Creación de una infraestructura en la nube para ser utilizada como un ambiente estable y protegido en la Caja Costarricense de Seguro Social

Creation of an infrastructure on the cloud to be used as a stable and protected environment on the Caja Costarricense de Seguro Social

Jesús Martínez Alvarado[1],

Sebastián Ríos Luna[2],

Julio Córdoba Retana[3],

Universidad Latinoamericana de Ciencia y Tecnología

2022

Resumen

Según la PwC Interamericana, desde el mes de abril de 2022, varias entidades gubernamentales costarricenses fueron víctimas de un ataque con ransomware por el grupo Conti, que sustrajo al menos un terabyte de datos del gobierno. Los ataques interrumpieron numerosos servicios gubernamentales, incluidos, las plataformas de impuestos y aduanas del país, los servicios digitales de tesorería y al menos un proveedor de energía (p. 1). Por esta razón, la Caja Costarricense de Seguro Social está tomando en cuenta, como un tema clave, la seguridad y sostenibilidad de sus recursos tecnológicos. Fortalecer la seguridad e integridad de recursos tecnológicos en cualquier institución o asociación es de gran importancia, debido a que cada vez dependemos más de la sostenibilidad de la tecnología. Por eso, se formuló la siguiente pregunta de investigación: ¿Cómo construir e implementar los servicios de la nube para obtener una nueva infraestructura tecnológica en la Caja Costarricense de Seguro Social? El alcance de la investigación es obtener la percepción de los profesionales sobre aspectos de recursos e infraestructuras en la nube, como la de los funcionarios públicos dentro de la gestión de la Caja Costarricense de Seguro Social, en cuanto a la seguridad de la infraestructura de la actualidad y las buenas prácticas que se pueden implementar en esta nueva infraestructura.

Palabras clave: ransomware, Caja Costarricense de Seguro Social, infraestructura en la nube, recursos tecnológicos.

[1] Jesús Martínez Alvarado: Ingeniero en Sistemas. Con más de 5 años de experiencia en TI. Laborando, actualmente, para Microsoft.
Orcid: 0000-0002-4165-1577
Correo electrónico: jesmart18@outlook.com

[2] Sebastián Ríos Luna: Ingeniero en Sistemas. Con más de 2 años de experiencia en Diseño Web. Laborando, actualmente, para Source 360 Group como Front End Developer/Software Specialist.
Orcid: 0000-0001-1748-0896
Correo electrónico: serilu1960@gmail.com

[3] Julio Córdoba Retana: Especialista en innovación. Con más de 20 años de experiencia en la gestión tecnológica en el mercado financiero latinoamericano, en organizaciones como BAC Credomatic, Promerica, DaVivienda y Colpatria. Ha dirigido la innovación para clientes en Centroamérica, Panamá, República Dominicana, México, Colombia y Ecuador. Ha acompañado a más de 50 clientes en América Latina en la introducción de prácticas como Customer Experience, Design Thinking, Lean, Scrum, Kanban, Agilismo Escalado (SAFe), CMMi 2.0, ISO 9001, ITIL y COBIT. Dirigió con éxito la certificación de Grupo Babel en ISO 9001:2015 y la evaluación de CMMi Dev Nivel 3.
Orcid: 0000-0002-1700-2358
Correo electrónico: jcordobar022@ulacit.ed.cr

Abstract

According to the Inter-American PwC, since April 2022, several Costa Rican government entities were victims of a ransomware attack by the Conti group, which stole at least one terabyte of government data. The attacks disrupted numerous government services, including the country's tax and customs platforms, digital treasury services, and at least one energy provider (p. 1). For this reason, the Costa Rican Social Security Fund is considering the security and sustainability of its technological resources as a key issue. Strengthening the security and integrity of technological resources in any institution or association is of great importance, since we increasingly depend on the sustainability of technology. For this reason, the following research question was formulated: How to build and implement cloud services to obtain a new technological infrastructure in the Costa Rican Social Security Fund? The scope of the research is to obtain the perception of professionals on aspects of resources and infrastructures in the cloud, such as that of public officials within the management of the Caja Costarricense de Seguro Social, in terms of current infrastructure security and good practices that can be implemented on this new infrastructure.

Keywords: ransomware, Caja Costarricense de Seguro Social, cloud infrastructure, technological resources.

Introducción

Año 2020, momento en el cual inicia una de las etapas más impactantes a nivel mundial el COVID-19. En esta etapa se detiene por un instante el mundo y cada país se detiene a pensar sobre lo que está sucediendo, mientras miles de personas se encuentran en cama muriendo y también es una fase durante la que el progreso económico se vio afectado. Por otro lado, está el 2022 donde surge la reactivación económica ya las personas regresan a sus trabajos, las organizaciones empiezan a retomar funciones como lo hacían previo a la pandemia y con esto se potencian las actividades delictivas que vuelven a cobrar vida.

Por su parte, la tecnología ha evolucionado de forma exponencial y ya la mayoría de las actividades se manejan con el uso del internet, un claro ejemplo de este avance es que la interacción física hoy es mínima. Por ejemplo, en una empresa dada donde es requerida la administración de servidores, hace algunos años se necesitaba la operación de al menos 5 ingenieros enfocados en diferentes tareas, pero actualmente, con la llegada de la tercerización de servicios y las plataformas virtuales, con una persona es más que suficiente para realizar dicha tarea, dado que esta es la encargada de administrar la plataforma donde residen los servicios necesarios para la organización. No obstante, muchas organizaciones no tienen clara la importancia de los servicios alojados en plataformas conocidas como la nube, razón por la cual surge esta investigación.

Asimismo, las plataformas de gestión de la nube (*Cloud Management Platforms*, CMP) son productos que proporcionan una plataforma para la gestión de entornos tanto en *nubes* públicas, privadas, híbridas o ambientes multi-nube. Los servicios ofrecidos por un CMP varían según el proveedor, sin embargo, todos ellos se integran en un solo entorno, un conjunto de herramientas de software destinadas para el autoaprovisionamiento y la gestión del funcionamiento de la nube (Guijarro, Caparrós y Cubero, 2020).

De esta manera, es importante destacar que durante la última década la seguridad informática se ha visto comprometida de manera grave, ya que grupos masivos de individuos, con conocimientos amplios en informática, pretenden *hackear* sistemas informáticos, entiéndase el término hackear o *hacking* en inglés como "la identificación de una debilidad en sistemas informáticos y/o redes y explotar esa debilidad para obtener acceso" (Nordeen, 2020).

Sin embargo, no solamente la tecnología ha avanzado, también lo han hecho los criminales o como son conocidos en internet, "*hacker*". Como lo define la Avast Academy (2022) "es la aplicación de tecnología o conocimientos técnicos para superar alguna clase de problema u obstáculo. Nótese que nuestra definición no incluye, intencionadamente, nada de naturaleza delictiva. Aunque muchos hackers pueden utilizar sus habilidades con fines malvados, y de hecho lo hacen, y aunque mucha gente asocia el hackeo únicamente con el hackeo delictivo o de seguridad, el concepto va más allá".

Tal es el caso de Costa Rica, ya que se convirtió en el objetivo de un grupo de *hackers* y han atacado varias organizaciones a nivel nacional entres las cuales se pueden mencionar: el Ministerio de Hacienda y la Caja Costarricense de Seguro Social (CCSS). Estos acontecimientos han llegado a ser tan severos que la efectividad de las organizaciones gubernamentales se ha visto directamente afectada, pues dichas instituciones han tenido que implementar nuevamente procesos tradicionales y poco eficientes a la hora de realizar trámites.

Del mismo modo, es fundamental conocer cómo puede ser utilizado e implementado un entorno o infraestructura que sea estable y segura para la CCSS, sobre todo, debido a los acontecimientos que ocurrieron durante el 2022. Dicho ciberataque hacia los servidores de la CCSS dejó a toda la institución vulnerable y además la CCSS no contaba con un plan de contingencia durante el ciberataque, sin embargo, días después del ataque el Ministerio de Salud avaló un plan de contingencia que asegura la continuidad de la vigilancia de eventos de la salud pública (Ministerio de Salud de Costa Rica, 2022).

Por ello, es importante mencionar que dicho plan de contingencia está enfocado en la detección y cuidado de pacientes que posean muestras positivas de COVID-19. Un enunciado por el Ministerio de Salud indica lo siguiente, "Es importante aclarar, que, a partir de la oficialización de esta instrucción (plan de contingencia), la CCSS priorizará la toma de muestras por COVID-19 para los pacientes que tengan condiciones de riesgo clínico-epidemiológico, según lo establece el Lineamiento de Vigilancia de COVID-19 del Ministerio de Salud vigente" (Ministerio de Salud de Costa Rica, 2022).

