Propuesta de un modelo de ciberseguridad para la pequeña empresa en Costa Rica

Proposal for a cybersecurity model for small businesses in Costa Rica

Angie Carolina Leiva Montero[1],

Luis Arturo Mantilla Quesada[2],

Julio Córdoba Retana[3],

Universidad Latinoamericana de Ciencia y Tecnología

2022

Resumen

Según el Ministerio de Economía, Industria y Comercio de Costa Rica (MEIC), las pequeñas y medianas empresas representan aproximadamente el 97% de la fuerza empresarial del país (Microsoft, 2022). Muchas de estas empresas se han visto en la tarea de adaptarse a la era tecnológica que se vive actualmente, y esto las ha expuesto a peligros de ciberseguridad, especialmente por falta de conocimientos, personal o recursos económicos que permitan abordar esta problemática. El alcance de esta investigación es realizar un análisis de la situación de ciberseguridad de las pequeñas empresas costarricenses en los años 2021 y 2022 con respecto a mecanismos de seguridad informática y ataques para, así, ofrecerles recomendaciones y herramientas como el NIST que puedan mejorar su situación actual con respecto a la ciberseguridad. Para lograr esto se efectuó un estudio cualitativo y de tipo exploratorio a través de entrevistas a pequeñas empresas de distintos sectores en Costa Rica. Los principales hallazgos encontrados indican que estas empresas utilizan mecanismos y herramientas de ciberseguridad de nivel muy básico y no se estima una concienciación empresarial para abordar o evitar las vulnerabilidades en seguridad que se puedan presentar. Se incita a las pequeñas empresas a implementar, en la medida de lo posible, las mejores herramientas y mecanismos ofrecidos para abordar la ciberseguridad y que se capacite de mejor

[1] Desarrolladora de software con especialización en desarrollo y diseño de aplicaciones web. Bachiller en Ingeniería Informática de la Universidad Latinoamericana de Ciencia y Tecnología.
https://orcid.org/0000-0002-3324-9270
Correo: aleivam127@ulacit.ed.cr

[2] Actualmente laborando en Ernst & Young desde noviembre del 2021 en Technical Support Risk Management. Especialización en desarrollo y diseño de aplicaciones web. Bachiller en Ingeniería Informática de la Universidad Latinoamericana de Ciencia y Tecnología. https://orcid.org/0000-0002-0920-0725
Correo: lmantillaq319@ulacit.ed.cr

[3] 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.
https://orcid.org/0000-0002-1700-2358
Correo: jcordobar022@ulacit.ed.cr

manera a todos los departamentos de la empresa para aplicar las prácticas de ciberseguridad que se recomiendan en la presente investigación.

Palabras clave: ciberseguridad, pymes, seguridad informática, pequeñas empresas, seguridad tecnológica

Abstract

According to the Ministry of Economy, Industry and Commerce of Costa Rica (MEIC), small and medium-sized companies represent approximately 97% of the country's business force (Microsoft, 2022). Many of these companies have been faced with the task of adapting to the current technological era, and this has exposed them to cybersecurity risks, especially due to a lack of knowledge, personnel, or financial resources to address this problem. The scope of this research is to carry out an analysis of the cybersecurity situation of Costa Rican small businesses in the years 2021 and 2022 with respect to computer security mechanisms and attacks to offer recommendations and tools such as NIST that can improve their current cybersecurity situation. To achieve this, a qualitative and exploratory study was carried out through interviews with small companies from different sectors in Costa Rica. The main findings found that these companies use very basic cybersecurity mechanisms and tools and there is no business awareness to address or avoid security vulnerabilities that may arise. Small businesses are encouraged to implement as much as possible the best tools and mechanisms offered to address cybersecurity and to offer a better education around all company departments to apply the cybersecurity practices recommended in this research.

Keywords: cybersecurity, SMEs, computer security, small businesses, technological security

Introducción

El auge de la tecnología ha ayudado a que más pequeñas empresas se unan a su uso para mejorar la gestión de sus procesos y el manejo de la información, y no verse tan rezagadas con respecto a las grandes empresas; a su vez contribuyen con su propio crecimiento. Sin embargo, el cambio digital también conlleva peligros que en muchas ocasiones las pequeñas empresas no toman en cuenta por falta de asesoramiento o capacidad económica. Uno de estos peligros es la seguridad tanto de los sistemas como de la información que estas albergan. Una mala gestión de la seguridad en sistemas informáticos puede generar pérdidas tecnológicas y de información por distintos ataques de ciberseguridad, y las pequeñas empresas son un blanco perfecto para esta clase de problemática (Beltrán, 2022).

En Costa Rica, según el Ministerio de Economía, Industria y Comercio (MEIC), el sector de las pequeñas y medianas empresas representa más del 97% de la fuerza empresarial del país (Microsoft, 2022). Un estudio realizado por Microsoft y comisionado a la firma Edelman en 2022 a 320 pequeñas y medianas empresas, demuestra que la pandemia del COVID-19 trajo consigo la aceleración del proceso de transformación digital en el 96% de estas empresas costarricenses, aumentando así sus riesgos de sufrir ataques a la seguridad de sus sistemas e información. El mismo estudio revela que el 75% de estas empresas ven la ciberseguridad como

un tema de prioridad, pero a pesar de haber hecho inversión en tecnología e implementar políticas de refuerzo de seguridad, un tercio de las pequeñas y medianas empresas aseguran haber sufrido de problemas con respecto a este tema (Microsoft, 2022).

El país es consciente de los problemas cibernéticos que acechan el mundo de la tecnología y es que, en el año 2017, el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) dio a conocer la Estrategia Nacional de Ciberseguridad, la cual tenía como objetivo diseñar un marco de acciones orientativas para establecer un uso seguro de las tecnologías de la información (Banco Interamericano de Desarrollo y Organización de los Estados Americanos [OEA], 2020). Cabe destacar que, a pesar de todos estos esfuerzos, Costa Rica se ubica en el puesto 48 según el índice Nacional de Seguridad Cibernética (NCSI), superado por países como Chile y Paraguay, y en los últimos años ha presentado severos ataques a los sistemas informáticos de muchas instituciones en el país (Rámirez y Gónzales, 2020).

