con una solicitud de API ilimitada.

Por otra parte, permitir el acceso al controlador compromete toda la integridad de la solución y su comportamiento. Se deben de implementar mecanismos descritos en la sección 5.1.2.2 Administración de identidades para evitar esta afectación.

- **OWASP Top 10 de seguridad de APIs**. Se debe de revisar de forma continua el OWASP Top 10 de seguridad de APIs para la seguridad de su implementación. Desde la banca, el comercio, el transporte, el Internet de las cosas (IoT), los vehículos autónomos y las ciudades inteligentes, las API son una parte esencial de las aplicaciones web y móviles de hoy, y se pueden encontrar tanto en las aplicaciones raíz como en el cliente.

  Por su propia naturaleza, las API exponen la lógica de la aplicación y los datos confidenciales, como la información de identificación personal (PII), y, por lo tanto, son cada vez más un objetivo para los atacantes. Sin API seguras, sería imposible innovar rápidamente. Es por esto que el proyecto sin fines de lucro, Open Web Application Security Project (OWASP), trabaja para mejorar la seguridad del software, al crear una lista de las 10 amenazas más frecuentes, las cuales son verificadas y revisadas periódicamente para comprender su nivel de riesgo y qué contramedidas se deben de aplicar para mitigarlas.

Web Application Firewall (WAF)

Estos ayudan a proteger las aplicaciones web al filtrar y monitorear el tráfico HTTP entre la aplicación web e Internet. Por lo general, protege las aplicaciones

web de ataques como la suplantación de identidad web, los archivos adjuntos y la inyección de SQL.

Este método de prevención de ataques a menudo forma parte de un conjunto de herramientas que, en conjunto, crean una defensa integral contra varios vectores de ataque. Al implementarlo, se coloca un intermediario entre la aplicación web e Internet.

5.1.3 Comprobación de problemas de ciberseguridad

Se enumeran las técnicas propuestas para la comprobación de problemas de ciberseguridad y se describen los roles típicamente encontrados en una estructura organizacional de un departamento de Seguridad de Información, para brindar al lector una referencia base sobre las responsabilidades generales de dichas técnicas.

Las técnicas por mencionar deben de realizarse de acuerdo con los resultados que el implementador espera recibir y los objetivos de negocio definidos en el alcance de la comprobación de controles de cada organización. Por lo tanto, estas se pueden ejecutar en paralelo, de forma conjunta o independiente, pero siempre tomando en cuenta una correcta planificación, así como definiciones para los objetivos esperados.

5.1.3.1 Descripción de roles

Director o directora de seguridad de la información. CISO (Chief Information Security Officer, por sus siglas en inglés). Es un rol de nivel gerencial, cuya función principal es alinear la seguridad de la información con los objetivos de negocio, asegurando la protección adecuada de la información de la empresa.

Algunas de sus responsabilidades incluyen desarrollar e implementar políticas de seguridad de la información, garantizar la seguridad y protección de los

datos, supervisar la administración del control de acceso a la información, ser el responsable del equipo de respuesta a incidentes de seguridad de la información y supervisar la arquitectura de seguridad de la información, por mencionar algunas.

Gerente de ciberseguridad. Responsable de administrar los miembros que conforman el equipo de seguridad de la información, así como las tecnologías y herramientas utilizadas por el equipo.

Arquitectos o arquitectas de ciberseguridad. Un arquitecto de seguridad es responsable de crear estructuras de seguridad complejas para garantizar que los sistemas informáticos permanezcan seguros. Debe de tener una comprensión y conocimiento profundos de la tecnología y los sistemas de información de la organización, para proporcionar el nivel adecuado de seguridad.

Ingeniero o ingeniera de ciberseguridad. Algunas de las responsabilidades incluyen la creación de nuevas soluciones para resolver problemas de seguridad existentes, mejorar las capacidades de seguridad evaluando nuevas tecnologías y procesos, la definición, implementación y mantenimiento de políticas corporativas de seguridad,

configuración e instalación de firewalls y sistemas de detección de intrusos, supervisar cambios en software, hardware, instalaciones, telecomunicaciones y necesidades de los usuarios, así como brindar apoyo recomendando modificaciones en áreas legales, técnicas y regulatorias que afecten la seguridad informática.

Analista de ciberseguridad. Un analista de ciberseguridad detecta amenazas cibernéticas y busca implementar cambios necesarios para proteger la organización. Administrar y configurar herramientas de monitoreo de actividad de red, analizar informes de dichas herramientas para identificar comportamiento inusual en la red,

planificar y recomendar cambios para mejorar la seguridad de la red y aplicar parches de seguridad para esta.

***Penetration tester*.** Este también es conocido como hacker ético y se encarga de explotar las vulnerabilidades del Sistema o la red, justo como un hacker lo haría. Deben documentar y registrar los resultados de las pruebas realizadas.

En la Figura 32 se muestra a manera de jerarquía los roles mencionados y definidos.

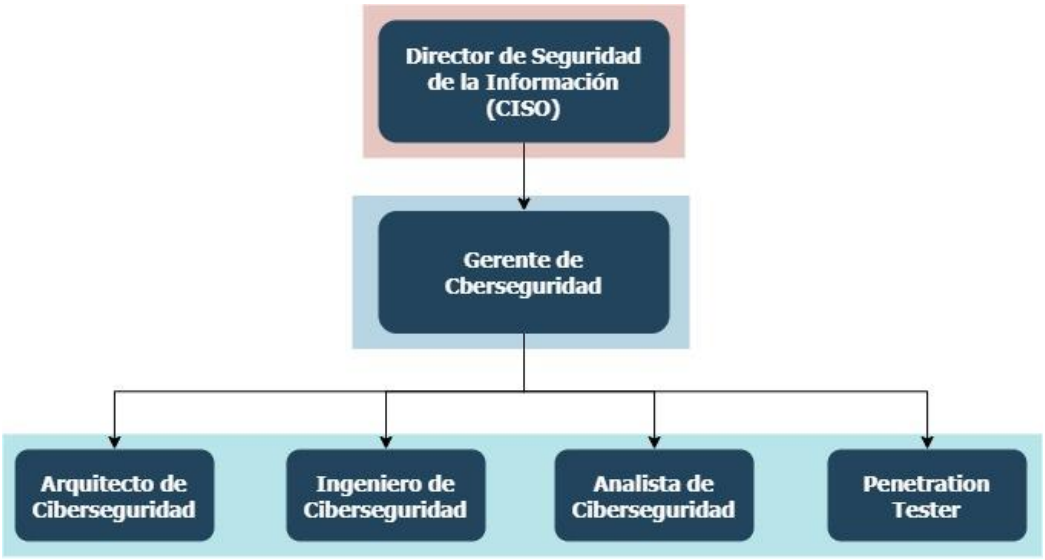

Figura 32: Estructura y jerarquía organizacional de un departamento de Seguridad de Información. Fuente: Elaboración propia. Elaborado usando el sitio draw.io

En la Figura 33 se representan, de manera general, las técnicas propuestas para la comprobación de problemas de ciberseguridad, para su mejor visualización.

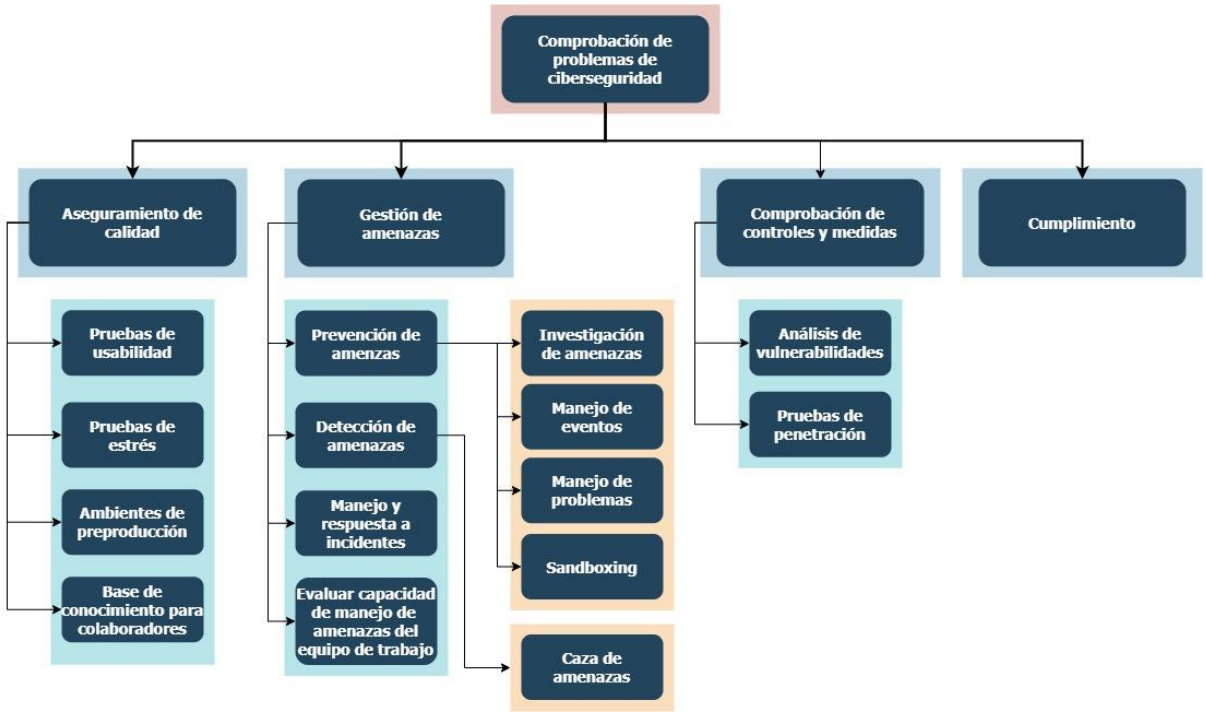

Figura 33: Técnicas para comprobación de problemas de seguridad. Fuente: Elaboración propia. Elaborado usando el sitio draw.io

5.1.3.2 Aseguramiento de Calidad

Las pruebas de control de calidad (QA, por sus siglas en inglés) son un proceso que se utiliza para asegurarse de que los productos y servicios cumplan con las reglamentaciones específicas. Es una forma de evitar que ocurran problemas y defectos buscando asegurar la satisfacción del cliente con el producto final. Estas pruebas también están destinadas a verificar que el producto cumpla con los propósitos previstos, lo que generalmente incluye la comprobación de los requisitos funcionales.