Así, la mayoría de los servicios y procesos que se realizaban de forma digital, por parte de la organización, tuvieron que sufrir un cambio radical e implementar una metodología tradicional y arcaica que impactó de forma grave la eficiencia y estabilidad de dichos procesos. No solo los funcionarios públicos y los procedimientos de la CCSS fueron impactados, también mucha de la información sobre los pacientes fue suprimida, como, por ejemplo, citas médicas, estados de salud acerca de los pacientes e internados, información registrada dentro del Expediente Digital Único en Salud (EDUS), información acerca del seguro social de las personas que utilizan la CCSS como centro de salud, entre otras.

Justamente, uno de los mayores impactos consistió en que muchas personas que estaban en tratamientos críticos se quedaron sin la información sobre el proceso de recuperación, ya que fue borrada, lo cual impide comparar el desarrollo de dichos tratamientos y esto puede acarrear trágicas y fatales consecuencias. Por ejemplo, pacientes que están siendo tratados por cáncer o metástasis avanzada, pues su proceso de recuperación puede llegar a ser directamente afectado, debido a que no se puede llegar a examinar o verificar los resultados capturados antes del incidente informático.

Por su parte, otro impacto significativo, que sucedió como consecuencia del ataque cibernético, fue la afectación en la solicitud de citas médicas en los centros de salud. Muchas personas que ocupaban una cita médica, normalmente solicitaban la cita vía internet o por la aplicación EDUS, sin embargo, con este gran impacto, las citas tienen que solicitarse de manera presencial, lo cual afecta de manera directa la eficiencia de la CCSS al atender pacientes que lo requieren.

Pregunta de investigación

¿Cómo construir e implementar los servicios de la nube para obtener una nueva infraestructura tecnológica en la Caja Costarricense de Seguro Social?

Objetivo general

Crear una infraestructura en la nube segura y de alta disponibilidad que pueda ser implementada en la Caja Costarricense de Seguro Social.

Objetivos específicos

1. Descubrir los ataques cibernéticos realizados recientemente contra las organizaciones costarricenses.
2. Compilar un análisis del tipo de infraestructura en la nube, el cual se adapte mejor para impedir nuevos ataques hacia la Caja Costarricense de Seguro Social.
3. Planificar estrategias y guías de conocimiento para educar a todos los funcionarios públicos de Caja Costarricense de Seguro Social sobre la nueva infraestructura.
4. Recomendar las mejores prácticas de desarrollo, implementación y seguridad, las cuales necesita la infraestructura para protegerla de los ciberataques hacia la Caja Costarricense de Seguro Social.

Forma de alcanzar los objetivos

Para lograr los objetivos de la investigación se realizó una revisión bibliográfica en diferentes bases de datos como EBSCOhost, Google Scholar, Google Books, SciELO, artículos periodísticos, así como en sitios web oficiales que adicionalmente se tomaron en cuenta. Se verificó que el contenido fuera confiable y veraz, contribuyendo así con el análisis requerido.

Además, se tomaron en consideración artículos provenientes de organizaciones internacionales como Microsoft y se consideraron puntos de visto de expertos en el tema. También se consultaron los estudios preparados por universidades y de autores independientes que abordan el tema de migración a la nube y la transparencia y flexibilidad que esta brinda.

En último lugar, las encuestas dirigidas a actores claves en el tema de estudio representan fuentes primarias de información, requeridas para el desarrollo de la investigación.

Revisión bibliográfica

Hoy, surgen ataques cibernéticos en cualquier momento y son dirigidos hacia organizaciones importantes, tanto nacionales como internacionales. Este es un tema de dominio público, es posible encontrarlo en cualquier noticiero. La seguridad informática depende no solo de la integridad de un servidor, sino también de mantener la privacidad de la información, la cual se encuentra inmersa en dichos servidores. Así, la vulnerabilidad puede implicar un compromiso en la información de los pacientes de la CCSS, ya que esta se presenta en la organización como se puede leer a continuación:

> Los ataques cibernéticos en Costa Rica han alcanzado a 27 instituciones estatales en el último mes y nueve de ellas están "muy afectadas", informó este lunes el presidente del país centroamericano, Rodrigo Chaves, al reconocer un impacto "enorme" en el comercio exterior y la recaudación de impuestos... El Ministerio de Hacienda tiene desactivados los sistemas usuales de cobro de impuestos, lo que impide a miles de contribuyentes hacer sus declaraciones, mientras un sistema alternativo solo atenúa la salida de operaciones de la plataforma aduanera para exportaciones e importaciones, dijo Chaves. (Reuters, 2022)

De esta manera, se evidencia la afectación por la falta de uso de recursos o plataformas tecnológicas actuales. Por eso es necesaria la guía de cómo utilizar estos. A continuación, se puede identificar los tipos de infraestructuras existentes.

Primeramente, las características básicas de una infraestructura en la nube conocida como Infraestructura como Servicio (IaaS) son recopiladas en la definición planteada por la Universidad Católica de Cuenca por Muñoz y Zhindón (2020):

> La infraestructura como servicio (IaaS) funciona según el llamado principio de corresponsabilidad o responsabilidad compartida (*shared responsability mencionado en inglés*), según el cual el proveedor y su cliente se ocupan de tareas diferentes, necesarias para poder hacer uso o aprovisionar los recursos de la nube de la forma más adecuada. (p. 1539)

De este modo, el proveedor (el operador de IaaS) se encargará de realizar una administración, la cual incluye mantener actualizados los centros de datos donde parte de los puntos considerados son la protección contra factores externos, asegurar que dichos equipos cuentan con los recursos necesarios para ejecutar las tareas en términos de la unidad central de procesamiento (CPU), acceso aleatorio de memoria (RAM) y memoria de almacenamiento. Adicionalmente, está encargado de proveer estructuras de servidor, red y bases de datos. En lo que respecta al funcionamiento, se tiene que crear un entorno de virtualización con el que los clientes puedan acceder a los recursos de IaaS que ofrece y además, es necesario suministrar el software con el cual los clientes puedan administrar la infraestructura virtualizada.

Por otro lado, el usuario también tiene algunas tareas que considerar y debe realizar ciertas configuraciones con base en los requerimientos del negocio, según se puede apreciar a continuación, ya que es necesario seleccionar y organizar la infraestructura virtual que se desea donde se deben ejecutar ciertas tareas una vez definido el tipo de infraestructura y para el caso de máquinas virtuales hay que instalar, configurar y actualizar constantemente los sistemas operativos y los programas que utilice la empresa para sus propios objetivos. Proteger los sistemas operativos incluyendo el software instalado esto toma en cuenta también las aplicaciones propias al utilizar programas de seguridad. Este tema de seguridad es algo que no se debe dejar de lado por la que existe una gran importancia de cifrar los datos y las conexiones de datos en reposo y algo que se trabaja en forma conjunta es la configuración de mecanismos de autentificación y controles de identidad y acceso.

Adicionalmente, existen otros modelos de servicio, los cuales pueden llegar a ser complementarios junto al IaaS y estos se pueden definir como una:

> Plataforma como servicio (PaaS): Incluye el diseño, desarrollo y hospedaje de aplicaciones. Otros servicios incluyen colaboración, integración de base de datos, seguridad, servicio web integración, escalado, etc. Los usuarios no necesitan preocuparse por tener sus propios recursos de hardware y software o contratar expertos para la gestión de estos recursos y software como servicio (SaaS): los proveedores de servicios en la nube son responsables de ejecutar y mantener el software de aplicación, el sistema operativo y otros recursos. (Rashid y Chaturvedi, 2019)

Precisamente, la CCSS se beneficiaría al implementar una infraestructura en la nube con un enfoque de mayor seguridad, donde sea casi imposible penetrar los puntos de seguridad del IaaS.

Es por eso que una de las grandes compañías de servicios en la nube como Microsoft brinda una gran cantidad de ventajas de dicha implementación, la cual se ilustra en la tabla 1.

Tabla 1

Ventaja de implementación del IaaS	Descripción
Aumenta la estabilidad, la confiabilidad y la compatibilidad	Con IaaS, no hay necesidad de mantener ni actualizar el software y el hardware, ni de solucionar problemas en los equipos. Con el contrato adecuado, el proveedor de servicios garantiza que la infraestructura es confiable y cumple los acuerdos de nivel de servicio.
Mejora la continuidad empresarial y la recuperación ante desastres	Lograr una alta disponibilidad, continuidad empresarial y recuperación ante desastres resulta caro, porque requiere una cantidad importante de tecnología y personal. Pero, con el acuerdo de nivel de servicio adecuado, IaaS ayuda a reducir este costo. También facilita el acceso a las aplicaciones y los datos con normalidad durante un desastre o una interrupción.
Mejora la seguridad	Con el acuerdo de servicio adecuado, un proveedor de servicios en la nube puede ofrecer más seguridad para sus aplicaciones y datos que la que usted pueda alcanzar en su entorno local.
Ayuda a innovar y a entregar las nuevas aplicaciones a los usuarios en menos tiempo	Con IaaS, una vez que haya decidido lanzar un nuevo producto o iniciativa, la infraestructura informática necesaria puede estar lista en cuestión de minutos u horas, en lugar de en días o semanas. Además, como no tiene que configurar la infraestructura subyacente, IaaS le permite entregar las aplicaciones a los usuarios con mayor rapidez.