Costa Rica está consistentemente en proceso de innovación, por lo que también se debe tomar en consideración en el sector de innovación tecnológica, sin embargo, no se debe ignorar los ataques cibernéticos a los que ha sido expuesto el país en los últimos años, en especial cuando el mayor objetivo de las organizaciones criminales a la hora de realizar ataques en nuestro país ha sido el robo de información y daño de sistemas. Esto nos ha dejado en sí como país, tanto en el sector público como privado y las pequeñas, grandes, y medianas empresas, un sinsabor con respecto a los temas de ciberseguridad y cómo las vulnerabilidades que se producen relativos a estos pueden llegar a causar impactos de mayor nivel para la empresa costarricense, y aún más si no se cuenta con los mecanismos adecuados de combate y protección ante estos.

Tomando esto en cuenta, es importante analizar que, si bien existen recursos para mejorar en cuanto al tema de ciberseguridad como país, la inversión en nuevas tecnologías y creación de leyes y entes encargados de regular estas situaciones, no han prevenido ni siquiera a los sistemas públicos costarricenses de sufrir ataques de ciberseguridad. Y si esto se presenta en sistemas que reciben mejor inversión en el ámbito tecnológico y protección por parte del Estado, no cabe duda de que las pequeñas empresas del país están aún más expuestas a caer en las probabilidades de verse afectadas de manera significativa en caso de sufrir ataques cibernéticos para el daño de sistemas o robo de información.

Pregunta de investigación

¿Cómo utilizar las mejores prácticas de ciberseguridad utilizando la estructura National Institute of Standards and Technology (NIST) para aumentar la seguridad tecnológica en la pequeña empresa costarricense?

Objetivo General

Proponer un modelo de ciberseguridad que pueda ser aplicado a las pequeñas empresas en el área metropolitana de Costa Rica.

Objetivos Específicos

1. Modelar un diagnóstico que permita identificar el tipo de seguridad que utilizan las pequeñas empresas en Costa Rica.
2. Evaluar el tipo de ataques cibernéticos recibidos en pequeñas empresas en Costa Rica en 2021 y 2022.
3. Diseñar estrategias para fomentar la educación en las pequeñas empresas sobre la importancia de tener una buena seguridad tecnológica.
4. Elaborar un manual informativo en donde se explique a las pequeñas empresas cómo se realizan los ataques cibernéticos más comunes y cómo evitarlos.
5. Crear una estrategia que permita compartir por medio de diferentes canales los manuales informativos propuestos.

Formas de alcanzar los objetivos:

Para cumplir el alcance de los objetivos propuestos se utilizó varias plataformas de investigación como son Google Scholar, EBSCO host. Además, por estos medios de plataformas web se investigó los ataques cibernéticos más comunes en Costa Rica.

El tipo de investigación es cualitativa por lo que se entrevistó a 15 empresas pequeñas de las cuales se obtuvieron los contactos por parte de la Universidad Latinoamericana de Ciencia y Tecnología.

Las entrevistas se realizaron por medio de videoconferencia Zoom, así mismo, se hizo una serie de preguntas con el fin de conocer más sobre la seguridad tecnológica de las empresas y su forma de manejar este tema.

Revisión Bibliográfica

El aumento del uso de la tecnología en las empresas no solo trae consigo beneficios, sino que también ha dado paso a la explotación de puntos débiles y uno de estos es la ciberseguridad. El crecimiento en la digitalización no ha venido de la mano con los progresos en la ciberseguridad, lo cual resulta preocupante cuando en la actualidad los datos se consideran más valiosos que el petróleo y estos se ven cada vez más expuestos a riesgos. Un ejemplo de este predicamento de seguridad se ve reflejado en el ciberataque de carácter global que se dio en mayo de 2017, cuando más de 230.000 computadoras alrededor del mundo se vieron afectadas. Un mes más tarde, se produjo otra variante del ciberataque con un impacto más dañino. Desde este acontecimiento, los ataques contra distintas empresas alrededor del mundo han sucedido constantemente y no solo por parte de agentes externos, sino que también internos (Mendivil, Sanz y Gutiérrez, 2022). Y es que la mayoría de los ciberataques (casi un 86% de estos) están motivados por la obtención de ganancias económicas y los atacantes no discriminan entre las empresas víctimas de estos daños (Ulloa-Mora, 2021).

En la actualidad, los ataques cibernéticos han evolucionado y se han convertido en amenazas más sofisticadas y complejas que afectan no sólo a estructuras débiles, sino que también a estructuras críticas, y se llevan a cabo tanto por grupos organizados como por individuos; esto

en muchas ocasiones por el camuflaje anónimo que ofrecen los espacios digitales (Méndez, 2021). En América Latina, la gestión de los problemas de ciberseguridad tanto en empresas públicas como privadas se ha convertido en un reto complicado por dos factores: el aumento en los ataques y la evolución en las técnicas empleadas para estos, así como la baja credibilidad e importancia que se le da a estos por parte de gerentes, accionistas, entre otros, cuando se debe disponer de recursos para brindar protección informática (Rodríguez, 2019). A su vez, en la región de América Latina las pequeñas y medianas empresas son las más afectadas por esta problemática de ciberseguridad, pues no tienen personal capacitado o un departamento de ciberseguridad para luchar contra posibles ataques lo que conlleva a que estas se vean expuestas a ataques informáticos (Cando-Segovia y Medina-Chicaiza, 2021).

Las áreas de oportunidad y retos para la ciberseguridad en América Latina según el National Cyber Security Índex (NCSI) indica que:

> Tienen un total de doce indicadores, *los cuales son,* 1) desarrollo de política de seguridad cibernética, 2) delimitación de amenazas en el ciberespacio, 3) educación y formación de especialistas capacitados en ciberseguridad y concientización de la población, 4) aportación de cada país para mejorar el contexto global de ciberseguridad, 5) nivel de desarrollo digital del país, 6) protección de servicios esenciales por el Estado de Infraestructura Nacional Crítica, 7) servicios digitales y confidencialidad en la vida diaria, 8) Protección de datos y garantía de privacidad, 9) respuesta a ciber incidentes por parte de equipos de emergencia informática (CSIRT o CERT) ante ciber incidentes, 10) capacidad para administrar una crisis cibernética del Estado-Nación, 11) grado de compromiso del Estado para luchar contra el cibercrimen, y 12) capacidad de operaciones militares de las fuerzas armadas en el ciberespacio (Aguilar, 2021).