- **Pruebas de usabilidad.** En ellas se pone a prueba qué tan bien un cliente puede usar el sistema o la aplicación web para completar una tarea.

  Responsables: gerente de ciberseguridad / ingeniero o ingeniera de ciberseguridad.

- **Pruebas de estrés.** Se busca probar cuánta tensión puede soportar el sistema antes de que falle. Esto se considera un tipo de prueba no funcional. Responsables: gerente de ciberseguridad / ingeniero o ingeniera de ciberseguridad.
- **Ambientes de preproducción.** Las aplicaciones deben probarse continuamente para asegurarse de que funcionen bien juntas, ya que el desarrollo de software a menudo se divide en proyectos más pequeños realizados por personas y equipos separados. Se debe de asegurar de que todas las funciones tengan el comportamiento esperado y que cada parte de la aplicación interactúe correctamente con las otras. Esto reduce la cantidad de errores que los usuarios pueden encontrar al usar la aplicación y da como resultado una mayor tasa de uso y usuarios más satisfechos. Responsables: gerente de ciberseguridad / ingeniero o ingeniera de ciberseguridad.
- **Crear una base de conocimiento para sus colaboradores.** Una base de conocimiento es una biblioteca de autoservicio en línea de información sobre un producto, servicio, departamento o tema.

  Los datos de la base de conocimientos pueden provenir de cualquier parte. Por lo general, los colaboradores con bastante conocimiento en los temas relevantes enriquecen y amplían la base de conocimientos.

  Responsables: gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad

5.1.3.3 Gestión de Amenazas

La gestión de amenazas es un proceso utilizado para prevenir ciberataques, detectar ciber amenazas y responder a incidentes de seguridad.

- Prevención de amenazas

- **Realizar investigación de amenazas**. El propósito es localizar indicadores de compromiso sospechosos en la red. Si esta es el objetivo de un ataque en curso o de una amenaza persistente avanzada, la investigación de amenazas puede evaluar el daño causado por el ataque dirigido, proporcionar información sobre la llegada y la evolución del ataque y ayudar a planificar una respuesta eficaz a los incidentes de seguridad.

  Esto va de la mano con la inteligencia de amenazas, que son datos recopilados, procesados y analizados para comprender la motivación, los objetivos y los comportamientos de los atacantes. Además, permite tomar decisiones de seguridad más rápidas e informadas basadas en datos y cambiar el comportamiento de reactivo a proactivo en la lucha contra los actores maliciosos.

  Responsables: gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / ingeniero o ingeniera de ciberseguridad / analista de ciberseguridad.

- **Manejo de eventos.** Cada sistema genera algún tipo de evento de seguridad. Esto puede ser útil, ya que además de registrar la actividad de la red, también mantiene un registro histórico de eventos y estados del sistema en un formato secuencial.

  Estos eventos de seguridad pueden ayudar al determinar lo que pasó, en la detección de intrusos, contención de incidentes, análisis forense, alertas en tiempo real de actividad maliciosas, así como en la comprensión de la intención del atacante, por mencionar algunas.

No obstante, la cantidad de datos generados puede ser abrumadora y los eventos críticos pueden perderse sin un sistema de eventos de seguridad eficaz. Saber qué actividades y sistemas monitorear, y el cuándo, es clave para filtrar y ubicar la causa raíz de una brecha de seguridad. Responsables: gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / analista de ciberseguridad.

- **Manejo de problemas.** Corresponde a identificar y gestionar problemas utilizando métodos preventivos e identificando las causas raíz para ayudar a prevenir problemas futuros. Ayuda a eliminar incidentes recurrentes, minimiza el impacto de interrupciones inesperadas y apoya la prevención de problemas antes de que ocurran. Responsables: gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / ingeniero o ingeniera de ciberseguridad / analista de ciberseguridad
- **Ejecución en ambientes controlados y aislados (*Sandboxing*).** Proporcionan una capa adicional de seguridad para analizar amenazas y separarlas de la red, con lo que se garantiza que estas no comprometan las operaciones. Brinda un entorno seguro para abrir archivos sospechosos o ejecutar programas no confiables sin afectar los dispositivos en los que residen. Se puede usar en cualquier momento y en cualquier situación para examinar de forma segura un archivo o un código potencialmente malicioso, aislándolo del ambiente en general.

  Se utiliza también como recurso para probar el software y clasificarlo como "seguro" o "no seguro", lo que permite comprender cómo

funciona antes de que infecte algún dispositivo con malware o virus, lo cual brinda información y sugerencias sobre qué buscar en otras situaciones. A medida que el malware se vuelve más frecuente y peligroso, los enlaces, las aplicaciones y las descargas maliciosas pueden obtener acceso ilimitado a los datos de su red si no se controlan primero. Responsables: gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / ingeniero o ingeniera de ciberseguridad

- Detección de amenazas
    - **Realizar ejercicios de caza de amenazas.** La caza de amenazas, o *Threat Hunting* en inglés, es una función de seguridad que combina metodología proactiva, tecnología innovadora e inteligencia de amenazas para detectar y detener actividades maliciosas. Responsables: gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / ingeniero o ingeniera de Ciberseguridad
- Manejo y respuesta a incidentes

Un incidente es un suceso que puede interrumpir o provocar la pérdida de operaciones, servicios o funciones. La gestión de incidentes describe las acciones necesarias que se deben llevar a cabo para analizar, identificar y corregir problemas, así como para tomar medidas que puedan prevenir problemas futuros. Busca restaurar el funcionamiento normal del servicio, al minimizar el impacto en las operaciones productivas manteniendo la calidad.

La respuesta a incidentes es un enfoque estructurado para hacerle frente a diferentes tipos de incidentes de seguridad, ciber amenazas y

filtraciones de datos. La respuesta a incidentes tiene como objetivo identificar, contener y minimizar el costo de un ciberataque o un incidente en curso.

Responsables: CISO / gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / ingeniero o ingeniera de ciberseguridad / analista de ciberseguridad

- Evaluar la capacidad de manejo de amenazas del equipo de trabajo**.**

  La detección de amenazas alerta sobre actuales o potenciales intrusos. Sin esta capacidad de detectar amenazas por adelantado, los datos, información confidencial y otros activos corren el riesgo de quedar expuestos a actores maliciosos. Al reconocer las amenazas a tiempo, es posible responder a ellas adecuadamente y mitigar el daño.

  Para realizar esta evaluación se deben de plantear escenarios de prueba, recreaciones de escenarios, medir la capacidad de reacción en la ejecución de procesos, medidas y aprovechamiento del conjunto de herramientas disponibles que soportan el manejo de amenazas.

  Responsables: CISO / gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / ingeniero o ingeniera de Ciberseguridad.

5.1.3.4 Comprobación de controles y medidas

Para evaluar con precisión cómo funcionan los controles de seguridad de forma individual y colectiva, es esencial realizar una validación de control de seguridad de alto nivel. Existen gran cantidad de opciones cuando se trata de productos de seguridad. Sin embargo, la simple superposición de producto sobre producto no garantiza una seguridad organizativa eficaz, más bien, el uso de docenas de controles de seguridad diferentes puede aumentar considerablemente la complejidad dentro de un sistema.

Llevar a cabo validación de los controles de seguridad proporciona una evaluación definitiva de la solidez general de la seguridad de la organización.

- **Análisis de vulnerabilidades.** Pruebas sistemáticas de un sistema para determinar la idoneidad de los controles de seguridad, identificar las deficiencias de seguridad, proporcionar datos que puedan predecir la eficacia de las medidas de seguridad propuestas y confirmar la eficacia de dichas medidas después de la implementación.

  Responsables: gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / *penetration tester* / analista de ciberseguridad

- **Pruebas de penetración.** Un método de prueba que se enfoca en componentes binarios individuales o en la aplicación como un todo para determinar si las vulnerabilidades dentro o entre componentes pueden explotarse para comprometer la seguridad de una aplicación, sus datos o los recursos de su entorno.

  Responsables: gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / ingeniero o ingeniería de Ciberseguridad / *penetration tester*

5.1.3.5 Cumplimiento

Son las acciones o actividades destinadas a cumplir una regulación. Las regulaciones son pautas de alto nivel creadas para industrias específicas para abordar problemas específicos.

Algunos ejemplos de regulaciones que conciernen a los departamentos de TI y seguridad son las siguientes:

La industria financiera utiliza números de tarjetas de crédito, los cuales deben cifrarse para evitar robos, por lo cual se creó el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS, por sus siglas en inglés).

La industria de salud utiliza información del paciente (PHI, por sus siglas en inglés) que debe intercambiarse de forma segura con los consultorios médicos y oferentes de seguros, por lo que Estados Unidos creó la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA, por sus siglas en inglés).

Los gobiernos federales se involucran en la seguridad nacional, por consiguiente, Estados Unidos creó la Ley Federal de Gestión de Seguridad de la Información (FISMA, por sus siglas en inglés) para garantizar que todas las agencias protejan sus datos.