Nota: Microsoft Azure (2022).

Otro gran proveedor de servicios IaaS es Amazon Web Services o AWS. Además de cumplir con los mismos criterios de aceptación y alcance que Microsoft Azure. Gartner reporta muchas de las ventajas que brinda la solución de IaaS por parte de AWS, en términos de flexibilidad, control y facilidad de configuración.

> AWS no solo tiene una cartera muy amplia de servicios, sino que esos servicios tienen muchas opciones y matices. Esto permite a cada cliente una mayor capacidad de configuración y una adaptación más precisa a las necesidades del cliente. AWS ofrece a los clientes control y flexibilidad sobre cómo definen sus entornos, incluida la topología de la red, los controles de seguridad, la resiliencia, la ubicación

> geográfica y el equilibrio entre precio y rendimiento. Los cimientos de seguridad de AWS son sólidos y proporciona un conjunto completo de funciones y servicios relacionados con la seguridad. Proporciona muchas capacidades para la gestión, operación y gobierno de los entornos de los clientes. La AWS cartera de servicios está cubierta por una amplia gama de certificaciones e informes de cumplimiento. (Leong & Wong, 2021)

Adicionalmente a los diferentes tipos de proveedores de nube que existen, también hay distintos tipos de nube o clasificaciones como se definen a continuación:

> La primera clasificación se refiere a las nubes públicas donde la infraestructura de la nube se pone a disposición del público en general o de un gran grupo industrial y es propiedad de una organización de terceros. Los servicios de nube pública se venden bajo demanda, generalmente, por minutos u horas. Los clientes pagan solo por la CPU, el almacenamiento o el ancho de banda que consumen. Esta es una forma rentable de ofrecer soluciones de TI, especialmente, para las pequeñas y medianas empresas.
>
> Como lo menciona Gartner en su publicación, los líderes en lo que respecta a proveedores en la nube son Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP) sin dejar por fuera a Alibaba Cloud como un visionario (Bala, R. et al, 2021).
>
> Al mismo tiempo, se tiene el concepto de nubes privadas, el cual es posible entenderlo como aquella infraestructura en la nube donde se ofrecen muchos de los mismos beneficios que una nube pública, pero se ejecuta, exclusivamente, para una organización. La nube puede ser administrada por la organización o por un tercero y la infraestructura puede existir en el sitio o fuera del sitio. Las nubes privadas brindan un mayor control sobre la infraestructura de la nube y, a menudo, son ideales para organizaciones más grandes.
>
> Adicionalmente, se tiene lo que se conoce como nubes híbridas donde se da una combinación de una nube pública y una privada, con orquestación y automatización entre las dos. Se utiliza una nube pública para información no crítica y cargas de trabajo máximas que deben escalar según la demanda, mientras que la información confidencial se mantiene en una nube privada controlada por la organización. Una estructura de nube híbrida permite a los usuarios aprovechar la flexibilidad de la nube y conjuntamente aprovechar los beneficios de una infraestructura de TI tradicional. (Attaran & Woods 2019)

No obstante, la implementación de servicios en la nube puede llegar a ser retadora en muchas organizaciones. Por ello, es importante tener conocimiento sobre las implicaciones que esto

conlleva. Antes de tomar una decisión a la ligera sobre la implementación de la nube, cabe destacar que se debe tomar en cuenta la seguridad de la información, pues:

> Los tres pilares de la seguridad informática corresponden a los requisitos de confidencialidad donde solo los usuarios autorizados conocen la información, lo cual evita el acceso malintencionado o no autorizado de esta, integridad se entiende como la capacidad de que solo el personal autorizado podrá modificar la información, ya que esta debe ser siempre exacta y completa, y el requisito de disponibilidad el cual se refiere a que la información sea solo accesible por los usuarios autorizados. Y que la información debe ser disponible cuando sea necesario. Además, existen otros requisitos los cuales son el de autenticación le cual garantiza que el usuario es quien dice ser, no repudio donde asegura que ninguna de las partes involucradas en el manejo de cierta información pueda negar su participación y trazabilidad el cual registra las acciones y en qué momento se han llevado a cabo por parte de un usuario o proceso en el sistema (Postigo, 2020)

Con el fin de cumplir con los requisitos de los pilares de la seguridad de la información, se tiene que a nivel de nube, indistintamente del proveedor del servicio, por lo general existen dos tipos de encriptación que se realizan, los cuales se mencionan seguidamente:

> El cifrado de datos en reposo se ocupa de la información que se almacena en medios físicos independientemente de su formato digital. Los medios pueden incluir todos aquellos datos que residen actualmente en cualquier medio magnético u óptico, datos archivados y copias de seguridad de datos. Está disponible para servicios independientemente del modelo de servicio en la nube...
>
> El cifrado de datos en tránsito se ocupa de los datos que tienen que fluir de una ubicación a otra... Añade otro nivel de seguridad al cifrar los datos en tránsito mediante https... (Chakraborty, Ghosh & Mandal, 2021)

Asimismo, conocer sobre la arquitectura y la funcionalidad de la nube, como se menciona anteriormente, es de gran importancia a nivel técnico, dado que no existe una única estrategia en lo que a la adopción de la nube se refiere, ya que cada organización debe determinar el plan de acción. Sin embargo, se pueden mencionar varios pasos comunes, los cuales usualmente forman parte de dicho proceso. Según Patiño y Valencia (2019), se pueden tomar los pasos que contemplan crear la estrategia y el mapa de TI, determinar la estructura de la computación en la nube, determinar el costo y la selección del proveedor.

Igualmente, es importante recalcar las guías de conocimiento elaboradas por los mismos proveedores. Microsoft tiene un conjunto de documentación sobre guías de implementación y buenas prácticas conocida como *Cloud Adoption Framework* (CAF), según Microsoft se puede entender como:

> Una guía de eficacia probada que se ha diseñado para ayudarle a crear e implementar las estrategias empresariales y tecnológicas necesarias para que todo le vaya bien a su organización en la nube. Ofrece procedimientos recomendados, documentación y herramientas que los arquitectos de la nube, los profesionales de TI y los responsables de la toma de decisiones empresariales necesitan para conseguir sus objetivos a corto y largo plazo. Los procedimientos recomendados de *Cloud Adoption Framework* permiten a las organizaciones alinear mejor sus estrategias empresariales y técnicas para asegurar un resultado satisfactorio. (Microsoft Azure, 2022)

Al surgir la necesidad de la adopción de la nube en una organización enfocada a la salud es importante tomar en cuenta qué tanto se puede estar sin servicio o bien como se conoce en inglés *downtime,* dado que es un término, el cual va de la mano con este son los Service Level Agreements (SLA) y este se puede definir como:

> Un SLA proporciona métricas para medir los niveles de rendimiento de los objetivos de nivel de servicio (SLO). Las pautas de SLA se utilizan para evaluar las implementaciones de servicios en la nube y detectar violaciones de SLO. Los SLA son esenciales para cualquier categoría de procesos subcontratados basados en TI y asumen un lugar dominante en los estándares de gestión de servicios de TI (ITSM) como ITIL. Los proveedores de servicios de TI procesan miles de SLA por día para diferentes inquilinos y distintos tipos de servicios en el panorama informático orientado a servicios (Dhirani y Newe, 2020)

Una vez que se entiende qué es un SLA y cuál es la importancia de este en la contratación de servicios en la nube, se debe tener en cuenta que los distintos proveedores pueden brindar diferentes tipos de SLA en el caso de Microsoft para la nube de Azure se tiene el siguiente ejemplo:

> Diferentes servicios tienen diversos SLA. Office 365 garantiza un tiempo de actividad del 99,9 por ciento. Las máquinas virtuales de instancia única en Azure vienen con una garantía de tiempo de actividad del 99,9 por ciento. Pero esto se puede aumentar al 99,95 % con un conjunto de disponibilidad, e incluso al 99,99 % con dos conjuntos de disponibilidad. Solo para aumentar la complejidad, los SLA pueden interactuar entre sí. Suponga que tiene un balanceador de carga con un SLA del 99,95 % frente a una máquina virtual con un SLA del 99,95 %. Esto equivale a un SLA de solo el 99,9 por ciento (99,95 por ciento * 99,95 por ciento = 99,9 por ciento). Depende de ambos y cada uno puede bajar el 0,05 por ciento del tiempo. Eso da un tiempo de inactividad combinado de 0.1 por ciento. Es vital comprender estos acuerdos de nivel de servicio compuestos. Al menos, deberías al menos entender el concepto. Es muy relevante para su evaluación de a qué se compromete un proveedor de servicios. (Scarfe, Morris, Bennett & Bricknell, 2019)