Según el NCSI *Costa Rica está calificado en el lugar 60 en el 2019 en cuanto la ciberseguridad; los indicadores generales de la ciberseguridad se califican de la siguiente forma:* Desarrollo de políticas de seguridad cibernética en un 86%, en Educación y Desarrollo profesional en un 67% y en la Respuesta a incidentes cibernéticos en un 83%.” (NCSI, 2019)

Debido a la pandemia el estado de cibercrimen ha aumentado en Costa Rica por lo que según Roberto Lemaitre comenta acerca de los ataques cibernéticos que han aumentado, estos se enfocan en ataques a aplicaciones móviles en un 9%, ataques a aplicaciones web en un 18%, denegación de servicios 7%, fuga de información en un 9%, la ingeniería social o también conocida como phishing, *esos forman parte de las estafas como son las telefónicas para engañar a las víctimas a brindar información confidencial, estos conforman un* 29%, virus troyanos forman parte de un 26% y otros un 2% (Lemaitre, 2021, 12:43). Las empresas deben tener mucha precaución a la hora de proteger su información ya que un ataque DDos o también conocido como denegación de servicios es un ataque cibernético en al área de redes, el cual detiene toda máquina o recursos de redes (periféricos de computadoras). Un comportamiento de estos ataques se demuestra el siguiente hecho:

> Un ataque distribuido de denegación de servicio (DDoS) dio como resultado la pérdida de calefacción en dos edificios de la ciudad de Lappeenranta en el este de Finlandia,

> según reportaron los medios locales, el último de los ejemplos de los efectos derivados de los ataques cibernéticos en infraestructura interconectada. [...] Según una declaración publicada por la firma local Valtia especializada en gestión de TI, y un reporte de la Autoridad Reguladora de las Comunicaciones Finlandesas, el ataque fue detectado después de que un sistema de automatización de edificios usado en dos propiedades comenzó a emitir alarmas extrañas y no podía ser accedido remotamente. La causa fue un sostenido ataque de denegación de servicio que estaba inundando el sistema con falso tráfico de internet, lo cual causaba su reinicio a los pocos minutos y les denegaba a los administradores remotos de Valtia el acceso al dispositivo. El ataque se prolongó desde el 3 al 4 de noviembre (Tully, 2020).

Existen diferentes pronósticos que se presentaron en el 2021 con la temática de ciberseguridad y seguridad, —ataques de malware, ingeniería social, inyecciones de bases de datos— cuya función es secuestrar los datos de las empresas, esto ha causado pérdidas en las empresas en cuanto información, económica y clientes, por ello:

> Estos ataques se han convertido en uno de los activos más importantes de las organizaciones, *ya que grandes cantidades de información equivale a una gran cantidad de dinero para las empresas ya que si pierden o es robada se ve perjudicada la empresa con su imagen y su capital* [...] Reconocer dónde se ubican aquellos que resultan más valiosos y saber cómo se están protegiendo, debería ser una prioridad para las organizaciones del siglo XXI. Sin embargo, muchas veces la información de mayor relevancia termina en los lugares menos indicados o más inesperados, como quiera que su uso resulta de manejo diario o muchas veces compartido entre diferentes personas (Cano, 2020).

La aceleración digital es otro pronóstico que se pudo presentar al inicio de la pandemia COVID-19, ya que las empresas e instituciones tuvieron que tomar medidas y cambiar las modalidades de trabajo, así mismo:

> Se pasó de forma urgente de un modelo centralizado de operaciones y aseguramiento, a uno ampliamente basado en terceros (desconectados del marco de seguridad empresarial), con una cultura organizacional de seguridad de la información basada en personas informadas (algunos más conscientes que otras) y con un marco de trabajo en casa que responde a la práctica individual de higiene informática vigente en el hogar (Cano, 2020).

En Costa Rica existe muchos tamaños de empresas grandes o transnacionales, medianas y pequeñas (PYMES). “De acuerdo con el último informe del Ministerio de Economía, Industria y Comercio (MEIC) para el 2017 las Pymes representan el 97.5 % de las empresas del país y este número va en aumento año tras año lo que significa que cada vez más familias tienen ingresos para sus hogares” (Valverde, 2022). Sin embargo, muchas empresas cuentan con diversas dificultades ya que:

> Al ser un ambiente empresarial globalizado a nivel mundial y competitivo como el que existe en la actualidad, las pequeñas y medianas empresas, sociedades y las compañías dependen cada vez más de la tecnología específicamente de un sistema de información y deben crear políticas de seguridad como un medio de protección, pues se ha demostrado que tienen una enorme influencia para aumentar su nivel de competitividad. Sin embargo, sin una adecuada gestión de la seguridad algunos de ellos carecen de valor real, ya que no pueden aportar las suficientes garantías de continuidad a las empresas. [...] Así mismo, las pequeñas y medianas empresas, sociedades y compañías empiezan a tener conciencia de la enorme importancia que tiene el poseer unos sistemas de seguridad de la información adecuados, así como una correcta gestión de estos. (René, Arce, Romero y Soledispa, 2019)

En Costa Rica desde el 18 de abril de 2022, varios sistemas operados por las instituciones gubernamentales fueron atacados con ransomware (Sulima y Mora, 2022). Costa Rica está sufriendo de ataques ciberterrorista y por eso el presidente de Costa Rica Rodrigo Chaves ha decretado estado de emergencia, dijo el presidente en referencia a la declaratoria decretada al asumir la presidencia, el 8 de mayo (Reuters, 2022). En consecuencia, muchas instituciones se vieron afectadas; el mandatario afirmó que su gobierno recibe apoyo de Israel, Estados Unidos y España para proteger los sistemas y reparar los daños, cuya magnitud no se ha medido aún, dijo el ministro de Ciencia y Tecnología, Carlos Enrique Alvarado.