Los profesionales de la ciberseguridad deben comprender completamente estas regulaciones, ya que cada una incluye una cantidad específica de controles de seguridad que deben ser implementados.

Responsables: CISO / gerente de ciberseguridad / arquitecto o arquitecta de ciberseguridad / ingeniero o ingenieria de ciberseguridad

5.1.3.6 Reflexión de la propuesta

Para la propuesta de generalidades sobre las recomendaciones, los mecanismos de ciberseguridad para la protección de chatbots y la identificación y comprobación de problemas en estos, se utilizó información actualmente disponible, por lo que se recomienda de igual manera continuar con la verificación de actualizaciones con respecto a estas secciones, ya que esta no contempla posibles implementaciones a futuro o el descubrimiento de amenazas de día cero.

Finalmente, la propuesta descrita reúne elementos cuya selección o implementación dependen del criterio del lector y la arquitectura que se encuentre en utilización del chatbot.

Capítulo 6. Conclusiones y Recomendaciones

Se presentan en este capítulo las conclusiones a los objetivos planteados en la investigación y una serie de recomendaciones que pueden ayudar a mejorar este tipo de investigación.

6.1 Conclusiones

Conclusiones del objetivo 1: "Describir la tecnología de inteligencia artificial conversacional "chatbot", definiendo sus elementos y su aplicabilidad en diferentes industrias para comprender su adopción y empleabilidad".

Este objetivo fue alcanzado y se concluye:

- Las soluciones de chatbot conversacional se encuentran implementados mediante diferentes mecanismos, sin embargo, predomina la implementación en páginas web para la oferta de sus beneficios.
- Se determina que existe una mayor adopción de este tipo de tecnología en el sector financiero, donde principalmente la solución se enfoca en apoyar procesos de servicio al cliente y la mejora de atención.
- Existe una oportunidad considerable en la utilización de esta tecnología para el apoyo y la realización de procesos específicamente en ciberseguridad. Es posible que esto se deba a una preocupación sobre la seguridad y la confianza en esta, pero inclusive la propuesta generada serviría como referencia para realizar una implementación segura en esta área.
- Se logró describir y comprender cada uno de los módulos y elementos de la arquitectura de la tecnología y su interacción, para que estos sean considerados en el desarrollo y conclusión de los siguientes objetivos.

Conclusiones del objetivo 2: "Explicar las posibles vulnerabilidades, riesgos y contramedidas de ciberseguridad asociados con los chatbots, informando

sobre las posibles afectaciones y controles para poder identificar su superficie de ataque y disminuirla".

Este objetivo fue alcanzado y se concluye:

- Se describieron los términos principales asociados con la ciberseguridad para dar al lector una idea con respecto a la cobertura de las vulnerabilidades, riesgos y contramedidas.
- Se evidenciaron las vulnerabilidades y contramedidas, sus características y tareas por módulo que componen la arquitectura de chatbot. Esto con el fin de informar al lector y que pueda separar el módulo de su interés, los controles que desea aplicar para disminuir la superficie de ataque relacionada y, de esta manera, el riesgo.
- Se brindó información respecto a las amenazas generales que podrían afectar el funcionamiento del chatbot en su totalidad y, a su vez, las contramedidas generales que se podrían aplicar para proteger la arquitectura de este.

Conclusiones del objetivo 3: "Efectuar una revisión de las prácticas empleadas en el uso y adopción mediante la aplicación de una entrevista a expertos en esta tecnología para obtener una base de recomendaciones a nivel técnico y de ciberseguridad."

Este objetivo fue alcanzado y se concluye:

- Se logró efectuar las entrevistas a expertos en el uso de la tecnología chatbot con la finalidad de obtener una base de recomendaciones a nivel técnico y de ciberseguridad.
- Ambos expertos indicaron desconocer sobre la existencia de regulaciones o leyes aplicadas específicamente a la tecnología investigada a nivel nacional.

Adicionalmente, enfatizaron en la importancia, pues tanto las regulaciones nacionales como las internacionales influyen de sobremanera en la toma de decisión de controles que se utilizarán y su disponibilidad.

- Se obtuvo un valor agregado a la investigación, pues también brindaron información relacionada al uso responsable de la tecnología y la orientación para brindar una experiencia óptima y transparente al usuario.
- Se facilitó información con respecto a vulnerabilidades, riesgos, manejo de datos, privacidad del usuario y contramedidas para la retroalimentación de la propuesta.

Conclusiones del objetivo 4: "Descubrir el estado de la implementación en producción y mecanismos de protección relacionados con los chatbots, mediante la aplicación de cuestionarios a empresas del sector para contrastar con respecto a las medidas sugeridas por los expertos y las que arrojará la investigación".

Este objetivo fue alcanzado y se concluye:

- Cada una de las respuestas a las preguntas fueron analizadas para poder interpretar y contrastar el estado actual de la implementación de chatbots con respecto al cumplimiento de objetivos previos y determinar los mecanismos que se encuentran en ejecución.
- Se constata que la implementación más común es a través de páginas web y que la interacción con esta es, con mayor frecuencia, externa a la organización.
- Se determina que con mayor frecuencia las organizaciones consultadas, tienen una inclinación por la adquisición de los servicios de un tercero para el

aprovechamiento de la tecnología y que la seguridad es un aspecto importante durante el proceso de evaluación.

- Se logra comprobar la versatilidad y aplicabilidad de la tecnología al revisar los diferentes tipos de servicios con los que interactúan las diferentes organizaciones. Se mencionan, por ejemplo, servicios bancarios, consultas frecuentes (mesa de ayuda), recursos de nube y automatización de procesos.
- Se comprueba que actualmente las diferentes organizaciones no están utilizando la tecnología como parte de los procesos o funciones de ciberseguridad.
- Se logra complementar las medidas sugeridas por los expertos y las obtenidas a partir de la investigación con las resultantes de la aplicación de estos cuestionarios. Este complemento permite iniciar con la propuesta final de buenas prácticas en ciberseguridad para el sector privado costarricense.
- Se resalta la importancia de valorar y considerar a profundidad mecanismos que permitan validar que los controles en ejecución, y la solución como tal, se encuentren funcionando de manera correcta.
- Se destaca que no existe el uso de un consentimiento informado como práctica estándar que sea presentado al usuario previo a su interacción con el chatbot. Sin embargo, en la mayoría de los casos, afirman que el usuario posee la potestad de solicitar la eliminación de sus datos e información colectada por este medio.

Conclusiones del Objetivo General: “Proponer buenas prácticas de ciberseguridad mediante la elaboración de un análisis del uso de chatbots y sus riesgos, para la disminución de estos y fomentar la utilización segura de esta tecnología en el sector privado costarricense”.

En primer lugar, se debe de resaltar que existe una coincidencia alta en la información obtenida a partir de las referencias consultadas, los expertos entrevistados y los cuestionarios aplicados a empresas del sector privado costarricense en la consideración y aplicación de contramedidas. Por ejemplo, coincidencias en el cifrado de extremo a extremo, la autenticación, el entrenamiento de la solución, entre otros. Se rescatan recomendaciones en la utilización e implementación efectiva para la adopción por parte de los usuarios de la tecnología.

Por otra parte, existe una oportunidad de mejora a nivel del manejo de datos de los usuarios, la implementación del consentimiento informado, la exploración de casos de uso, la aplicación de mecanismos que permitan garantizar la efectividad de los controles y la calidad en la interacción de la solución con el usuario. Es por esto, que a pesar de que la tecnología de chatbot es reciente, se logra realizar una propuesta que posibilita a las organizaciones utilizar como referencia buenas prácticas de ciberseguridad, tanto para implementaciones nuevas como existentes. Dicha propuesta apoya los esfuerzos para la disminución de riesgos en las empresas interesadas del sector.

6.2 Recomendaciones

Se presentan, a continuación, algunas recomendaciones de la experiencia obtenida al realizar el trabajo, tanto desde el punto de vista del alcance en la obtención de información, como a nivel de la administración de recursos y tiempo dedicado a la investigación.

Dado que el presente trabajo corresponde a un trabajo conjunto entre los masterandos, se recomienda el uso de herramientas colaborativas como Google Drive, y procesos de control de versiones de los diferentes documentos con el fin de sincronizar esfuerzos y evitar la pérdida de datos.

Dado el ámbito en el que se desarrolló el proyecto, el cual involucró la consulta de expertos en chatbots y la obtención de información con respecto a la consideración de controles de ciberseguridad aplicados a estos en empresas del sector privado costarricense, se recomienda para trabajos futuros, igualmente realizar la consulta a expertos en estas áreas y sectores o a cualquier otra que se considere necesaria, a fin de añadir mayor credibilidad y validez a los resultados.

Se recomienda adicionalmente al lector mantenerse actualizado en el uso de la tecnología y ciberseguridad para evitar cualquier posible afectación derivada de la evolución de estas y que aún no se encuentre descubierta.

Capítulo 7. Reflexiones Finales

El planteamiento y desarrollo de la investigación nace a partir de la inquietud por parte de los autores con respecto al conocimiento de la inteligencia artificial y su aplicabilidad en el proceso de comunicación conocido como chatbots, así como la intención de explorar las vulnerabilidades, amenazas y explotaciones posibles asociadas para poder generar una propuesta que permita referenciar una base de buenas prácticas para la minimización del riesgo derivado.

Fue considerado el sector privado costarricense debido a qué es el sector reconocido como mayoritariamente productivo en el país, por lo que enriquece más el proceso de conocimiento y descubrimiento del estado actual de la solución y de los controles asociados a la tecnología, los cuales también retroalimentaron la propuesta en conjunto con la información obtenida a partir de las opiniones brindadas por expertos en esta área. Se comprueba que al inicio del proyecto no existían iniciativas locales similares por lo que queda en evidencia la posibilidad de explotar la temática y las áreas relacionadas en trabajos futuros.