Cuando se tiene un proyecto para crear e implementar una plataforma en la nube, es recomendado seguir al pie de la letra con las buenas prácticas y recomendaciones que brinda el proveedor y los expertos en el tema acerca de infraestructuras en la nube, según un estudio realizado por *Journal of Economics and Business* estas son las razones de por qué adaptar Microsoft CAF a este tipo de proyectos:

> La decisión de migrar a la nube es una decisión estratégica de la empresa, sin embargo, hay ciertos desencadenantes los cuales que pueden influir en la decisión de basar la empresa en la nube, los cuales son relacionados con temas como los requisitos para nuevas capacidades técnicas, la necesidad de las flexibilidad para cumplir con las necesidades del mercado, costos más bajos, reducir la dependencia del proveedor o la complejidad técnica, aumentar el grado de agilidad, optimización de los procesos de negocio de la empresa, mejorar la experiencia del usuario, cambios en el mercado debido a la aparición de nuevos competidores/productos. (Tatić, Džafić, Haračić & Haračić, 2020)

No obstante, no es necesario solo conocer la nube y conceptos básicos internos de esta al contrario es importante saber que riesgos se tienen tal es el caso, de conocer la definición de que es un ciberataque y ciertos ejemplos de cómo Costa Rica ha tratado de luchar contra estos tipos de amenazas a lo largo de esta era tecnológica. A continuación, se logran distinguir las medidas que ha tomado Costa Rica y también lo que se conoce como ciberataque, según un estudio por la Universidad Nacional de Costa Rica (Mora, Mora, Lizano, Zúñiga y Bolaños, 2019):

> El cibercrimen es un nuevo tipo de delito que se comete en el ciberespacio para realizar actos delictivos. Según el artículo de Pedro Rodríguez, "el concepto de cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el computer hacking, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otros crímenes contrala moralidad y el crimen organizado" ... los ataques cibernéticos, se dan más por vulnerabilidades de software y sistemas como debilidades en el protocolo de cifrado HTTPS o fallas en bibliotecas de desarrollo. Otra de las causas es el Malware o los códigos maliciosos son una preocupación hoy en día. Esta problemática se ha vuelto una preocupación, ya que se dejó de lidiar con incipientes amenazas como los virus, para tener que enfrentar software malicioso cada vez más sofisticado, que tiene un único fin generar ganancias económicas para sus creadores. En Costa Rica el OIJ cuenta desde 1997 con la Sección de Delitos Informáticos, la cual es la encargada de investigar las infracciones de esta índole y otros actos delictivos en donde la informática fue utilizada para la realización de éstos o pueda ser útil para esclarecer la verdad de los hechos. (2019, p 2)

Metodología

Para generar una investigación correcta y alcanzar el objetivo, es fundamental establecer una metodología, la cual deje en evidencia los componentes y actividades de la presente investigación, entre los cuales se pueden mencionar: el enfoque, el tipo de estudio, la muestra, el tipo de muestreo, la hipótesis y los instrumentos de recolección de datos. Esto permite comprender el ¿qué?, ¿quién?, ¿cuándo?, ¿dónde?, ¿cómo? y ¿cuánto? De esta forma, se logra evidenciar la confiabilidad de los datos como fuentes de referencia.

En primera instancia, la presente investigación tiene un enfoque cualitativo, dado que se necesita conocer la opinión de expertos en el tema de la nube con el fin de determinar cuáles factores son imprescindibles en la implementación de una infraestructura segura en la nube. Conjuntamente, se pretende obtener el punto de vista de funcionarios públicos de la CCSS, lo cual es de importancia, ya que ayuda a determinar cómo procedió la institución después del incidente y cómo actuaba antes del mismo. Según lo define Piza, Amaiquema y Beltrán (2029), utiliza como técnica fundamental la observación de realidades subjetivas, donde la naturaleza de la realidad cambia en dependencia de las observaciones y la recolección de datos… Adicionalmente, facilita el aprendizaje de culturas diversas y provee al investigador de diferentes representaciones para explorar el conocimiento y la forma en que los colaboradores comparten sus experiencias.

De esta manera, para lograr comprender profundamente el fenómeno de investigación y responder a las preguntas de estudio, se eligió una muestra de expertos en el tema. Con base a lo mencionado por Conejero (2020) la selección de la muestra corresponde al individuo o grupo a estudiar. Puede ser desde una persona a muchos individuos si se quiere estudiar una población en particular (p. 243). Por lo tanto, se cuenta con la perspectiva y opinión de 6 profesionales que cuentan con conocimiento y experiencia en la nube. Se eligieron expertos que poseen el conocimiento en implementación y soporte de la nube para cuestionar los incidentes enfrentados por las organizaciones públicas en Costa Rica, dando un enfoque en las mejoras que pueden ser aplicadas por parte de la CCSS.

Aunado a ello, se cuenta con la perspectiva de dos funcionarios públicos de la CCSS que poseen conocimiento sobre los acontecimientos provocados por el ciberataque. Con esto se puede tener una perspectiva mucho más amplia del tipo de infraestructura y metodología de proceso, antes y después del incidente con los servidores de la CCSS.

Debido a que se asume un enfoque cualitativo, el proceso de recolección de información y el análisis de los datos es caracterizado repetitivo y frecuente, lo cual significa que se puede realizar todo de manera simultánea o correspondiente. Según un artículo sobre el significado de entrevista (Significados, s.f.), para la recolección de datos e información se realizaron entrevistas a dos distintos grupos seleccionados. Se conoce como entrevista la conversación que sostienen dos o más personas que se encuentran en el rol de entrevistador y entrevistado, a fin de que el primero obtenga del segundo, información sobre un asunto particular. Al tener un enfoque

cualitativo, también pueden existir cambios en la hipótesis general como en el muestreo de datos recolectados, ya que se pueden descubrir nuevas conclusiones mientras se recolectan los datos.

Según Zamorano (2018), una hipótesis es aquella o aquellas guías específicas de lo que se está investigando, aquello que el investigador está buscando y que será el nuevo conocimiento o también todo aquello que una vez concluido se podrá probar. Con base a esta definición, la hipótesis general es que la CCSS sí necesita implementar una nueva infraestructura en la nube (IaaS), enfocándose en implementar las buenas prácticas realizadas por Microsoft CAF y fortalecer la seguridad de esta en el próximo año.

Según Hernández y Carpio (2019), el muestreo se clasifica en dos grandes grupos: probabilísticos y no probabilísticos. Unos son los probabilísticos, basados en el fundamento de equiprobabilidad. Utilizan métodos que buscan que todos los sujetos de una población tengan la misma probabilidad de ser seleccionados para representarla y formar parte de la muestra, generalmente, son los más utilizados porque buscan mayor representatividad. En los métodos no probabilísticos se seleccionan cuidadosamente a los sujetos de la población utilizando criterios específicos, buscando hasta donde sea posible representatividad. Aún así, no se utilizan para la inferencia de resultados sobre la población. Con base a la descripción anterior, la investigación contiene un muestreo de tipo no probabilístico, debido a que se seleccionó un equipo específico de personas a quienes se les realizaron las entrevistas.

Según Vázquez (2022), existen diferentes tipos de entrevistas. Las entrevistas informales y conversacionales son ideales como una primera aproximación en la investigación de campo a través de preguntas abiertas que permiten obtener un contexto rico y detallado. Por otro lado, la entrevista a profundidad consiste en una reunión pactada entre dos personas en la que el entrevistador utiliza una guía de entrevista para ayudar a orientar la conversación hacia los temas de interés.

En nuestro caso, se implementaron entrevistas a profundidad, debido a que se utilizó una guía elaborada antes de la misma, con el fin de lograr profundizar lo más posible en los temas acerca de las infraestructuras en la nube y sobre los acontecimientos sucedidos en la CCSS. También, este tipo de entrevista fue seleccionada para la investigación, dado que permite mantener preguntas semiestructuradas y el orden de estas de manera organizada. Las entrevistas para los expertos en la nube como para los funcionarios públicos de la CCSS se dividieron en dos partes, dicha división se logra distinguir en el apéndice. Cada una de las entrevistas se realizará por medio de Microsoft Teams por parte de los expertos en el área de infraestructura de la nube y de forma presencial con los funcionarios públicos. Cada una de las entrevistas tiene un promedio de 15 a 20 minutos en total.