Las pequeñas empresas tienen varias limitantes que conllevan a esta gran afectación en su nivel de seguridad, entre estas se encuentran: acceso limitado a herramientas de protección, falta de conocimiento por parte de los colaboradores con respecto a las tecnologías de la información y por último, un manejo inadecuado de la tecnología por parte de aquellos colaboradores que sí se manejan con estas herramientas (Pruna, Jeada y Jumbo, 2020). Existe la tendencia a creer que una de las soluciones para mitigar los problemas de ciberseguridad, especialmente en pequeñas empresas, es crear una concientización en estos temas, sin embargo, a pesar de que es un punto de partida inicial, solo la concientización no ha dado buenos resultados, es necesario crear arquitecturas de seguridad cibernética y de sistemas para salvaguardar la ciberseguridad de estas empresas (Carnero, Armas, Carbajal y Madrid, 2020).

Existen diversos tipos de acciones y herramientas que se deben tomar para evitar los ataques cibernéticos más comunes contra pequeñas empresas o PYMES:

> Anti-Malware, el malware es un tipo de amenaza en ciberseguridad que se instala de forma maliciosa en los equipos para dañarlos o interrumpir sus operaciones. Las herramientas antimalware adecuadas se ocupan de analizar los dispositivos y memorias internas y externas para detectar y neutralizar el malware. El siguiente es el Antispyware es otro tipo de problema de seguridad informática cuyo objetivo es recolectar información para emplearla con fines fraudulentos.
>
> Los protocolos antispyware detectan y eliminan los potenciales problemas de spyware. Correo y navegación seguros, el uso del correo y los navegadores suponen vulnerabilidades en seguridad informática, pues actúan como canales para la llegada de

> amenazas que pueden poner en riesgo el control de los equipos y los datos almacenados. Por ello, resulta esencial contar con herramientas de seguridad informática que sean capaces de atajar estos problemas, como los filtros antispam y antiphishing (correos fraudulentos que imitan a los de otras entidades para capturar datos sensibles, como contraseñas).
>
> La Monitorización proactiva ante amenazas, si bien muchos protocolos de seguridad informática se basan en reaccionar una vez que ocurre un problema, el enfoque proactivo permite poner remedio a vulnerabilidades antes de que tenga lugar un ataque. Auditoría y puesta en marcha de equipo se trata de un proceso clave si la empresa ya estaba en funcionamiento, ya que se enfoca en solucionar los problemas que, potencialmente, ya están ocurriendo en la actualidad, antes de avanzar hacia protocolos de ciberseguridad adicionales. Las copias de seguridad son procesos clave para que las empresas puedan preservar su información en caso de que los datos o equipos originales queden dañados. (Santaolalla, 2022)

Las PYMES sufren de ataques cibernéticos al igual que cualquier otra empresa, "Según José Rosell, socio-director de S2 grupo, el 74% de las pymes ha sufrido alguna vez problemas relacionados con su seguridad" (Marques, 2021). Esto causa una "disminución de la capacidad de la compañía, exposición a la competencia, riesgo reputacional, posible extorsión por parte de terceros" (Revista Summa, 2022).

Las empresas medianas y grandes tienen diversas medidas de seguridad por su volumen de trabajadores que constantemente utilizan códigos de programación para proteger los datos y buscar soluciones si han sufrido de ataques cibernéticos. El tema de la importancia de la protección de ataques cibernéticos ha sido de mucha consciencia para estos tamaños de empresas *"*[...] mientras que las pymes necesitan de más tiempo, en gran parte porque pensaron, en un primer momento, que carecían de atractivo para los hackers maliciosos. Hoy día sabemos que en torno al 50 % de los ataques se producen a pymes.*"* (Rosa y Galán, 2019).

Dentro del área de ciberseguridad es imposible establecer una seguridad informática absoluta *ya que existen diversas maneras de realizar ataques cibernéticos, sea porque dentro de la institución o empresa descarguen un virus o porque las metodologías de seguridad no sean óptimas, sea por no realizar respaldos semanales, no actualizar contraseñas constantemente, entre otros.*[...] Medrano comentó que, a nivel internacional, los especialistas recomiendan que las personas deben mantener la posición defensiva, recalca Medrano tener un pensamiento alerta: "no es si me van a atacar, es cuándo me van a atacar" para poder prevenir una acción de este tipo, porque asegura que en la seguridad informática no se puede garantizar un cien por ciento de eficacia" (UCR, 2022).

Las PYMES deben tomar en consideración que el departamento de IT y de sistemas debe evolucionar más que la simple reparación de hardware. Las limitaciones presupuestarias de las pymes son su punto débil" y así mismo su perdición al perder información esencial como cuentas bancarias, bases de datos. (IBIS, 2021).

A lo largo de los últimos años se han presentado distintas alternativas para mejorar el panorama de la ciberseguridad en las pequeñas empresas, como ejemplo de esto por medio de un estudio de casos de cibercrimen, Trujillo propone cinco puntos vitales a tomar en cuenta para ganar la batalla contra las amenazas de ciberseguridad: realizar actualizaciones a tiempo para proteger información sensible, identificar aquellos programas que ya no se utilizan y que pueden significar un riesgo para la empresa, practicar el uso de contraseñas robustas, concientizar sobre los peligros de la ingeniería social (la cual consiste en obtener información por medio de factores sociales), y por último, considerar los factores de doble autenticación en caso de tener cuentas con información importante o datos personales (Trujillo, 2019).

Cabe destacar que, si bien hacer concientización sobre estos aspectos mencionados anteriormente es importante, también se deben tomar en cuenta otras soluciones que van más allá de solo recomendaciones de este tipo. Como por ejemplo, Cedeño propone un marco de referencia para la implementación de controles de seguridad informática en una empresa de fabricación de muebles guiado por la norma CIS versión 8. Esta norma es propuesta por el Center for Internet Security y junta prácticas de ciberseguridad y recomendaciones de defensa en caso de ataques informáticos, se divide en tres grupos de implementación que dependen de la experiencia en una organización con respecto a ciberseguridad y lo que propone CIS es que las empresas deben autoevaluarse y hacer uso de los puntos de control de seguridad acorde al grupo perteneciente (Cedeño, 2022). Otro ejemplo de este calibre es la implementación que se realizó en la empresa Udersol de la normativa internacional ISO 27001, la cual se basa en la gestión de seguridad de forma continua apoyada en la identificación de riesgos también de forma continua, gracias a esto se permitió identificar riesgos y establecer controles de manejo para estos y aumentar la confidencialidad de la información y los sistemas (Solano, 2020).