El manejo de tiempo para la aproximación a los actores requeridos para la retroalimentación de la investigación debe de contemplarse con antelación para poder lograr el nivel de enriquecimiento buscado y que los resultados sean de calidad.

Como resultado del proceso investigativo se logró obtener información con respecto al funcionamiento de la arquitectura de la tecnología chatbot y mejorar el conocimiento actual sobre las vulnerabilidades y amenazas, así como de las contramedidas que se pueden tomar en cuenta para resguardar el correcto funcionamiento de esta y la información que allí se maneja en la interacción o almacenamiento.

Una enseñanza que deja la investigación es que aún existe una oportunidad de mejora y aprovechamiento en la exploración de casos de uso para la tecnología mencionada, ya que se podría aplicar a otras áreas o procesos de la tecnología o fuera de esta.

Adicionalmente, se expone la oportunidad para profundizar en el análisis de la tecnología, su riesgo y las contramedidas de forma exhaustiva, pues hoy la información existente se encuentra muy enfocada en el desarrollo realizado por compañías de tecnología y no de forma agnóstica.

Finalmente, se resalta que, a pesar de que la tecnología chatbot es reciente, existen expertos con un amplio conocimiento sobre esta dispuestos a colaborar con la mejora continua en los procesos de utilización, manejo de información y ciberseguridad. También, existen empresas que hoy se encuentran sacando provecho en sus procesos productivos y sin sacrificar la seguridad requerida.

Capítulo 8. Trabajos a Futuro

Como acompañamiento al proceso natural de la evolución de la tecnología, es importante realizar una verificación periódica de los elementos que componen la tecnología de chatbots, sus metodologías de desarrollo para así también poder identificar, dar atención a cualquier posible vulnerabilidad o amenaza que pueda afectar o comprometer la ciberseguridad de estos elementos y, como consecuencia de esto, poder disminuir la superficie de ataque, por tanto, el riesgo asociado.

Esta revisión es recomendable incorporarla en los procesos de prevención de riesgo y revisión de la calidad de controles que deben estar descritos en la política de seguridad organizacional o en la sección correspondiente de esta.

Se podría considerar para una elaboración futura, temas relacionados con otras áreas de la inteligencia artificial que pudieran estar o no relacionadas con el tema desarrollado. Por ejemplo, el uso de asistentes inteligentes cuya interacción es realizada por medio de comandos de voz, como los actualmente más reconocidos de gigantes de la tecnología: Alexa (Amazon), Sam (Samsung), Siri (Apple), Cortana (Microsoft), Celia (Huawei), Asistente de Google.

Adicionalmente, se podría desarrollar la temática de ventajas y beneficios de implementar chatbots como un mecanismo de agilización mediante la automatización de procesos en ciberseguridad, sus áreas derivadas y de esta manera los actores relacionados podrían enfocarse en tareas prioritarias y de mejora continua.

Glosario

Algoritmo

Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. Fuente: https://dictionary.cambridge.org/es/diccionario/ingles-espanol/algorithm

Amenazas de día Cero

Es una vulnerabilidad de software descubierta por los atacantes antes de que el proveedor se haya percatado de ella. Debido a que los proveedores no lo saben, no existe un parche para las vulnerabilidades de día cero, lo que hace que los ataques tengan más probabilidad de ser exitosos. Fuente: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

API

Una API es un conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el software de las aplicaciones. API significa interfaz de programación de aplicaciones. Fuente: https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces

Aprendizaje automático

Aprendizaje Automático (AA, o Machine Learning, por su nombre en inglés) es la rama de la Inteligencia Artificial que tiene como objetivo desarrollar técnicas que permitan a las computadoras aprender. Fuente: https://azure.microsoft.com/es-es/overview/what-is-machine-learning-platform/

Autenticación de múltiples factores

Es un enfoque en capas para proteger cuentas en línea y los datos que contienen. Cuando se habilita MFA (Multi-factor authentication, por sus siglas en inglés) en servicios en línea (como el correo electrónico), se debe proporcionar una combinación de dos o más autenticadores para verificar la identidad antes de que el servicio otorgue acceso. Fuente: https://www.cisa.gov/mfa

Defensa en profundidad

También conocida como estrategia de seguridad en profundidad. Es un enfoque de ciberseguridad que utiliza múltiples capas de seguridad para una protección holística. Una defensa en capas ayuda a las organizaciones de seguridad a reducir vulnerabilidades, contener amenazas y mitigar riesgos. Fuente: https://www.cyberark.com/es/what-is/defense-in-depth/

Honeypot

Un honeypot es un mecanismo de ciberseguridad que utiliza un objetivo de ataque fabricado para alejar a los ciberdelincuentes de los objetivos legítimos. También recopilan inteligencia sobre la identidad, los métodos y las motivaciones de los adversarios. Fuente: https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/

HTTPS

Es un protocolo de comunicación de Internet, que provee protección para l integridad y confidencialidad de los datos de los usuarios entre sus dispositivos y el sitio. HTTPS significa protocolo seguro de transferencia de hipertexto (HyperText Transfer Protocol Secure e inglés). Fuente: https://developers.google.com/search/docs/advanced/security/https?hl=es

NLP

El procesamiento del lenguaje natural (NLP, por sus siglas en inglés) se refiere a la rama de la informática, y más específicamente, la rama de la inteligencia artificial, que se ocupa de brindar a las computadoras la capacidad de comprender textos y palabras habladas de la misma manera que los seres humanos. Fuente: https://www.ibm.com/cloud/learn/natural-language-processing

SDK

SDK significa kit de desarrollo de software (Software Development Kit en inglés). También conocido como devkit, es un conjunto de herramientas de creación de software para una plataforma específica, incluidos los componentes básicos, los depuradores y, a menudo, un marco o grupo de bibliotecas de código, como un conjunto de rutinas específicas para un sistema operativo. Fuente: https://www.ibm.com/cloud/blog/sdk-vs-api

Serverless

Serverless significa "sin servidor". Es un modelo de desarrollo nativo de la nube que permite a los desarrolladores crear y ejecutar aplicaciones sin tener que administrar servidores. Fuente: https://www.redhat.com/en/topics/cloud-native-apps/what-is-serverless

SQL

SQL (Structure Query Language, por sus siglas en inglés) es una forma de comunicarse con una base de datos relacional que le permite definir, consultar, modificar y controlar los datos. Fuente: https://docs.microsoft.com/en-us/cpp/data/odbc/sql?view=msvc-170#:~:text=SQL%20(Structured%20Query%20Language)%20is,modify%2C%20and%20control%20the%20data

Superficie de ataque

El conjunto de puntos en el límite de un sistema, un elemento del sistema o un entorno, donde un atacante puede intentar ingresar, causar un efecto o extraer datos de ese sistema, elemento del sistema o entorno. Fuente: https://csrc.nist.gov/glossary/term/attack_surface

Tiempo promedio de detección (MTTD)

Se refiere a la cantidad media de tiempo que le toma a la organización descubrir, o detectar, un incidente. Cuanto antes se entere una organización de un problema, mejor. Fuente: https://www.sentinelone.com/blog/mttd-mean-time-to-detect-detailed-explanation/

Tiempo promedio a respuesta (MTTR)

MTTR (mean time to respond, por sus siglas en inglés) es el tiempo promedio que se tarda en recuperarse de una falla del sistema o del producto desde el momento en que se le alertó por primera vez de esa falla. Esto no incluye ningún tiempo de retraso en su sistema de alerta. Fuente: https://www.atlassian.com/incident-management/kpis/common-metrics

TLS

Transport Layer Securrity, por sus siglas en inglés, es un protocolo de cifrado para proporcionar conexiones seguras, haciendo posible que dos partes se comuniquen con privacidad e integridad de datos. Fuente: https://www.ibm.com/docs/es/ibm-mq/9.1?topic=mechanisms-cryptographic-security-protocols-tls

Xiaoice

Es el chatbot social más popular en el mundo. XiaoIce tiene un diseño único como una inteligencia artificial acompañante con una conexión emocional para satisfacer la necesidad humana de comunicación, afecto, y pertenencia social. Fuente: https://www.microsoft.com/en-us/research/publication/the-design-and-implementation-of-xiaoice-an-empathetic-social-chatbot/

Referencias

Aliyev, A. I. (2021). *Artificial Intelligence and Personal Data: International and National Framework.* Obtenido de Peace Human Rights Governance: http://phrg.padovauniversitypress.it/2021/1/4

Atlassian. (s.f.). *MTBF, MTTR, MTTF, MTTA: Understanding incident metrics.* https://www.atlassian.com/incident-management/kpis/common-metrics

Atlassian. (s.f.). *What is a knowledge base?* Obtenido de https://www.atlassian.com/itsm/knowledge-management/what-is-a-knowledge-base

AT&T Cybersecurity. (s.f.). *Security Event Management & Monitoring.* Obtenido de https://cybersecurity.att.com/solutions/security-event-management-and-monitoring

Avast. (s.f.). *¿Qué es el sandboxing?* Obtenido de https://www.avast.com/es-ww/business/resources/what-is-sandboxing#pc

Baker, K. (17 de marzo de 2022). *What is Cyber Threat Intelligence?* Obtenido de CrowdStrike: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

box. (8 de febrero de 2022). *What is threat detection. Box Blog.* Obtenido de https://blog.box.com/what-is-threat-detection