Discusión de los resultados

Todas las personas entrevistadas cuentan con una amplia experiencia en el área de estudio, se tiene desde ingenieros, los cuales se encargan de dar soporte a la nube y los diferentes servicios

que esta provee; arquitectos, quienes se encargan de realizar el diseño de los ambientes de las organizaciones en la nube y desarrolladores que brindan un punto de vista en referencia a desde cuándo se está construyendo la aplicación tal como aquellos permisos, los cuales deben de existir para asegurarse de que no todas las personas tengan libre acceso a los recursos de la nube y de esta forma, identificar quién y en qué momento realizó una acción dada.

Después de analizar cada una de las respuestas de los encuestados, en su mayoría se tuvo como respuesta que no hay un proveedor perfecto que cuente con el mejor SLA y soporte para la resolución de problemas. Esto a raíz de que, según los comentarios, va a depender de las necesidades del negocio y el contrato adquirido con el proveedor de la nube, ya que se tienen que tomar en cuenta factores tales como el tamaño de la organización, el impacto que un corte de servicio podría tener en el ambiente de producción y el dinero que dicha compañía esté dispuesta a invertir. Esto porque una compañía, la cual invierte una suma alta de dinero, va a tener una atención más pronta que una que contrata servicios básicos, esto es a nivel de contrato de atención al cliente, sin embargo, a nivel de disponibilidad van a tener el mismo porcentaje. Es por esta razón que los SLA entran en juego y es importante comparar cada proveedor con el fin de tomar una decisión guiada.

Del mismo modo, gran parte de los encuestados concuerdan en que para tener un ambiente seguro se debe tener una correcta planeación y definir paso a paso sin dejar nada por fuera. Se deben tomar en cuenta todas las aristas, desde el tipo de nube que se desea implementar hasta la forma en que se hace el despliegue del código de las aplicaciones. Otro punto importante es definir qué significa seguridad para la compañía, debido a que una compañía de venta de autos no tendrá el mismo nivel de seguridad que un banco; por ello se debe tomar en cuenta el apetito del riesgo y así, definir las reglas de seguridad.

Por otra parte, algunos de los encuestados mencionan que existen algunos factores clave para mantener la seguridad en la nube, tal es el uso de un corta fuegos, un dispositivo de red, el cual filtre las solicitudes a los servidores cuando se habla de IaaS tal como el uso de una puerta de enlaces de aplicaciones o el uso de una red privada virtual (VPN). Al mismo tiempo, se menciona el usar redes privadas y utilizar un tipo de emparejamiento de red para acceder a estos recursos en las redes privadas. Por añadidura, un comentario muy importante apunta a no exponer puertos innecesarios a internet, solo los requeridos, dado que esto abre una puerta a los hackers para que sean capaces de robar información.

Por lo demás, se cuenta con un punto de visto, el cual menciona que en muchas ocasiones las compañías no tienen respaldos y por ende si ocurren algún tipo de pérdida de información, ya se accidental por parte de los involucrados en la organización o por un desastre climático, no hay forma de recuperar la información perdida. Es decir, no es posible restaurarla cuando en la nube esto se puede obtener con un par de clics, lo cual asegura la disponibilidad de la información, la integridad de esta y en los grandes proveedores de la nube encriptan la información en diferentes niveles. Además de tener la información al alcance, al habilitar respaldos que ahorran horas de

trabajo en caso de pérdida y no tienen que volver a realizar el trabajo desde cero. Este es un punto de suma importancia, el cual no es tomado en cuenta por muchas organizaciones ni siquiera se menciona cuando se está realizando dicho planeamiento.

Por su parte, una persona encuestada en particular habla sobre la importancia de adherirse al Cloud Adoption Framework (CAF), el cual va a depender de cada proveedor de la nube, dado que las etapas de este pueden variar con base en el proveedor. Sin importar el proveedor, los pasos generales siempre se enfocan en lo mismo, es importante conocer el negocio, determinar aquellos procesos y aplicaciones que son de vital importancia y todas las dependencias que estos contienen, sin dejar de lado el apetito al riesgo que se posee. Este último es esencial, pues se deben tener documentadas aquellas tareas y/o procesos que son críticos para el funcionamiento del negocio.

Según las encuestas realizadas, un tópico que sale a la luz son las regulaciones internas que existen a nivel nacional en lo que respecta al almacenamiento de datos costarricenses en el exterior. Entiéndase esto como bases de datos o archivos que contiene información relacionada con los datos personales que están siendo resguardados en centros de datos ajenos al país. Es primordial saber que se puede entender como datos personales según el Diccionario panhispánico del español jurídico (2019) los datos personales son “cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de otro tipo concerniente a personas físicas identificadas o identificables” (párr. 1.). No obstante, según la investigación realizada, no existe una ley que prive a las organizaciones de guardar la información fuera del territorio nacional, sin embargo, sí existe una clase de consideraciones que se deben tomar en cuenta para cumplir con las leyes de protección de datos.

Con relación a las razones por las cuales las empresas u organizaciones empiezan a adoptar la nube, los encuestados mencionaron los siguientes beneficios: alta flexibilidad para ejecutar un cambio en cuestión de minutos, pues cualquier cambio necesario para adaptar el hardware es sencillo realizarlo desde la plataforma del proveedor de la nube. También se menciona la administración del hardware dado que, independientemente del modelo escogido, una gran parte de la gestión del recurso cae en manos del proveedor de esta. Por ejemplo, a nivel de IaaS, este debe responder a temas relacionados con redes, almacenamiento y virtualización; de esta forma se empieza a obtener un ahorro monetario, debido a que ya no es necesario tener una persona que esté encargada de realizar las tareas de administración de los servidores.

Seguidamente, se devela que los funcionarios públicos de la CCSS entrevistados tienen mucha experiencia en el área de su respectivo enfoque y al tener tanta experiencia se posibilita realizar una comparación entre el antes y el después del ciberataque ocurrido recientemente, debido a que pueden dar una visión clara del funcionamiento de la CCSS como del departamento del área de experiencia.

En el caso del primer entrevistado, menciona que su área de experiencia es la Ortopedia. Según la Biblioteca Nacional de Medicina (2022), la ortopedia o servicios ortopédicos es la

especialidad médica que involucra el tratamiento del sistema musculoesquelético. Incluye huesos, articulaciones, ligamentos, tendones y músculos... Los cirujanos ortopédicos reciben cinco o más años, adicionales de formación después de graduarse. Se especializan en el cuidado de trastornos de los huesos, músculos, tendones y ligamentos. Están capacitados para el manejo de problemas articulares con técnicas quirúrgicas y no quirúrgicas... Los médicos fisiatras y médicos rehabilitadores tienen 4 o más años de formación después de la facultad de medicina. Se especializan en este tipo de atención. También se denominan fisiatras. No realizan cirugías, aunque pueden aplicar inyecciones en las articulaciones.

Por parte del segundo entrevistado, aclara que su área de experiencia es la Radiología. Según la Biblioteca Nacional de Medicina (2022), la radiología diagnóstica les ayuda a los proveedores de atención médica a ver estructuras dentro del cuerpo. Los médicos que se especializan en la interpretación de estas imágenes se denominan radiólogos de diagnóstico. Mediante estas imágenes, el radiólogo u otros médicos con frecuencia pueden: diagnosticar la causa de sus síntomas, vigilar qué tan bien está respondiendo su cuerpo a un tratamiento que se está recibiendo para una enfermedad o afección y detectar diferentes enfermedades como cáncer de mama, cáncer de colon o cardiopatía... Los radiólogos intervencionistas son médicos que utilizan imágenes tales como tomografía computarizada (TC), ecografía, resonancia magnética (RM) y fluoroscopia para ayudar a guiar los procedimientos. Las imágenes son útiles para el médico al introducir catéteres (sondas), alambres y otros instrumentos y herramientas pequeñas en su cuerpo. Esto particularmente se considera para incisiones (cortes) pequeñas.

Otra gran observación por parte de los funcionarios acerca del impacto a la productividad en su trabajo, se refiere a cómo fue un impacto bastante negativo y nefasto. En este caso, el primer entrevistado resalta que es un impacto negativo en la productividad por parte de los pacientes como la productividad de los médicos o funcionarios, debido a que ya no existe acceso al expediente digital. Normalmente, los pacientes deben de actualizar o visualizar su expediente por medio de EDUS para agilizar el proceso que llevan a cabo con la CCSS, al igual que los médicos utilizan el EDUS para visualizar datos o imágenes de gran importancia para el trato de los pacientes. De esta manera, el historial médico, las imágenes, los análisis de laboratorio, entre otros fueron perdidos como consecuencia del ciberataque. La pérdida de estos recursos digitales genera un impacto negativo para la atención del paciente.