Ahora bien, tomando en cuenta cómo la aplicación de distintos marcos de referencia puede colaborar en la creación de protocolos de seguridad más robustos para las pequeñas empresas, se debe hacer énfasis en uno de los marcos de referencia de seguridad más importantes globalmente como es el NIST Cybersecurity Framework, pues es utilizado como guía en la presente investigación. Este marco de referencia propuesto por el National Institute of Standards and Technology (NIST) se encarga de proveer un lenguaje común que permite comprender, gestionar y expresar los riesgos de ciberseguridad para las personas interesadas. Permite la identificación y priorización de tareas para la reducción en el riesgo por ataques a la ciberseguridad de una empresa, uno de sus aspectos más llamativos es que se puede implementar para manejar los riesgos de ciberseguridad en distintas áreas de una empresa y distintos tipos de entidades pueden utilizar este marco de referencia pues se ajusta a cualquier tipo de organización (Frayssinet et al, 2021).

Las soluciones de ciberseguridad implementadas se pueden utilizar con el enfoque NIST Framework el cual se divide en 5 etapas, estas son:

> 1) Protección que es la aplicación de controles (técnicos, políticas, procesos) para mitigar riesgos, contempla proteger los activos de la organización tomando como criterio la información obtenida durante la identificación de amenazas y riesgos, 2) Detección, es el control y monitoreo, contempla actividades para identificar la

> ocurrencia oportuna de un evento de ciberseguridad, 3) Identificar, el cual busca comprender el contexto, conocer los activos e identificar las amenazas existentes y la probabilidad de que se materialicen; desarrolla la comprensión organizacional para administrar el riesgo de ciberseguridad para sistemas, activos, datos y capacidades, 4) Recuperar, esta etapa es la que desarrolla e implementa actividades para mantener los planes de resiliencia y restaura las capacidades/servicios afectados en un incidente; una vez resuelta la crisis, se ejecutan tareas para recuperar el sistema afectado y devolverlo a su estado original, 5) Responder, este incluye actividades necesarias para tomar medidas con respecto a un incidente de ciberseguridad detectado, desarrollando la capacidad de contener el impacto de un potencial incidente (Apuy, 2022).

Un estudio realizado por Cordero-Robles en el 2021 se dio a la tarea de hacer uso del NIST Cybersecurity Framework para proponer un conjunto de herramientas de evaluación de riesgos de ciberseguridad para mejorar y estandarizar de mejor manera las evaluaciones tecnológicas en el área de TI (Tecnologías de Información) que da apoyo a auditorías financieras, esto mediante el análisis de documentación del área de TI y los componentes propuestos por el NIST Cybersecurity Framework. Gracias a este estudio, se pudo determinar los procedimientos a evaluar dentro de la empresa para detectar los riesgos a la ciberseguridad y se proporcionaron las herramientas necesarias para identificar estos riesgos de forma clara (Cordero-Robles, 2021). Aunado a esto y con un enfoque más direccionado a las pequeñas empresas, Cabezas ha tomado como referencia el NIST Cybersecurity Framework en conjunto con otros marcos de referencia, para la creación de un marco de trabajo que permite aplicar conceptos de ciberseguridad en pequeñas y medianas empresas. La inclusión del NIST Cybersecurity Framework en este caso se lleva a cabo como guía para implementar actividades de ciberseguridad, así como dar base a las políticas de ciberseguridad propuestas en el proyecto (Cabezas, 2020). De esta forma, dicha propuesta busca aplicar este framework a las PYMES de Costa Rica con el fin de identificar los ataques más comunes de estas empresas.

Metodología

Para crear una investigación con fundamento y precisión se debe considerar su enfoque, ya que existen diversos tipos de perspectivas que se pueden utilizar para recolectar información de una población. Para esta investigación el estilo de enfoque es cualitativo. Ya que dicho enfoque "*es* la obtención y recolección de los datos, no está orientada a medir variables y efectos: al reducir palabras y actos de la gente a ecuaciones matemáticas y estadísticas se pierde el aspecto humano de la vida social". Dicho enfoque no busca específicamente una población grande y con mucho análisis estadístico, sino es una investigación más social, ya que lo que destaca es la conversación con la población por lo que se puede profundizar el tema y las respuestas que se buscan para realizar la investigación (Donadei, 2019).

La metodología cualitativa incluye un número diverso de técnicas y procedimientos para recolectar la información pertinente. En estos enfoques se utilizan varios métodos que engloban distintas técnicas para recolectar la información necesaria para dirigir una investigación. Estas técnicas han probado ser de conveniencia para conocer, aprender e instruirse sobre las personas, la vida de estas, su comportamiento, las relaciones sociales, sistemas de reproducción, entre

otros aspectos pertinentes a los individuos. En la presente investigación estos aspectos son de suma importancia pues se indaga más a fondo en los entornos laborales de los participantes en función de comprender y aprender más sobre estos (Piza et al., 2019).

El estudio de esta investigación consiste en un alcance exploratorio, esto se lleva a cabo cuando se desea explorar un tema o problemática que ha sido estudiado vagamente y sobre el cual existen muchas incertidumbres o que en su totalidad no se ha tratado de abordar en estudios anteriores. Esta situación sugiere que, en los registros de literatura relacionados con el tema o problemática de estudio, se resaltan solamente ideas vagas y poco concisas, o bien que se desea indagar sobre estos desde una nueva perspectiva que no ha sido explorada (Landázuri, 2019). Así, extrapolando a las PYMES que son empresas pequeñas o microempresas con poco conocimiento, el objetivo es examinar y brindarles suficiente información de ciberseguridad, especialmente porque es un tema que esta población no aplica o desconoce en la mayoría de las ocasiones.

A pesar de que existe el prejuicio sobre cómo las investigaciones con enfoque cualitativo no son científicas por ser estudios que prescinden de la cuantificación, es importante destacar que no todos los fenómenos son mesurados. El enfoque cualitativo se presenta como una alternativa diferente a la generación de conocimientos científicos, en donde se busca lograr mayor profundización para obtener información valiosa que permita comprender la dinámica para explicar los hechos que se presentan en la información recopilada. Además de esto, al aplicar las técnicas y métodos que se disponen en el enfoque cualitativo, se puede lograr una interpretación amplia de los datos recopilados (Sánchez, 2019).