Bakovic, T., Biallas, M., Caballero, A., Lopez Conde, M., Cook, P., Diwan, P., Vivien Houngbonon, G., Kaleem, H., Makala, B., Manchanda, S., Menes, R., Mockel P., Mou, X., Mrazek, M., Myers, G., Nejkov, K., Niforos, M., O'Neil, F., Rana, A. N.,... Twinn, Ian (marzo de 2021). *Artificial Intelligence In Emerging Markets - Opportunities, Trends, and Emerging Business Models.* Obtenido de

https://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/artificial+intelligence+in+emerging+markets

Bozic, J., & Wotawa, F. (diciembre de 2020). *Interrogating Virtual Agents: In Quest of Security Vulnerabilities.* In IFIP International Conference on Testing Software and Systems (pp. 20-34). Springer, Cham. https://doi.org/10.1007/978-3-030-64881-7_2

Bulin Shaqiri (2021). *Development and Refinement of a chatbot for Cybersecurity Support.* Obtenido de https://files.ifi.uzh.ch/CSG/staff/franco/extern/theses/BA-B-Shaqiri.pdf

Cambridge Dictionary. (s.f.). *Algoritmo*. Obtenido de https://dictionary.cambridge.org/es/diccionario/ingles-espanol/algorithm

Cambridge Dictionary. (s.f.). *Ataque*. Obtenido de https://dictionary.cambridge.org/dictionary/spanish-english/ataque

Cambridge Dictionary. (s.f.). *Lenguaje*. Obtenido de https://dictionary.cambridge.org/dictionary/spanish-english/lenguaje

Cambridge Dictionary. (s.f.). *Problema.* Obtenido de https://dictionary.cambridge.org/dictionary/spanish-english/problema

Cambridge Dictionary. (s.f.). *Usuario.* Obtenido de https://dictionary.cambridge.org/dictionary/spanish-english/usuario

Chotia, R. (19 de abril de 2021). *Conversational AI Chatbot Security – What You Need To Know*. Obtenido de Verloop.Io: https://verloop.io/blog/conversational-ai-chatbot-security/

CISA. (s.f.). *Multi-Factor Authentication*. Obtenido de CISA - Cybersecurity & Infrastructure Security Agency: https://www.cisa.gov/mfa

CISA. (s.f.). *Ransomware 101*. Obtenido de CISA Stop Ransomware: https://www.cisa.gov/stopransomware/ransomware-101

Collins Dictionary. (s.f.). *Privacy*. Obtenido de https://www.collinsdictionary.com/us/dictionary/english/privacy

Comiter, M. (agosto de 2019). *Attacking Artificial Intelligence - AI's Security Vulnerability and What Policymakers Can Do About It.* Obtenido de Belfer Center for Science and International Affairs Paper, Harvard Kennedy School: https://www.belfercenter.org/publication/AttackingAI

CrowdStrike. (9 de marzo de 2022). *What is a Honeypot? How It Can Trap Cyberattackers*. Obtenido de https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/

CyberArk. (s.f.). *What is Defense-in-Depth?* Obtenido de https://www.cyberark.com/es/what-is/defense-in-depth/

Davis, N. (31 de julio de 2013). *Secure Software Development Life Cycle Processes.* Obtenido de CISA - Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/uscert/bsi/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes

EC-Council. (s.f.). *What is Incident Response?* Obtenido de https://www.eccouncil.org/what-is-incident-response/

Fingold, J., & Iqbal, K. (3 de noviembre de 2021). *Bot Framework security guidelines*. Obtenido de Microsoft Docs: https://docs.microsoft.com/en-us/azure/bot-service/bot-builder-security-guidelines?view=azure-bot-service-4.0

Frank, J. (5 de octubre de 2018). *Your Next Move: Security Architect.* Obtenido de CompTIA. https://www.comptia.org/blog/your-next-move-security-architect

Google Developers. (s.f.). *Proteger sitios con el protocolo HTTPS*. Obtenido de https://developers.google.com/search/docs/advanced/security/https?hl=es

Hasal, M., Nowaková, J., Saghair, K. A., Abdulla, H., Snášel, V., & Ogiela, L. (3 de june de 2021). *Chatbots: Security, privacy, data protection, and social aspects*. Obtenido de Wiley Online Library: https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.6426

IBM. (s.f.). *¿Qué son las pruebas de software y cómo funcionan?* Obtenido de https://www.ibm.com/ar-es/topics/software-testing

IBM. (s.f.). *What is Threat Management?* Obtenido de https://www.ibm.com/sg-en/topics/threat-management

IBM. (20 de abril de 2021). *Protocolos de seguridad de cifrado: TLS.* Obtenido de IBM Documentación. https://www.ibm.com/docs/es/ibm-mq/9.1?topic=mechanisms-cryptographic-security-protocols-tls

IBM Cloud Education. (3 de junio de 2020). *Inteligencia artificial (IA)*. Obtenido de IBM: https://www.ibm.com/mx-es/cloud/learn/what-is-artificial-intelligence

IBM Cloud Education. (2 de julio de 2020). *Natural Language Processing (NLP)*. Obtenido de IBM: https://www.ibm.com/cloud/learn/natural-language-processing

IBM Cloud Education. (13 de julio de 2021). *SDK vs. API: What's the Difference?* Obtenido de IBM: https://www.ibm.com/cloud/blog/sdk-vs-api

Imperva. (s.f.). *What is Penetration Testing? - Step-By-Step Process & Methods.* Obtenido de https://www.imperva.com/learn/application-security/penetration-testing/

INCIBE. (30 de septiembre de 2016). *CEO, CISO, CIO. . . ¿Roles en ciberseguridad?* Obtenido de INCIBE - Instituto Nacional de Ciberseguridad de España. https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad

International Telecommunications Unit (ITU). (noviembre de 2010). *Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación*. Obtenido de https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Kaspersky. (s.f.). *What is a Zero-day Attack? - Definition and Explanation.* Obtenido de https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Lane, P. (3 de febrero de 2020). *Compliance in Cybersecurity: What You Need to Know to Stay Ahead of Regulations, Part 1.* Obtenido de CompTIA. https://www.comptia.org/blog/compliance-in-cybersecurity-part-1

Macmillan Dictionary. (s.f.). *Intelligence*. Obtenido de https://www.macmillandictionary.com/dictionary/british/intelligence

McCraw, D. B. (8 de julio de 2020). *Your Next Move: Cybersecurity Analyst.* Obtenido de CompTIA. https://www.comptia.org/blog/your-next-move-security-analyst

Microsoft. (s.f.). *Responsible AI principles.* Obtenido de https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6

Microsoft. (s.f.). *What is a chatbot?* Obtenido de Microsoft Power Virtual Agents: https://powervirtualagents.microsoft.com/en-us/what-is-a-chatbot/

Microsoft Azure. (s.f.). *¿Qué es el aprendizaje automático?* Obtenido de https://azure.microsoft.com/es-es/overview/what-is-machine-learning-platform/

Mnisterio de Ciencia, Tecnología y Telecomunicaciones (MICITT) de Costa Rica. (2017). *Estrategia Nacional de Ciberseguridad de Costa Rica*. Obtenido de https://www.micitt.go.cr/sites/default/files/estrategia-nacional-de-ciberseguridad-costa-rica-19-10-17.pdf

Mnisterio de Ciencia, Tecnología y Telecomunicaciones (MICITT) de Costa Rica. (2018). *Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 2018–2022*. Obtenido de https://www.micitt.go.cr/sites/default/files/estrategia-tdhcrb.pdf

Mora, W. (18 de julio de 2019). *Costa Rica en posición 66 de ranking mundial de 194 países en inteligencia artificial*. Obtenido de Portal de la Investigación - Universidad de Costa Rica: https://vinv.ucr.ac.cr/es/noticias/costa-rica-en-posicion-66-de-ranking-mundial-de-194-paises-en-inteligencia-artificial

NIST. (s.f.). *Attack Surface*. Obtenido de NIST - Information Technology Laboratory - Computer Security Resource Center (CSRC). https://csrc.nist.gov/glossary/term/attack_surface

NIST. (s.f.). *Penetration Testing.* Obtenido de NIST - Information Technology Laboratory - Computer Security Resource Center (CSRC). https://csrc.nist.gov/glossary/term/penetration_testing

NIST. (s.f.). *Risk*. Obtenido de NIST - Information Technology Laboratory - Computer Security Resource Center (CSRC): https://csrc.nist.gov/glossary/term/risk

NIST. (s.f.). *Vulnerability Analysis.* Obtenido de NIST - Information Technology Laboratory - Computer Security Resource Center (CSRC). https://csrc.nist.gov/glossary/term/vulnerability_analysis

Oracle. (n.d.). *What is a chatbot?* Obtenido de https://www.oracle.com/chatbots/what-is-a-chatbot/

Organización Mundial de la Propiedad Intelectual (OMPI). (2019). *Informe de la OMPI sobre tendencias de la tecnología - La inteligencia artificial*. Obtenido de https://www.wipo.int/publications/es/details.jsp?id=4396

Organización Mundial de la Propiedad Intelectual (OMPI). (31 de enero de 2019). *El primer estudio de la OMPI sobre "tendencias de la tecnología" se centra en la inteligencia artificial*. Obtenido de https://www.wipo.int/pressroom/es/articles/2019/article_0001.html

OWASP. (s.f.). *OWASP API Security - Top 10.* Obtenido de https://owasp.org/www-project-api-security/

OWASP. (s.f.). *OWASP Top 10:2021*. Obtenido de https://owasp.org/Top10/

Oxford Insights & International Development Research Centre (IDRC). (2019). *Government AI Readiness Index 2019*. Oxford Insights. Obtenido de https://www.oxfordinsights.com/ai-readiness2019

Oxford Insights & International Development Research Centre (IDRC). (2020). Government AI Readiness Index 2020. Oxford Insights. https://www.oxfordinsights.com/government-ai-readiness-index-2020