Igualmente, el segundo entrevistado aclara que la productividad de todos, dentro de los centros médicos manejados por la CCSS, fue reducida radicalmente. Se destaca que, aunque hayan sufrido de un ciberataque aún reciben la misma cantidad de pacientes, sin embargo, los tratan o reciben de una manera más lenta o ineficiente. Un dato de gran importancia habla de cómo los pacientes oncológicos puede que sean los pacientes más impactados por este ciberataque. Los pacientes oncológicos, debido a su estado es de esencial revisar constantemente sus expedientes de diferentes laboratorios realizados a lo largo de su tratamiento, para llegar a saber si han mejorado o empeorado.

Por su parte, Molina (2016), da una clara idea de lo que sufre un paciente oncológico. El cáncer es un problema sanitario de primera magnitud a escala mundial. Su tratamiento es uno de los mayores campos de innovación y desarrollo en medicina. La visión del cáncer como una enfermedad sistémica, heterogénea y de una elevada complejidad hace que los enfermos deban recibir una atención oncológica de calidad, proporcionada por equipos multidisciplinares altamente cualificados. Además de la gran incidencia de malnutrición en estos pacientes, la intervención nutricional precoz puede mejorar su pronóstico, aumentar la calidad de vida y disminuir la tasa de complicaciones de la enfermedad. Por ello, es necesaria una estrecha colaboración entre el oncólogo y el experto en nutrición.

También se realizaron preguntas acerca del impacto general y en sus respectivas áreas de trabajo a consecuencia del ciberataque. El primer entrevistado recalcó, nuevamente, que no existe forma detallada o concisa de visualizar datos importantes sobre los pacientes. Tanto los médicos como los pacientes deben de acudir a documentos e imágenes físicas para darle continuidad a dicho tratamiento. Otro punto negativo, rescatado de la entrevista habla de cómo muchos de los pacientes tuvieron que repetir exámenes, laboratorios, muestras, entre otros, debido a la pérdida de información a consecuencia del ciberataque.

Esto puede terminar en consecuencias económicas para los pacientes, ya que deben pasar por el mismo proceso, el cual requiere volver a solicitar una cita y gastar fondos monetarios en dicho proceso. Sin embargo, también es una consecuencia económica para la CCSS, debido a que están gastando recursos innecesariamente, ya que están repitiendo estudios a pacientes que en su momento ya habían realizado.

A su vez, el segundo entrevistado, habla sobre lo mismo que recalcó el primer entrevistado, pero alude a que un punto de gran importancia es que el ciberataque impactó en todos los sentidos a la CCSS. Con esto se refiere a la vista de la agenda de citas, la programación de las citas, el otorgar citas para los estudios, el acceso de datos para contactar al cliente. Todos estos aspectos fueron afectados negativamente y son procesos que la CCSS está trabajando para lograr integrar nuevamente de forma eficiente. Adelante, se logra entender el proceso para sacar citas que la CCSS incorporó antes de que sucediera el ciberataque.

Según el Campo Virtual de Salud Pública (2019), la CCSS ofrece el servicio de gestión de citas por internet en el primer nivel de atención, como parte de los programas que forman parte del EDUS. El objetivo es brindar a los usuarios la posibilidad de obtener o cancelar sus citas de medicina general, mediante el uso de internet. Esta herramienta institucional está disponible para la población adscrita a las áreas de salud que tienen el EDUS, alrededor del 40% de las unidades médicas del primer nivel de atención. Esta opción permite a la institución dar más accesibilidad a los usuarios, les brinda una nueva herramienta que ayuda a las personas a no desplazarse hasta las sedes de las áreas de salud y los EBAIS para solicitar citas para la atención médica, reduce las filas y brinda una atención oportuna.

Adicionalmente, se abarcó el tema de las medidas que tomó la CCSS ante este ciberataque. Por parte del primer entrevistado, el cual labora en el Hospital México, indicó que el primer aviso inmediato fue localizar y organizar los expedientes viejos o físicos de todos los pacientes que estaban tratando. Nuevamente se recalca, que este es un proceso bastante tedioso, ya que se está retrocediendo en los pasos de la innovación tecnológica. Además, muchos de los expedientes físicos son escritos a mano y no todos son muy legibles, lo cual atrasa la atención al paciente.

Por el otro lado, el segundo entrevistado define un diferente primer aviso, el cual fue apagar y bloquear todos los sistemas tecnológicos y de comunicación para así evitar que el ciberataque se prolongue y se extienda a otra zona no afectada. Pero, ambos tuvieron el mismo aviso sobre retornar a utilizar expedientes antiguos, en el caso de las placas físicas para los radiólogos. Así,

> la placa o radiografía consiste en la obtención de una imagen radiológica de la zona anatómica que se desea estudiar. Esta imagen surge de la interposición de la zona anatómica a estudio entre una fuente emisora de radiación ionizante (rayos X) y una placa radiográfica o un registro fotográfico digital... El estudio radiológico se realiza en la sala de radiología del centro médico u hospital por parte de un técnico en radiología. El paciente deberá desnudar la zona anatómica a estudio; en algunos casos se le facilitará una bata para cubrirse; al mismo tiempo deberá retirase sus objetos personales, especialmente joyas y objetos metálicos que pueden interferir las imágenes radiológicas. (HIMA, 2022)

Luego, cuando se consultó si la CCSS instauró un nuevo tipo de metodología o procedimientos con sus servidores caídos, ambos entrevistados respondieron que por ahora no existe ningún tipo de implementación nueva. Sin embargo, se menciona que se implementaron soluciones locales y a poca escala, para mantener los servicios médicos para quien los ocupe. Estas soluciones locales son las que se han mencionado anteriormente, como utilizar expedientes viejos y físicos, apagar y bloquear cualquier tipo de servicio tecnológico que utilizan en el trabajo, entre otros.

Según el Instituto Nacional de Psiquiatría (2020), el expediente clínico es un instrumento de gran relevancia para la materialización del derecho a la protección de la salud. Se trata del conjunto único de información y datos personales de un paciente, que puede estar integrado por documentos escritos, gráficos, imagenológicos, electrónicos, magnéticos, electromagnéticos, ópticos, magneto-ópticos y de otras tecnologías, mediante los cuales se hace constar, en diferentes momentos del proceso de la atención médica, las diversas intervenciones del personal del área de la salud, así como describir el estado de salud del paciente; además de incluir en su caso, datos acerca del bienestar físico, mental y social del mismo.

El ultimo extracto de la entrevista habla acerca de las diferencias más importantes entre el antes y el después del ciberataque que sufrió la CCSS. Ambos entrevistados indicaron que los procesos internos como externos se vieron afectados severamente. Describen que el trabajo con los recursos tecnológicos disponibles era mucho más ágil y se tenía una mejor atención al paciente. Se menciona también que mucho del personal trabajador, dentro de los centros médicos, ya

estaban acostumbrados al nuevo sistema tecnológico y su facilidad de acceso. La caída de estos recursos desmotivó a mucho del personal, ya que los procesos se volvieron muy lentos y tediosos a la hora de tratar con un paciente.

Según Guerrero, Amell y Cañedo (2019), en el sentido más amplio,

> la tecnología posibilita transformar el mundo, según las necesidades del hombre. Estas transformaciones pueden obedecer a requerimientos de supervivencia como alimento, higiene, servicios médicos; refugio o defensa o pueden relacionarse con aspiraciones humanas como el conocimiento, el arte o el control. La tecnología es un medio importante para crear entornos físicos y humanos nuevos. Sin embargo, los resultados de cambiar el mundo son impredecibles con frecuencia. Anticiparse a los efectos de la tecnología es tan importante como prever comprender sus potencialidades (p. 2)

Conclusiones y recomendaciones

Con base en el objetivo específico, Descubrir los ataques cibernéticos realizados recientemente contra las organizaciones costarricenses. Al recolectar los datos e información, es importante explicar y recalcar algunas definiciones técnicas para entender, en un nivel más técnico, la experiencia y perspectiva de los funcionarios públicos. Es esencial publicar y comunicar los sucesos o acontecimientos relacionados al ciberataque para así, tomar las medidas requeridas, ya que los pasados ciberataques no fueron documentados ni tomados en cuenta.

Otra recomendación muy importante, a la hora de planificar estrategias y guías de conocimiento para educar a todas las personas funcionarias públicas de la CCSS sobre la nueva infraestructura es utilizar guías anteriores como referencia. Gracias a la información brindada por los entrevistados, sabemos que los funcionarios públicos han tenidos capacitaciones anteriores de todo tipo y el resultado ha sido bastante positivo. La recomendación es utilizar las mismas ideas que las guías de conocimiento anteriores y aplicar los mismos principios, así se puede casi que garantizar que van a tener el mismo resultado y consecuencias.

Asimismo, realizar un estudio de mercado siempre es útil con el fin de determinar cuáles son las características y servicios que los diferentes proveedores brindan. Después de tener clara la necesidad del negocio, esto ayuda a la toma de decisiones.