Debido a que el presente estudio consiste en una investigación con enfoque cualitativo el tamaño de la población es menor en comparación con los otros enfoques, por lo que se tomó en cuenta a quince empresas PYMES pertenecientes al Gran Área Metropolitana de Costa Rica. De estas fueron entrevistadas las personas con el conocimiento necesario sobre la situación de ciberseguridad en la que se encuentran las empresas en la actualidad. Estas entrevistas se llevaron a cabo por medio de la herramienta Zoom, Microsoft Teams y llamada telefónica, esto debido a que gracias a estas plataformas se pueden realizar grabaciones con el fin de tener referencia de cada PYME entrevistada y recolectar la información con mejor precisión, siempre pasando por el proceso de consultar el consentimiento del entrevistado para proceder con la grabación de las respectivas entrevistas. En el Anexo A se presenta con mayor detalle el proceso de entrevista y las preguntas realizadas.

Análisis de Resultados

El análisis de resultados constituye la parte conclusiva de una investigación, en esta etapa comúnmente se procesa toda la información que se recolectó del estudio y se presenta de una manera ordenada y comprensible de manera que sirva para apoyar los resultados, así como el cierre de los objetivos (criterios de salida) y también provee la base de conclusión y recomendaciones.

Para llevar a cabo una exitosa investigación cualitativa se escogió una población mucho más limitada y con el personal calificado para la investigación, en especial empresas pequeñas del

Gran Área Metropolitana cuyo conocimiento de tecnología no sea del mismo calibre que el de una empresa mediana o grande por lo que se realizaron mediante sesiones a la escogencia del encuestado, estas se realizaron por medio de las aplicaciones de Zoom y Teams y por llamada telefónica utilizando el medio de Whatsapp.

Además, para el cumplimiento de la investigación se solicitó apoyo de quince empresarios de los cuales todos los entrevistados respondieron todas las preguntas que se le solicitaron ya que, previo a las entrevistas, se les indicó que al ser un tema de seguridad tecnológica podían escoger cuáles preguntas querían responder y cuáles no.

Dichas entrevistas tuvieron una duración entre 5 a 15 minutos. Las entrevistas contaban con 12 preguntas abiertas lo que permitió obtener una gran cantidad de información acerca de diferentes perspectivas de los términos de seguridad, las buenas prácticas de tener una seguridad y sus experiencias de ataques cibernéticos y así mismo cómo se contrarrestaron. Al ser preguntas abiertas y tener un aproximado de 1 minuto y medio para la respuesta sí implicó el estar dirigiendo las respuestas con ejemplos y definiciones operacionales. Esto dio como resultado la creación de un manual más amplio acerca de las buenas prácticas de seguridad para las pequeñas empresas y requirió complementar e ilustrar, con varios ejemplos brindados por los encuestados, los métodos utilizados para contrarrestar los ataques cibernéticos.

Primeramente, se debe mencionar que los entrevistados pueden tener conocimiento de ciberseguridad pero si ellos no aplican ese conocimiento, de nada servirá el poder aspirar a tener una mejor seguridad tecnológica, por esto mismo, se les consultó exactamente qué conocían del término de ciberseguridad, a lo cual el 98% de los entrevistados mencionan correctamente la definición, demostrando que debido al incremento de las necesidades de virtualización ocurrida durante el siglo XXI, han tenido que informarse y actualizarse en lo que respecta el tema de la seguridad tecnológica.

Con el transcurso de las entrevistas se identificó un empresario que no conocía mucho acerca de la ciberseguridad por lo que se le tenía que definir y explicar ciertos conceptos ya que previo a la entrevista mencionó que su empresa tiene solamente 2 años de consolidada, por lo que por el momento comentó que no tenía las herramientas suficientes para poder tener una buena ciberseguridad en su empresa, sin embargo, sí aplicaba las buenas prácticas básicas de una buena seguridad pero los adaptaba de una manera empírica.

En la figura 1 se muestra lo que es el “Framework Core”, el cual se conoce como la Estructura principal de NIST, cuyo marco de referencia proporciona actividades para lograr resultados específicos de ciberseguridad, y referencias que sirven como ejemplos de orientación para lograr esos resultados (National Institute of Standards and Technology, 2018). Esto permite brindarles con esta metodología una resolución de problemas más efectiva y rápida a la hora de presentar ataques cibernéticos a las PYMES.

Figura 1. *Framework Core NIST*

Nota: La figura representa las 5 etapas en las que se divide el Framework NIST. Fuente: Tomado de *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, 2018, p. 6 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf). (Traducción libre del autor).

Además, para la realización más efectiva de la estructura NIST se le preguntó a cada persona acerca de los ataques cibernéticos que han enfrentado las empresas ya que la funcionalidad de NIST consiste en dividirse en 5 etapas —Identificar, Proteger, Detectar, Responder y Recuperar—. Estas ayudan a una organización a expresar su gestión del riesgo de ciberseguridad, habilitando el riesgo decisiones de gestión, abordar la amenaza[...] Estas 5 etapas también se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en ciberseguridad (National Institute of Standards and Technology, 2018). La mayoría de los ataques comentados por los entrevistados son realizados por parte de ataques de ingeniería social como estafas por teléfono y estafas por correo. Solamente uno de los entrevistados indicó un ataque mayor a servidores.

En cuanto a temas relacionados con contraseñas, la respuesta de los entrevistados fue mixta pues algunos indicaron que sí tenían ciertos períodos para llevar a cabo cambio de contraseña (cada mes, tres meses o seis meses) y otros especificaron que no tenían un período establecido para realizar estos cambios. Otro aspecto importante es que indicaron que las contraseñas que se establecen tienen características como dígitos alfanuméricos, letras en mayúscula y minúscula, y caracteres especiales; otros solo indicaron que las contraseñas se dejaban a criterio de los colaboradores.

Por último, a la hora de preguntar sobre la seguridad de red se notó que pocos utilizan protección como VPN (Virtual Private Network) a la hora de navegar por internet, la mayoría conecta a la red normal ofrecida por el proveedor de servicios mientras que otros entrevistados indicaron que se utilizaba algún mecanismo de bloqueo de anuncios o demás para evitar problemas relacionados con estos en caso de tener la necesidad de navegar a través de la web.