Red Hat. (s.f.). *¿Qué es una API?* Obtenido de https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces

Red Hat. (31 de octubre de 2017). *What is serverless?* Obtenido de https://www.redhat.com/en/topics/cloud-native-apps/what-is-serverless

Robertson, C., Sharkey, K., Schonning, N., Jones, M., B, M., Hogenson, G., & Cai, S. (3 de agosto de 2021). *SQL*. Obtenido de Microsoft Docs: https://docs.microsoft.com/en-us/cpp/data/odbc/sql?view=msvc-170

SentinelOne. (29 de diciembre de 2020). *What Is MTTD (Mean Time to Detect)? A Detailed Explanation.* Obtenido de https://www.sentinelone.com/blog/mttd-mean-time-to-detect-detailed-explanation/

ServiceNow. (s.f.). *What is Incident Management?* Obtenido de https://www.servicenow.com/products/itsm/what-is-incident-management.html

ServiceNow. (s.f.). *What is Problem Management?* Obtenido de https://www.servicenow.com/products/itsm/what-is-problem-management.html

ServiceNow. (s.f.). *What is the Software Development Life Cycle (SDLC)?* Obtenido de https://www.servicenow.com/products/devops/what-is-sdlc.html

Sherwood, J. (20 de noviembre de 2017). *Your Next Move: Cybersecurity Engineer.* Obtenido de CompTIA. https://www.comptia.org/blog/your-next-move-cybersecurity-engineer

Shum, H., Gao, J., Li, D., Zhou, L., & Microsoft. (diciembre de 2018). *The Design and Implementation of XiaoIce, an Empathetic Social Chatbot*. Obtenido de Microsoft Research: https://www.microsoft.com/en-us/research/publication/the-design-and-implementation-of-xiaoice-an-empathetic-social-chatbot/

Stanford Encyclopedia of Philosophy. (18 de agosto de 2018). *Information.* Obtenido de https://plato.stanford.edu/entries/information/

Stanford Encyclopedia of Philosophy. (6 de septiembre de 2018). *Philosophy of Technology*. Obtenido de https://plato.stanford.edu/entries/technology/

Stanford Encyclopedia of Philosophy. (24 de febrero de 2020). *Rights*. https://plato.stanford.edu/entries/rights/

Trend Micro. (s.f.). *Exploit*. Obtenido de https://www.trendmicro.com/vinfo/us/security/definition/exploit

Trend Micro. (s.f.). *Threat Investigation.* Obtenido de https://docs.trendmicro.com/en-us/smb/worry-free-business-security-services-67-server-help/detection-and-respon/threat-investigation_001.aspx

Umaña, P. (24 de septiembre de 2019). *Sector privado genera el 86% de empleos del país*. Obtenido de El Observador. https://observador.cr/sector-privado-genera-el-86-de-empleos-del-pais/

Wilner, A. S. (2018). *Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation*. International Journal: Canada's Journal of Global Policy Analysis, 73(2), 308–316. https://doi.org/10.1177/0020702018782496

VMware. (s.f.). *What is Threat Hunting?* Obtenido de https://www.vmware.com/topics/glossary/content/cyber-threat-hunting.html

XM Cyber. (s.f.). *What is a Security Control Validation?* Obtenido de https://www.xmcyber.com/glossary/what-is-a-security-control-validation/

Ye, W., & Li, Q. (2021). *Chatbot Security and Privacy in the Age of Personal Assistants*. Obtenido de IEEE Xplore: https://ieeexplore.ieee.org/document/9355740

Zhang, D., Mishra, S, Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., Lyons, T., Manyika, J., Niebles, J. C., Sellitto, M., Shoham, Y., Clark, J., &

Perrault, R. (marzo de 2021). *The AI Index 2021 Annual Report.* Obtenido de AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA. https://aiindex.stanford.edu/ai-index-report-2021/

Apéndices

Como apéndices, se adjuntan las respuestas individuales obtenidas en el cuestionario descrito en la sección 3.6.1 Cuestionario, cuyo análisis conjunto fue descrito en la sección correspondiente. También se incluye la carta de revisión filológica.

Tabla 14: *Respuesta #1 al cuestionario.*

Preguntas	Opciones de respuesta
1. Indique en cuál industria del sector privado se desempeña.	(X) Financiero. ( ) Tecnología. ( ) Educación. ( ) Salud. ( ) Servicios. ( ) Transporte. ( ) Turismo. ( ) Mercadeo. ( ) Otro. Indique: _____
2. ¿Qué tipo de implementación de chatbot, posee su organización?	(X) Página web. ( ) App móvil. (X) App IM/Chat. (X) App inteligente. ( ) Otro. Indique: _____
3. ¿El chatbot implementado en su organización fue desarrollado a lo interno o adquirido por medio de un tercero?	( ) Desarrollo interno. (X) Tercero. ( ) Otros. Indique: _____
~~3.1 Si se desarrolló interno:~~ ~~¿Se contemplaron las buenas prácticas vigentes en la industria~~	~~( ) Sí.~~ ~~( ) No.~~

Preguntas	Opciones de respuesta
~~para el Ciclo de Vida de Desarrollo Seguro de Software (S-SDLC)?~~	
3.2 Si es de un tercero o contesta "Otros": ¿Se consideró la seguridad como un aspecto importante de la evaluación de la solución?	(X) Sí. ( ) No.
4. ¿Con que tipo de servicios interactúa el chatbot de forma principal en su organización?	Indique: _Servicios Bancarios_
5. ¿La herramienta se está utilizando como parte de los procesos / funciones de ciberseguridad?	( ) Sí. (X) No.
6. En la implementación de chatbot existente, ¿se consideró el cifrado como un elemento indispensable para la comunicación y manejo de datos en general?	(X) Sí. ( ) No.
7. ¿La herramienta se utiliza para uso interno, externo o ambos?	( ) Interno. ( ) Externo. (X) Ambos.
8. ¿La información obtenida por medio del Chatbot, es utilizada como beneficio empresarial para la mejora de interacción, servicios o consumo con un tercero? Seleccione las que aplique.	(X) Mejora de interacción. (X) Mejora de Servicios. ( ) Consumo de un tercero. ( ) Otro. Indique: _____
9. ¿Existe actualmente en su organización, algún documento o consentimiento informado que los usuarios deben aceptar	(X) Sí. ( ) No.

Preguntas	Opciones de respuesta
al utilizar el chatbot?	
10. Indique cuales, de los siguientes controles de seguridad, se han implementado en su organización para la implementación segura de chatbots:	(X) Validación de entrada de información. (X) Interacción segura con la BD. (X) Autenticación de múltiples factores (MFA). (X) Utilización de certificados digitales. (X) Almacenamiento seguro de la información recopilada. (X) Cumplimiento con regulaciones nacionales. (X) Cumplimiento con regulaciones internacionales. (X) Buenas prácticas recomendadas por el fabricante. (X) Manejo de errores y excepciones en el procesamiento de consultas y respuestas. (X) Aplicaciones de parches de seguridad. (X) Web Application Firewall (WAF). ( ) Load Balancer (LB). ( ) Next Generation Firewall (NGFW). (X) Data Loss Prevention (DLP). ( ) Otro. Indique: _____
11. ¿Cuáles de los siguientes mecanismos o técnicas utilizan en su organización para medir el nivel de riesgo de una solución chatbot?	(X) Pruebas de penetración (Pentesting). (X) Análisis de vulnerabilidades. ( ) Ejecución en ambientes controlados (Sandboxing). (X) Entornos de preproducción y post producción. (X) Pruebas de usabilidad. (X) Pruebas de estrés. ( ) Otro. Indique: _____
12. ¿Se está tomando en cuenta la privacidad de la información sensible de los usuarios en la utilización de chatbots?	(X) Sí. ( ) No.
13. ¿Tienen los usuarios de su organización el derecho de	(X) Sí. ( ) No.

Preguntas	Opciones de respuesta
solicitar la eliminación de sus datos personales de repositorios de almacenamiento utilizados por los chatbots, después de un periodo de tiempo?	
14. ¿La herramienta y los recursos de interacción propios de la misma (como el API) contienen características para control y manejo de tráfico a lo interno de la red?	(X) Sí. ( ) No.

Fuente: Elaboración propia.

Tabla 15: *Respuesta #2 al cuestionario.*

Preguntas	Opciones de respuesta
1. Indique en cuál industria del sector privado se desempeña.	( ) Financiero. ( ) Tecnología. ( ) Educación. ( ) Salud. (X) Servicios. ( ) Transporte. ( ) Turismo. ( ) Mercadeo. ( ) Otro. Indique: _____
2. ¿Qué tipo de implementación de chatbot, posee su organización?	(X) Página web. ( ) App móvil. ( ) App IM/Chat. ( ) App inteligente. ( ) Otro. Indique: _____
3. ¿El chatbot implementado en su organización fue desarrollado a lo interno o adquirido por medio de un tercero?	(X) Desarrollo interno. ( ) Tercero. ( ) Otros. Indique: _____
3.1 Si se desarrolló interno:	(X) Sí.

Preguntas	Opciones de respuesta
¿Se contemplaron las buenas prácticas vigentes en la industria para el Ciclo de Vida de Desarrollo Seguro de Software (S-SDLC)?	( ) No.
~~3.2 Si es de un tercero o contesta "Otros":~~ ~~¿Se consideró la seguridad como un aspecto importante de la evaluación de la solución?~~	~~( ) Sí.~~ ~~( ) No.~~
4. ¿Con que tipo de servicios interactúa el chatbot de forma principal en su organización?	Indique: _Mesa de ayuda_
5. ¿La herramienta se está utilizando como parte de los procesos / funciones de ciberseguridad?	( ) Sí. (X) No.
6. En la implementación de chatbot existente, ¿se consideró el cifrado como un elemento indispensable para la comunicación y manejo de datos en general?	(X) Sí. ( ) No.
7. ¿La herramienta se utiliza para uso interno, externo o ambos?	( ) Interno. ( ) Externo. (X) Ambos.
8. ¿La información obtenida por medio del Chatbot, es utilizada como beneficio empresarial para la mejora de interacción, servicios o consumo con un tercero? Seleccione las que aplique.	( ) Mejora de interacción. ( ) Mejora de Servicios. (X) Consumo de un tercero. ( ) Otro. Indique: _____
9. ¿Existe actualmente en su organización, algún documento o consentimiento informado	( ) Sí. (X) No.