Justamente, cuando se trabaja en la nube, siempre se tiene un contacto con internet, razón por la cual se deben de tomar una serie de consideraciones con el fin de asegurar que la comunicación de ambos lados no es interceptada por intrusos o individuos ajenos a las partes interesadas de dicha comunicación. La primera acción que se debe tomar es no exponer los puertos de conexión a internet. Tal es el caso de los puertos utilizados para conexiones remotas en el caso de máquinas virtuales Windows el puerto 3389 y para el caso de Linux sería el puerto 22. En el escenario en que sea estrictamente necesario abrir el puerto hacia internet entonces se recomienda cambiar dicho puerto.

Igualmente, es recomendable solo permitir el acceso a ciertos usuarios con permisos similares a los de root y deshabilitar el acceso con root, debido a que es el usuario principalmente utilizado para ejecutar los ataques hacia servidores Linux. Con el fin de realizar cambios en lo que respecta a la conexión a través de ssh en maquina Linux Rai (2022) explica en su libro como realizar dicho cambio

> es necesario solamente abrir el archivo, el cual contiene la configuración del demonio de ssh, el cual responde bajo el nombre sshd_config localizado en la ubicación /etc/ssh y para cambiar el puerto es necesario dirigirse hacia la sección *port* y cambiar el valor 22 por otro puerto disponible y guardar dicho cambio, adicionalmente si SELinux se encuentra habilitado se necesita refrescar dicha configuración para que tome el último cambio esto se hace al correr el comando: *semanage port –a –t ssh_port_t –p tcp #PORTNUMBER.*
>
> Tal y como se hace en Windows es posible realizar el cambio de puerto por defecto para las conexiones remotas en servidores Windows el valor por defecto es 3389 y este es posible ser reemplazado por cualquier otro disponible según Microsoft a continuación los pasos necesarios para cambiar la configuración en un servidor con sistema operativo Windows:
>
> ...la función de Escritorio remoto en su computadora "escucha" la solicitud de conexión a través de un puerto de escucha definido (3389 de manera predeterminada). Puede cambiar ese puerto de escucha en las computadoras con Windows modificando el registro.
>
> - Inicie el editor de registro. (Escriba *regedit* en el cuadro de búsqueda).
> - Navegue a la siguiente subclave del registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
> - Buscar número de puerto.
> - Haga clic en Editar > Modificar y luego haga clic en Decimal.
> - Escriba el nuevo número de puerto y luego haga clic en Aceptar.
> - Cierre el editor de registro y reinicie su computadora.
>
> La próxima vez que se conecte a esta computadora mediante la conexión de Escritorio remoto, debe escribir el nuevo puerto. Si está utilizando un firewall, asegúrese de configurar su firewall para permitir conexiones al nuevo número de puerto (Rai, 2022)

A su vez, se recomienda leer la ley Nº 8968, la cual se enfoca sobre el respeto que se debe mantener sobre los datos que definen a la persona o los bienes que esta posea. Información que también comprende datos personales y confidenciales, tales como los registros de salud.

En efecto, existen otros ataques cibernéticos a otras organizaciones como el Ministerio de Hacienda que tuvieron consecuencias similares a los de la CCSS. Sin embargo, este no es el primer ciberataque que recibe la CCSS. Anteriormente, gracias a la recolección de datos descubrimos que muchos miembros de la CCSS recibían correos clasificados como phishing. Después de analizar los datos, se concluye que las instituciones públicas han recibido varios ataques cibernéticos a lo largo de 5 años.

A raíz de ello, es importante crear y generar estrategias que vayan enfocadas en educar a las personas funcionarias públicas sobre la nueva infraestructura y sobre las nuevas metodologías que implementen después del ciberataque sucedido. Para muchas de las personas funcionarias públicas no fue tan fácil implementar y utilizar nuevas metodologías, debido a que no conocían bien los procesos y métodos tradicionales que la CCSS tuvo que implementar después de la caída de los servidores. Además, antes de que los servidores estuviesen caídos, muchas de las personas funcionarias públicas no sabían utilizar de forma eficiente los recursos tecnológicos disponibles. Esto recalca que es importante guiarlas y educarlas para poder utilizar todos los recursos disponibles de forma efectiva.

En efecto la utilización de la nube brinda un ambiente además de estable seguro para la organización, dado que muchas de las fallas que podrían ocurrir por mano humana desaparecen cuando se trabajan con servicios, los cuales son administrados. Esto no elimina la falla humana, pero se minimiza además de que en un ambiente en la nube todo se encuentra auditado es posible saber en pocos pasos quién hizo un cambio y cuándo lo hizo, siendo este otro enorme beneficio en comparación con los ambientes locales.

Como se observa en el documento anterior, es posible brindar mayor seguridad al ambiente cuando se toman ciertas medidas preventivas. Tal es el cambio de los puertos que se encuentran definidos por defecto se habló de conexiones remotas, no obstante, también es posible cambiar los puertos de conexión a la base de datos y los puertos de *Secure Soccket Layer* (SSL). Aunado a ello, es posible sacar el mayor provecho de las redes virtuales brindadas por el proveedor y las características que estas traen como el uso de redes privadas y el emparejamiento entre redes, de esta forma se crea un servidor que sirva como una caja de salto o *jumpbox* y a partir de este se conecta a los demás recursos necesarios, adicionalmente, gracias a los contratos de SLA se asegura que exista un nivel de disponibilidad del servicio. Es importante aclarar que la nube provee diferentes tipos de disponibilidad que pueden ser utilizados, lo que incrementa el porcentaje de disponibilidad de la solución brindando, una mejorar en esta la varía desde un 99% y es posible que alcance valores hasta con un 99.999%.

En lo que respecta a planificar estrategias con el fin de realizar dicha migración hacia la nube, los proveedores, como se menciona anteriormente, tiene un marco de trabajo de adopción de la nube (CAF), el cual empodera a la organización y le permite elaborar una hoja de ruta tecnológica o *roadmap*, donde este es un plan estratégico que enumera claramente todas las iniciativas tecnológicas que una empresa posee o tiene claras para ser implementadas en un futuro.

Según el punto de vista de uno de los entrevistados, cuando se desarrolla en la nube todo se encuentra controlado por lo que es necesario pedir permisos para instalar un paquete en la solución. Por ejemplo, esta es una evidencia de cómo se debe manejar el tema de desarrollo dentro de la organización. Es decir, implementar marcos de trabajo que permitan limitar las responsabilidades y que no dejan abierto a cualquier miembro pueda ejecutar acciones no autorizadas en el ambiente a través del manejo de roles, los cuales tienen definidas las acciones para que tienen acceso, controlados por el proveedor de la nube es posible cumplir con este requerimiento.

Finalmente, existen regulaciones nacionales que aplican a los datos, sin embargo, no existe una regulación que evite o especifique dónde se deben almacenar estos. Dicho esto, es seguro guardar la información en centros de datos en el exterior, entiéndase este como los centros de datos en Estados Unidos, utilizados por Azure o *Amazon Web Services*. No obstante, se debe cumplir con La ley Nº 8968.

Referencias

AlTwaijiry, A. (2020). The Determinants of Cloud Computing Adoption in Healthcare. *ResearchBerg Review, 1*(1), 9-20. https://doi.org/10.31219/osf.io/56d7b

Attaran, M. & Woods, J. (2019). Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship*, *31*(6), 495-519. https://doi.org/10.1080/08276331.2018.1466850

Bala, R., Gill, B., Smith, D., Ji, K. & Wright, D. (2021). *Magic Quadrant para servicios de infraestructura y plataforma en la nube*. Gartner. https://www.gartner.com/technology/media-products/reprints/AWS/1-271W1OTA-ESP.html

Belcic, I. (2020). *¿Qué es el hackeo?* Avast. https://www.avast.com/es-es/c-hacker

Bruen, A., Forcinito, M., & McQuillan, J. (2021). *Cryptography, Information Theory, and Error-Correction*. (2ª ed.) Wiley. https://books.google.co.cr/books?id=BPcyEAAAQBAJ

Chakraborty, R., Ghosh, A., & Mandal, J. K. (2021). *Machine Learning Techniques and Analytics for Cloud Security*. (1ª ed.) Wiley. https://books.google.co.cr/books?id=-RBSEAAAQBAJ

Conejero, J. (2020). Una aproximación a la investigación cualitativa. *Neumología Pediátrica, 15*(1). https://doi.org/10.51451/np.v15i1.57

Cordero, M. (8 de junio de 2022). Antes del hackeo, Caja recibió 37 oficios de Auditoría Interna con advertencias sobre ciberseguridad. *Semanario Universidad*. https://semanariouniversidad.com/pais/antes-del-hackeo-caja-recibio-37-oficios-de-auditoria-interna-con-advertencias-en-cuanto-a-ciberseguridad

Dhirani, L. & Newe, T. (2020). Hybrid Cloud SLAs for Industry 4.0: Bridging the Gap. *Annals of Emerging Technologies in Computing, 4*(5). https://doi.org/10.33166/aetic.2020.05.003