Discusión de los resultados

Para enfatizar la necesidad de por qué se está haciendo este esfuerzo en pequeña industria cabe destacar el impacto que tiene este sector dentro de la economía nacional; actualmente la contribución al Producto Interno Bruto (PIB) es del 36,05% (MEIC, 2021). El total de empleados en PYMES corresponde al 6,9% de la población económicamente activa de Costa Rica (INEC, 2019).

Debido a los altos ataques cibernéticos que han recibido en Costa Rica, muchas empresas han tenido que fortalecer e informarse más acerca de la ciberseguridad; las empresas pequeñas al tener un personal muy limitado en el área de tecnología permiten que los ciberdelincuentes realicen ataques a estas empresas con mayor facilidad. Con base en lo anterior, se consideró esencial preguntarle a la población de PYMES del Gran Área Metropolitana si en los años 2020 a 2022 se ha invertido en herramientas de seguridad, por lo que una gran parte de los encuestados mencionaron que no han invertido en herramientas de seguridad ya que existe el *Windows Defender* que está preinstalado en las computadoras. Otros comentaron que ya venían implementando medidas de seguridad previo a ese rango que se les indicó.

Al empezar el cuestionario una de las primeras preguntas exploratorias era si la compañía poseía o no herramientas de seguridad con el fin de entender si tenían una posible estructura de Soporte Técnico. Así, los empresarios, al indicar que sí contaban con herramientas de seguridad, daban a entender que posiblemente contaban con un personal de Soporte Técnico, el cual podría dar mantenimiento a estas herramientas de seguridad, sin embargo el 70 % de los entrevistados comentó que no tenían soporte técnico. Al ser una entrevista exploratoria con preguntas abiertas, al preguntar más en detalle indicaron que ellos mismos le daban el mantenimiento a los sistemas. Un 6% de los entrevistados comentó que para poder dar soporte técnico a sus empresas buscaban estudiantes del área de informática que necesitaban realizar el trabajo comunal por lo que así obtenían un soporte informal y a corto plazo lo que destruye el propósito de tener un plan de seguridad informática, porque probablemente se ejecutará una sola vez mientras el estudiante esté en el periodo. Al continuar con la entrevista el 30% restante respondió contar con personal de sistemas, lo cual ayuda grandemente a dichas compañías al tener un departamento o personal el cual debe de planear las necesidades de seguridad cibernética, teniendo como referente un país y diversas situaciones globales relacionadas con las amenazas actuales de ciberseguridad, para así poder plantear o visualizar un plan de ciberseguridad tecnológica actualizada y acorde con las necesidades actuales. Una de las principales sugerencias que se puede hacer en las organizaciones que dan soporte en las pequeñas industrias es el establecer entrenamientos periódicos y convenios con universidades para obtener grupos de soporte para la ayuda a este sector. El Ministerio de Economía, Industria y Comercio (MEIC) “para el 2017 indicó que las Pymes representan el 97.5 % de las empresas del país y este número va en aumento” (Valverde, 2022).

Uno de los más grandes retos que interpela este sector es la visión a corto plazo y la percepción de los grupos que se categorizan como de soporte, la pequeña industria considera todas las personas que trabajan en manufactura de un bien o de proveer un servicio como unidades principales y tienden a ver los grupos de soporte como un gasto; los grupos de tecnología de servicios caen dentro de esta última definición. De lo anterior se explica el por qué muchas empresas entrevistadas cuando se les consultó cuánto personal poseían relacionado con

tecnología adujeron tener el personal de seguridad y el de tecnología, pero de manera unificada, debido a que en promedio la cantidad de personas que laboran en estos tipos de empresas no llegan a ser mayor a 8 personas (MEIC, 2021).

La seguridad cibernética es esencial para poder contrarrestar a los cibercriminales ya que solamente en el 2019 se registraron 14.136 denuncias por delitos fraudulentos en Costa Rica, y durante el año 2019 el OIJ recibió en promedio una denuncia de fraudes cada 37 minutos, lo cual es un claro ejemplo de ingeniería social (ataques cibernéticos por medio de teléfono celulares) (Grosser.S, 2020). Otro ejemplo de cibercrimen y uno de los más graves se presentó en mayo de 2022 en Costa Rica, cuando fueron atacadas cibernéticamente diferentes instituciones públicas por diversas causas, entre ellas sus malas prácticas de seguridad, lo cual incluye la educación que se le proporciona a los empleados de la ciberseguridad. El no tener una buena defensa contra estos criminales puede ocasionar lo que ocurrió con la Asociación Nacional de Educadores (ANDE), la cual denunció irregularidades en el pago de salarios a personas funcionarias del MEP, justificadas por el ciberataque del ransomware Conti a las redes del Ministerio de Hacienda. Para el sindicato, si bien es cierto que el MEP no ha sido vulnerado por ataques cibernéticos, las afectaciones que ha tenido el Ministerio de Hacienda sí han incidido en los servicios que presta el Ministerio, en lo referente con el pago de la planilla. Cortés. S & Sáenz. R,2022). Las instituciones públicas, al manejar información crítica de la ciudadanía, debería invertir en ciberseguridad y no ser reactivos (despidos de personal y el tiempo que les tomó para reaccionar, inclusive incurriendo en las demandas de los ciberterroristas). Tómese en cuenta el siguiente escenario: ¿qué pasaría si, producto de un ataque de ciberseguridad, se afecta a las pequeñas empresas, las cuales contribuyen a más del 30% del Producto Interno Bruto? Por ello es importante proponer a las instituciones que apoyan a las PYMES programas y asesorías para proteger estas empresas de ataques cibernéticos.