Preguntas	Opciones de respuesta
que los usuarios deben aceptar al utilizar el chatbot?	
10. Indique cuales, de los siguientes controles de seguridad, se han implementado en su organización para la implementación segura de chatbots:	( ) Validación de entrada de información. ( ) Interacción segura con la BD. ( ) Autenticación de múltiples factores (MFA). (X) Utilización de certificados digitales. (X) Almacenamiento seguro de la información recopilada. ( ) Cumplimiento con regulaciones nacionales. ( ) Cumplimiento con regulaciones internacionales. ( ) Buenas prácticas recomendadas por el fabricante. ( ) Manejo de errores y excepciones en el procesamiento de consultas y respuestas. ( ) Aplicaciones de parches de seguridad. (X) Web Application Firewall (WAF). ( ) Load Balancer (LB). ( ) Next Generation Firewall (NGFW). ( ) Data Loss Prevention (DLP). ( ) Otro. Indique: _____
11. ¿Cuáles de los siguientes mecanismos o técnicas utilizan en su organización para medir el nivel de riesgo de una solución chatbot?	( ) Pruebas de penetración (Pentesting). ( ) Análisis de vulnerabilidades. ( ) Ejecución en ambientes controlados (Sandboxing). (X) Entornos de preproducción y post producción. (X) Pruebas de usabilidad. ( ) Pruebas de estrés. ( ) Otro. Indique: _____
12. ¿Se está tomando en cuenta la privacidad de la información sensible de los usuarios en la utilización de chatbots?	(X) Sí. ( ) No.
13. ¿Tienen los usuarios de su organización el derecho de	(X) Sí. ( ) No.

Preguntas	Opciones de respuesta
solicitar la eliminación de sus datos personales de repositorios de almacenamiento utilizados por los chatbots, después de un periodo de tiempo?	
14. ¿La herramienta y los recursos de interacción propios de la misma (como el API) contienen características para control y manejo de tráfico a lo interno de la red?	( ) Sí. (X) No.

Fuente: Elaboración propia.

Tabla 16: *Respuesta #3 al cuestionario.*

Preguntas	Opciones de respuesta
1. Indique en cuál industria del sector privado se desempeña.	( ) Financiero. (X) Tecnología. ( ) Educación. ( ) Salud. (X) Servicios. ( ) Transporte. ( ) Turismo. ( ) Mercadeo. ( ) Otro. Indique: _____
2. ¿Qué tipo de implementación de chatbot, posee su organización?	( ) Página web. ( ) App móvil. ( ) App IM/Chat. ( ) App inteligente. (X) Otro. Indique: __Desarrollamos para clientes de GBM__
3. ¿El chatbot implementado en su organización fue desarrollado a lo interno o adquirido por medio de un tercero?	(X) Desarrollo interno. ( ) Tercero. ( ) Otros. Indique: _____

Preguntas	Opciones de respuesta
3.1 Si se desarrolló interno: ¿Se contemplaron las buenas prácticas vigentes en la industria para el Ciclo de Vida de Desarrollo Seguro de Software (S-SDLC)?	(X) Sí. ( ) No.
~~3.2 Si es de un tercero o contesta "Otros":~~ ~~¿Se consideró la seguridad como un aspecto importante de la evaluación de la solución?~~	~~( ) Sí.~~ ~~( ) No.~~
4. ¿Con que tipo de servicios interactúa el chatbot de forma principal en su organización?	Indique: _AWS, AZURE, SAP_
5. ¿La herramienta se está utilizando como parte de los procesos / funciones de ciberseguridad?	( ) Sí. (X) No.
6. En la implementación de chatbot existente, ¿se consideró el cifrado como un elemento indispensable para la comunicación y manejo de datos en general?	(X) Sí. ( ) No.
7. ¿La herramienta se utiliza para uso interno, externo o ambos?	( ) Interno. (X) Externo. ( ) Ambos.
8. ¿La información obtenida por medio del Chatbot, es utilizada como beneficio empresarial para la mejora de interacción, servicios o consumo con un tercero? Seleccione las que aplique.	(X) Mejora de interacción. (X) Mejora de Servicios. (X) Consumo de un tercero. ( ) Otro. Indique: _____
9. ¿Existe actualmente en su	(X) Sí.

Preguntas	Opciones de respuesta
organización, algún documento o consentimiento informado que los usuarios deben aceptar al utilizar el chatbot?	( ) No.
10. Indique cuales, de los siguientes controles de seguridad, se han implementado en su organización para la implementación segura de chatbots:	(X) Validación de entrada de información. (X) Interacción segura con la BD. ( ) Autenticación de múltiples factores (MFA). (X) Utilización de certificados digitales. (X) Almacenamiento seguro de la información recopilada. (X) Cumplimiento con regulaciones nacionales. (X) Cumplimiento con regulaciones internacionales. (X) Buenas prácticas recomendadas por el fabricante. (X) Manejo de errores y excepciones en el procesamiento de consultas y respuestas. (X) Aplicaciones de parches de seguridad. (X) Web Application Firewall (WAF). ( ) Load Balancer (LB). ( ) Next Generation Firewall (NGFW). (X) Data Loss Prevention (DLP). ( ) Otro. Indique: _____
11. ¿Cuáles de los siguientes mecanismos o técnicas utilizan en su organización para medir el nivel de riesgo de una solución chatbot?	(X) Pruebas de penetración (Pentesting). (X) Análisis de vulnerabilidades. (X) Ejecución en ambientes controlados (Sandboxing). (X) Entornos de preproducción y post producción. (X) Pruebas de usabilidad. (X) Pruebas de estrés. ( ) Otro. Indique: _____
12. ¿Se está tomando en cuenta la privacidad de la información sensible de los usuarios en la utilización de chatbots?	(X) Sí. ( ) No.

Preguntas	Opciones de respuesta
13. ¿Tienen los usuarios de su organización el derecho de solicitar la eliminación de sus datos personales de repositorios de almacenamiento utilizados por los chatbots, después de un periodo de tiempo?	(X) Sí. ( ) No.
14. ¿La herramienta y los recursos de interacción propios de la misma (como el API) contienen características para control y manejo de tráfico a lo interno de la red?	(X) Sí. ( ) No.

Fuente: Elaboración propia.

Tabla 17: *Respuesta #4 al cuestionario.*

Preguntas	Opciones de respuesta
1. Indique en cuál industria del sector privado se desempeña.	(X) Financiero. ( ) Tecnología. ( ) Educación. ( ) Salud. ( ) Servicios. ( ) Transporte. ( ) Turismo. ( ) Mercadeo. ( ) Otro. Indique: _____
2. ¿Qué tipo de implementación de chatbot, posee su organización?	(X) Página web. ( ) App móvil. ( ) App IM/Chat. ( ) App inteligente. ( ) Otro. Indique: _____
3. ¿El chatbot implementado en su organización fue desarrollado a lo interno o	( ) Desarrollo interno. (X) Tercero. ( ) Otros. Indique: _____

Preguntas	Opciones de respuesta
adquirido por medio de un tercero?	
~~3.1 Si se desarrolló interno:~~ ~~¿Se contemplaron las buenas prácticas vigentes en la industria para el Ciclo de Vida de Desarrollo Seguro de Software (S-SDLC)?~~	~~( ) Sí.~~ ~~( ) No.~~
3.2 Si es de un tercero o contesta “Otros”: ¿Se consideró la seguridad como un aspecto importante de la evaluación de la solución?	(X) Sí. ( ) No.
4. ¿Con que tipo de servicios interactúa el chatbot de forma principal en su organización?	Indique: _Sitio web_
5. ¿La herramienta se está utilizando como parte de los procesos / funciones de ciberseguridad?	( ) Sí. (X) No.
6. En la implementación de chatbot existente, ¿se consideró el cifrado como un elemento indispensable para la comunicación y manejo de datos en general?	(X) Sí. ( ) No.
7. ¿La herramienta se utiliza para uso interno, externo o ambos?	( ) Interno. (X) Externo. ( ) Ambos.
8. ¿La información obtenida por medio del Chatbot, es utilizada como beneficio empresarial para la mejora de interacción, servicios o consumo con un tercero? Seleccione las que	(X) Mejora de interacción. (X) Mejora de Servicios. ( ) Consumo de un tercero. ( ) Otro. Indique: _____

Preguntas	Opciones de respuesta
aplique.	
9. ¿Existe actualmente en su organización, algún documento o consentimiento informado que los usuarios deben aceptar al utilizar el chatbot?	(X) Sí. ( ) No.
10. Indique cuales, de los siguientes controles de seguridad, se han implementado en su organización para la implementación segura de chatbots:	(X) Validación de entrada de información. (X) Interacción segura con la BD. ( ) Autenticación de múltiples factores (MFA). (X) Utilización de certificados digitales. (X) Almacenamiento seguro de la información recopilada. (X) Cumplimiento con regulaciones nacionales. ( ) Cumplimiento con regulaciones internacionales. (X) Buenas prácticas recomendadas por el fabricante. (X) Manejo de errores y excepciones en el procesamiento de consultas y respuestas. (X) Aplicaciones de parches de seguridad. (X) Web Application Firewall (WAF). (X) Load Balancer (LB). (X) Next Generation Firewall (NGFW). (X) Data Loss Prevention (DLP). (X) Otro. Indique: _Inteligencia artificial_
11. ¿Cuáles de los siguientes mecanismos o técnicas utilizan en su organización para medir el nivel de riesgo de una solución chatbot?	(X) Pruebas de penetración (Pentesting). (X) Análisis de vulnerabilidades. ( ) Ejecución en ambientes controlados (Sandboxing). ( ) Entornos de preproducción y post producción. (X) Pruebas de usabilidad. ( ) Pruebas de estrés. ( ) Otro. Indique: _____
12. ¿Se está tomando en cuenta la privacidad de la información	(X) Sí. ( ) No.