Guerrero, J., Amell, I. y Cañedo, R. (2019). Tecnología, tecnología médica y tecnología de la salud: algunas consideraciones básicas. *ACIMED, 12*(4). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000400007

Guijarro, J., Caparrós, J. y Cubero, L. (2020). *DevOps y seguridad cloud*. Editorial UOC. https://books.google.co.cr/books?id=hYvcDwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Hernández, C. y Carpio, N. (2019). Introducción a los tipos de muestreo. *Alerta: Revista científica del Instituto Nacional de Salud*. https://alerta.salud.gob.sv/introduccion-a-los-tipos-de-muestreo/

Hospitales HIMA San Pablo. (2022). *¿Qué es una radiografía (Placa)?* Hospitales HIMA San Pablo. https://himasanpablo.com/que-es-una-radiografia/

Instituto Nacional de Psiquiatría Ramón de la Fuente Muñiz. (2020) *¿Qué es el expediente clínico?* http://www.inprf.gob.mx/transparencia/archivos/pdfs/como_solicitar_expediente.pdf

Leong, L. & Wong, A. (2021). *Solution Scorecard for Amazon Web Services IaaS+PaaS*. Gartner. https://www.gartner.com/doc/reprints?id=1-27GFQN50&ct=210916&st=sb

MedlinePlus. (s.f.). *Imagenología y radiología*. MedlinePlus Información de salud para usted. https://medlineplus.gov/spanish/ency/article/007451.htm#:~:text=La%20radiolog%C3%ADa%20es%20una%20rama,radiolog%C3%ADa%20diagn%C3%B3stica%20y%20radiolog%C3%ADa%20intervencionista.

MedlinePlus. (s.f.). *Servicios ortopédicos*. MedlinePlus Información de salud para usted. https://medlineplus.gov/spanish/ency/article/007455.htm#:~:text=La%20ortopedia%2C%20o%20servicios%20ortop%C3%A9dicos,%2C%20ligamentos%2C%20tendones%20y%20m%C3%BAsculos.

Microsoft. (2021). *Change the listening port in Remote Desktop*. Microsoft. https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/change-listening-port

Microsoft Azure. (2022). *Microsoft Cloud Adoption Framework para Azure*. Azure. https://azure.microsoft.com/es-es/overview/cloud-enablement/cloud-adoption-framework/#overview

Microsoft Azure. (2022). *¿Qué es IaaS? Infraestructura como servicio*. Azure. https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-iaas/#overview

Ministerio de Salud de Costa Rica. (2022). *Ministerio de Salud avala plan de contingencia que asegura continuidad de vigilancia de eventos de salud pública*. Ministerio de Salud de Costa Rica. https://www.ministeriodesalud.go.cr/index.php/prensa/52-noticias-2022/1328-ministerio-de-salud-avala-plan-de-contingencia-que-asegura-continuidad-de-vigilancia-de-eventos-de-salud-publica

Molina, R. (2016). El paciente oncológico del siglo XXI: Maridaje terapéutico Nutrición-Oncología. *Nutrición Hospitalaria*, *33*. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S0212-16112016000700002

Mora, C., Mora, M., Lizano, F., Zúñiga, M. y Bolaños, L. (2019). Cultura digital sobre Ataques Cibernéticos un estudio exploratorio en personas jóvenes. https://181.193.125.13/index.php/memorias/article/view/4517/4089

Muñoz, P. y Zhindón, M. (2020). Computación en la nube: la infraestructura como servicio frente al modelo On-Premise. *Revista Científica Dominio de las Ciencias*, *6*(4), 1535-1549. https://www.dominiodelasciencias.com/ojs/index.php/es/article/download/1565/2950

Nordeen, A. (2020). *Hacking: Learn in 24 hours*. https://books.google.co.cr/books?id=NeX8DwAAQBAJ&lpg=PP1&dq=hacker%20types&hl=es&pg=PP1#v=onepage&q=hacker%20types&f=false

Organización Panamericana de la Salud. (2014). *La Caja Costarricense de Seguro Social de Costa Rica ofrece citas por Internet*. https://costarica.campusvirtualsp.org/la-caja-costarricense-de-seguro-social-de-costa-rica-ofrece-citas-por-internet

Patiño, J. y Valencia, A. (2019). Modelo para la Adopción de Cloud Computing en las Pequeñas y Medianas Empresas del Sector Servicios en Medellín, Colombia. *Información tecnológica*, *30*(6), 157-166. https://dx.doi.org/10.4067/S0718-07642019000600157

Piza, N., Amaiquema, F. y Beltrán, G. (2019). Métodos y técnicas en la investigación cualitativa. Algunas precisiones necesarias. *Conrado*, *15*(70). http://scielo.sld.cu/scielo.php?pid=S1990-86442019000500455&script=sci_arttext&tlng=pt

Postigo, A. (2020). *Seguridad informática*. Editorial Paraninfo. https://books.google.co.cr/books?id=UCjnDwAAQBAJ

Rai, V. (2022). *Expert Linux Administration: Guide*. BPB. https://www.google.com/books/edition/Expert_Linux_Administration_Guide/4NZzEAAAQBAJ?hl=es&gbpv=1&dq=change+port+ssh+linux&pg=PA260&printsec=frontcover

Rashid, A. & Chaturvedi, A. (2019). Cloud Computing Characteristics and Services: A Brief Review. *International Journal of Computer Sciences and Engineering*, *7*(2), 421-426.

Real Academia Española. (2019). *Dato de carácter personal*. Diccionario panhispánico del español jurídico. https://dpej.rae.es/lema/dato-de-car%C3%A1cter-personal

Reuters. (2022). *Casi 30 instituciones públicas de Costa Rica golpeadas por ciberataques en el último mes*. América economía. https://www.americaeconomia.com/costa-rica-golpeada-ciberataques

Scarfe, D., Morris, S., Bennett, F. & Bricknell, R. (2019). *Thinking of… Building a Digital Operating Model with Microsoft Cloud Adoption Framework for Azure? Ask the Smart Questions*. Smart Questions. https://azure.microsoft.com/mediahandler/files/resourcefiles/building-a-digital-operating-model-with-microsoft-cloud-adoption-framework/Building%20a%20Digital%20Operating%20Model%20with%20Microsoft%20Cloud%20Adoption%20Framework.pdf

Significados. (s.f.). *Significado de Entrevista*. Significados. https://www.significados.com/entrevista/

Tatić, K., Džafić, Z., Haračić, M. & Haračić, M. (2020). *The analysis of the key drivers and barriers of cloud migration in companies in Bosnia and Herzegovina*. https://web.p.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=10&sid=220c27b9-2fdf-41e0-8731-6bb5f86b2430%40redis

Velásquez, W. (2022). *Herramientas de recolección de datos cualitativos en investigaciones de mercado*. MINDTEC Neuromarketing & consulting. https://www.mindtecbolivia.com/herramientas-recoleccion-datos-cualitativos/

Zamorano, J. (2018). *La hipótesis en la investigación*. UAEH. https://www.uaeh.edu.mx

Apéndice

Propuesta de entrevistas

Parte I

Informar al especialista participante la finalidad de la investigación, que tiene carácter confidencial y que la participación es voluntaria. Se le solicita el consentimiento para utilizar su opinión para este estudio. El participante puede negarse a contestar o terminar la entrevista en el momento en que lo desee. La entrevista no durará más de 30 minutos.

Parte II

Guía de preguntas para entrevista.

Guía de preguntas para entrevista a profesionales en el área de la nube.

1. Por favor, indique su profesión, dónde trabaja y su área de experiencia.
2. Por favor, indique de qué forma los ambientes en la nube son seguros.
3. ¿Cuáles servicios en la nube conoce y dónde los ha visto?
4. ¿Cuál o cuáles proveedores de IaaS ha utilizado? ¿Cuál piensa usted que es el proveedor en la nube con mejor SLA o soporte para la resolución de problemas y por qué?
5. ¿Qué practicas recomienda usted para una correcta implementación de la nube en una organización?
6. ¿Cuáles considera usted que son las razones por las cuales las empresas u organizaciones empiezan a adoptar la nube?

Guía de preguntas para entrevistas a funcionarios públicos de la CCSS.

1. Por favor, indique su profesión en la CCSS y su experiencia en su área.
2. Por favor, indique de qué manera el ciberataque impactó la productividad en su trabajo.
3. Por favor, indique de qué manera el ciberataque impactó de manera general en su trabajo.
4. ¿Qué medidas tomó la CCSS o su jerarquía más alta ante este ciberataque?
5. ¿Cuáles son algunas características de la nueva metodología o procedimientos que implementó la CCSS con sus servidores caídos?
6. Por favor, indique las diferencias en la forma en que trabaja antes y después del ciberataque.