Preguntas	Opciones de respuesta
sensible de los usuarios en la utilización de chatbots?	
13. ¿Tienen los usuarios de su organización el derecho de solicitar la eliminación de sus datos personales de repositorios de almacenamiento utilizados por los chatbots, después de un periodo de tiempo?	(X) Sí. ( ) No.
14. ¿La herramienta y los recursos de interacción propios de la misma (como el API) contienen características para control y manejo de tráfico a lo interno de la red?	(X) Sí. ( ) No.

Fuente: Elaboración propia.

Tabla 18: *Respuesta #5 al cuestionario.*

Preguntas	Opciones de respuesta
1. Indique en cuál industria del sector privado se desempeña.	( ) Financiero. ( ) Tecnología. ( ) Educación. ( ) Salud. ( ) Servicios. ( ) Transporte. (X) Turismo. ( ) Mercadeo. ( ) Otro. Indique: _____
2. ¿Qué tipo de implementación de chatbot, posee su organización?	(X) Página web. ( ) App móvil. ( ) App IM/Chat. ( ) App inteligente. ( ) Otro. Indique: _____
3. ¿El chatbot implementado en	( ) Desarrollo interno.

Preguntas	Opciones de respuesta
su organización fue desarrollado a lo interno o adquirido por medio de un tercero?	(X) Tercero. ( ) Otros. Indique: _____
~~3.1 Si se desarrolló interno:~~ ~~¿Se contemplaron las buenas prácticas vigentes en la industria para el Ciclo de Vida de Desarrollo Seguro de Software (S-SDLC)?~~	~~( ) Sí.~~ ~~( ) No.~~
3.2 Si es de un tercero o contesta "Otros": ¿Se consideró la seguridad como un aspecto importante de la evaluación de la solución?	(X) Sí. ( ) No.
4. ¿Con que tipo de servicios interactúa el chatbot de forma principal en su organización?	Indique: _Información para respuesta a turistas a partir de sitio web _
5. ¿La herramienta se está utilizando como parte de los procesos / funciones de ciberseguridad?	( ) Sí. (X) No.
6. En la implementación de chatbot existente, ¿se consideró el cifrado como un elemento indispensable para la comunicación y manejo de datos en general?	(X) Sí. ( ) No.
7. ¿La herramienta se utiliza para uso interno, externo o ambos?	( ) Interno. (X) Externo. ( ) Ambos.
8. ¿La información obtenida por medio del Chatbot, es utilizada como beneficio empresarial para la mejora de interacción,	(X) Mejora de interacción. (X) Mejora de Servicios. ( ) Consumo de un tercero. ( ) Otro. Indique: _____

Preguntas	Opciones de respuesta
servicios o consumo con un tercero? Seleccione las que aplique.	
9. ¿Existe actualmente en su organización, algún documento o consentimiento informado que los usuarios deben aceptar al utilizar el chatbot?	( ) Sí. (X) No.
10. Indique cuales, de los siguientes controles de seguridad, se han implementado en su organización para la implementación segura de chatbots:	( ) Validación de entrada de información. ( ) Interacción segura con la BD. ( ) Autenticación de múltiples factores (MFA). (X) Utilización de certificados digitales. ( ) Almacenamiento seguro de la información recopilada. (X) Cumplimiento con regulaciones nacionales. ( ) Cumplimiento con regulaciones internacionales. ( ) Buenas prácticas recomendadas por el fabricante. ( ) Manejo de errores y excepciones en el procesamiento de consultas y respuestas. (X) Aplicaciones de parches de seguridad. (X) Web Application Firewall (WAF). ( ) Load Balancer (LB). (X) Next Generation Firewall (NGFW). ( ) Data Loss Prevention (DLP). ( ) Otro. Indique: _____
11. ¿Cuáles de los siguientes mecanismos o técnicas utilizan en su organización para medir el nivel de riesgo de una solución chatbot?	( ) Pruebas de penetración (Pentesting). ( ) Análisis de vulnerabilidades. ( ) Ejecución en ambientes controlados (Sandboxing). ( ) Entornos de preproducción y post producción. (X) Pruebas de usabilidad. ( ) Pruebas de estrés. ( ) Otro. Indique: _____

Preguntas	Opciones de respuesta
12. ¿Se está tomando en cuenta la privacidad de la información sensible de los usuarios en la utilización de chatbots?	(X) Sí. ( ) No.
13. ¿Tienen los usuarios de su organización el derecho de solicitar la eliminación de sus datos personales de repositorios de almacenamiento utilizados por los chatbots, después de un periodo de tiempo?	( ) Sí. (X) No.
14. ¿La herramienta y los recursos de interacción propios de la misma (como el API) contienen características para control y manejo de tráfico a lo interno de la red?	(X) Sí. ( ) No.

Fuente: Elaboración propia.

Tabla 19: *Respuesta #6 al cuestionario.*

Preguntas	Opciones de respuesta
1. Indique en cuál industria del sector privado se desempeña.	(X) Financiero. ( ) Tecnología. ( ) Educación. ( ) Salud. ( ) Servicios. ( ) Transporte. ( ) Turismo. ( ) Mercadeo. ( ) Otro. Indique: _____
2. ¿Qué tipo de implementación de chatbot, posee su organización?	( ) Página web. ( ) App móvil. ( ) App IM/Chat. ( ) App inteligente.

Preguntas	Opciones de respuesta
	( ) Otro. Indique: _RPA_
3. ¿El chatbot implementado en su organización fue desarrollado a lo interno o adquirido por medio de un tercero?	( ) Desarrollo interno. (X) Tercero. ( ) Otros. Indique: _____
~~3.1 Si se desarrolló interno:~~ ~~¿Se contemplaron las buenas prácticas vigentes en la industria para el Ciclo de Vida de Desarrollo Seguro de Software (S-SDLC)?~~	~~( ) Sí.~~ ~~( ) No.~~
3.2 Si es de un tercero o contesta "Otros": ¿Se consideró la seguridad como un aspecto importante de la evaluación de la solución?	(X) Sí. ( ) No.
4. ¿Con que tipo de servicios interactúa el chatbot de forma principal en su organización?	Indique: _Automatización de procesos_
5. ¿La herramienta se está utilizando como parte de los procesos / funciones de ciberseguridad?	(X) Sí. ( ) No.
6. En la implementación de chatbot existente, ¿se consideró el cifrado como un elemento indispensable para la comunicación y manejo de datos en general?	(X) Sí. ( ) No.
7. ¿La herramienta se utiliza para uso interno, externo o ambos?	( ) Interno. ( ) Externo. (X) Ambos.
8. ¿La información obtenida por medio del Chatbot, es utilizada	( ) Mejora de interacción. (X) Mejora de Servicios.

Preguntas	Opciones de respuesta
como beneficio empresarial para la mejora de interacción, servicios o consumo con un tercero? Seleccione las que aplique.	( ) Consumo de un tercero. ( ) Otro. Indique: _____
9. ¿Existe actualmente en su organización, algún documento o consentimiento informado que los usuarios deben aceptar al utilizar el chatbot?	( ) Sí. (X) No.
10. Indique cuales, de los siguientes controles de seguridad, se han implementado en su organización para la implementación segura de chatbots:	( ) Validación de entrada de información. ( ) Interacción segura con la BD. ( ) Autenticación de múltiples factores (MFA). (X) Utilización de certificados digitales. (X) Almacenamiento seguro de la información recopilada. (X) Cumplimiento con regulaciones nacionales. (X) Cumplimiento con regulaciones internacionales. (X) Buenas prácticas recomendadas por el fabricante. (X) Manejo de errores y excepciones en el procesamiento de consultas y respuestas. (X) Aplicaciones de parches de seguridad. (X) Web Application Firewall (WAF). ( ) Load Balancer (LB). (X) Next Generation Firewall (NGFW). ( ) Data Loss Prevention (DLP). ( ) Otro. Indique: _____
11. ¿Cuáles de los siguientes mecanismos o técnicas utilizan en su organización para medir el nivel de riesgo de una solución chatbot?	( ) Pruebas de penetración (Pentesting). (X) Análisis de vulnerabilidades. (X) Ejecución en ambientes controlados (Sandboxing). ( ) Entornos de preproducción y post producción. ( ) Pruebas de usabilidad.

Preguntas	Opciones de respuesta
	( ) Pruebas de estrés. ( ) Otro. Indique: _____
12. ¿Se está tomando en cuenta la privacidad de la información sensible de los usuarios en la utilización de chatbots?	(X) Sí. ( ) No.
13. ¿Tienen los usuarios de su organización el derecho de solicitar la eliminación de sus datos personales de repositorios de almacenamiento utilizados por los chatbots, después de un periodo de tiempo?	(X) Sí. ( ) No.
14. ¿La herramienta y los recursos de interacción propios de la misma (como el API) contienen características para control y manejo de tráfico a lo interno de la red?	(X) Sí. ( ) No.

Fuente: elaboración propia.