Por esta razón, las compañías de este tamaño son más vulnerables ante estos ataques cibernéticos, ya que pueden ser estafadas de varias maneras, como, por ejemplo, un cibercriminal que se haga pasar por un cliente o que los mismos antivirus que utilizan pueden contener muchos anuncios que terminan ejerciendo el mismo rol de un adware o descargar un posible virus. Para ilustrar lo anterior se le dieron a los entrevistados cuatro opciones para que escogieran cuáles herramientas de seguridad tecnológica han aplicado en sus empresas. Se complementó la explicación de las cuatro opciones brindándoles ciertos ejemplos en cada herramienta para poder asegurarse el entendimiento de la pregunta. La primera herramienta que se les comentó era si tenían algún Antivirus instalado y en funcionamiento dentro de las computadoras de las empresas y se les brindó ejemplos de antivirus para guiarlos tales como Norton, AVG Antivirus y McAfee. Otra herramienta que se les consultó fue la relacionada con Antispyware, la siguiente herramienta fue el Antimalware y la última herramienta el Firewall que tienen diversas opciones como el Windows Firewall, Linux Firewall y Netdefender. En caso de que no tuvieran ningún método de seguridad se les pidió que especificaran el motivo de por qué no tenían ninguna herramienta. Dicha pregunta demostró que el 100% de estas empresas tienen como mínimo una herramienta de seguridad, entre ellas destaca más tener Antivirus gratuitos que de paga, ya que comentaban que la opción gratuita ya brindaba suficiente protección ante los ataques cibernéticos.

En el estudio del año 2019 realizado por Ministerio de Economía, Industria y Comercio (MEIC) en Costa Rica sobre el Impacto de la pandemia por Covid-19 en las PYME costarricenses se menciona que solamente un 27% de estas pudieron continuar sus operaciones utilizando ventas por Internet, a través de redes sociales, mercados virtuales y otros, para reducir o eliminar el contacto físico con sus clientes. Asimismo, el 25% de las PYMES habían cerrado negocios durante el 2019 (MEIC, mayo 2020), tomando en cuenta la población de PYMES en el 2019 esto corresponde a 34,000 empresas las cuales representaban casi ¼ de millón de personas. Esto indica claramente la falta de flexibilidad respecto a los cambios en el ecosistema de negocios y que el grupo es altamente sensible a los impactos tecnológicos y a las consecuencias generados por estos (ventas vía web y teletrabajo). Ambos ejemplos citados implican un nivel de madurez en el ámbito de la tecnología de información de mediano a alto y estos no los poseían las PYMES en el 2019. Las entrevistas dieron como resultado que por lo menos un 53% de las empresas pequeñas pudieron implementar al menos un día de trabajo remoto, tal vez se vea muy poco 4 días al mes, pero tómese en cuenta que una persona teletrabajando ahorra en promedio dos millones ciento treinta ocho mil colones al mes. Esto representa un buen punto de venta para invertir en opciones pagadas de herramientas de seguridad tecnológica.

Durante la pandemia se siguió un modelo de trabajo híbrido al ser imposible poder mandar a los trabajadores a modalidad de trabajo remoto, este modelo imperó en las PYMES durante el 2019 y se está implementando en el 2022 en las empresas medianas y grandes. Este es un punto a favor de las PYMES ya que tuvieron 3 años de trabajo híbrido antes de las empresas grandes. El trabajo híbrido se define como la mezcla de días trabajados desde la casa y en la empresa. Este fue uno de los puntos más innovadores y flexibles que tuvieron las PYMES durante el 2019. Cabe destacar que tomando en cuenta lo mencionado en las entrevistas, a pesar de que se implementaron tanto el trabajo virtual en su totalidad y trabajo híbrido, muchas de las empresas no cuentan con una estructura correcta para poder protegerse en caso de que existan problemas relacionados con ciberseguridad, especialmente a la hora de hablar sobre el uso de los equipos para la implementación de trabajo virtual; muchos de los entrevistados mencionaron el uso de equipos personales para implementar la modalidad de trabajo virtual.

Con la finalidad de hacer énfasis sobre estos problemas de ciberseguridad, se destaca que como se indicó en las entrevistas, la mayoría de los ataques que estas empresas reciben vienen por medio de prácticas de ingeniería social. Esto no resulta una sorpresa, pues según un estudio realizado por la empresa proveedora de servicios de seguridad ESET en el año 2021, los ataques de ingeniería social son la segunda amenaza más grande a la ciberseguridad de las empresas en la región de Latinoamérica con un porcentaje del 20% según el estudio (ESET, 2021). Cabe destacar que esta clase de ataques no solo implica estafas telefónicas para robo de información como muchas personas creen, sino que también por medio de correos se corre el peligro de enfrentarse a posibles ataques mayores como la descarga de archivos maliciosos que pueden llegar a destruir sistemas. Siguiendo en esta misma línea, ya que la infraestructura tecnológica de este tipo de empresas no es de gran tamaño (a excepción de unos casos dentro de la población entrevistada), ataques a servidores, suplantación web y demás son poco comunes; esto no

quiere decir que estas empresas estén exentas de estos casos, en especial tomando en cuenta que se da en su mayoría una protección básica a la seguridad de los sistemas.

Ahora bien, a pesar de que mayoritariamente se tiene la creencia de que la seguridad contra los ataques informáticos ha mejorado a comparación con el año 2020, aún sigue existiendo un compromiso menor comparado con los esfuerzos realizados por medianas y grandes empresas. Tal como se ha mencionado, los ataques y las técnicas para atacar van evolucionando con el pasar de los años, pero el esfuerzo y la importancia que se le da a estos sigue estando en un nivel bajo (Rodríguez, 2019), y esto se puede observar considerando que la mayoría de las empresas entrevistadas mencionan como protección sistemas básicos como antivirus y las herramientas básicas que se ofrecen con los equipos de computación. Sí existe un compromiso para mejorar, y aunque siempre es un esfuerzo que puede conllevar inversión económica, las pequeñas empresas necesitan una mejor guía para mejorar con respecto a aspectos de seguridad y autoevaluarse críticamente sobre los esfuerzos realizados para este fin.

También es importante mencionar que de alguna u otra forma, existe cierto esfuerzo por mantener la seguridad de alguna u otra forma, ya sea por medio de mecanismos como antivirus o firewalls como se ha mencionado anteriormente, o por medio de una medida tan simple pero importante como es el manejo de credenciales como contraseñas. A pesar de que es una medida básica, asegurarse de que las contraseñas se manejen de manera correcta puede proveer mucha seguridad a la hora de proteger los sistemas y la información dentro de estos. Como se indica en las entrevistas, algunas de las empresas implementan cambios de contraseña al menos dos veces por año y en casos más particulares de manera mensual. Además, también existe la práctica de crear contraseñas que cumplan con ciertas reglas para hacer que estas sean más complicadas para los atacantes a la hora de que intenten interferir. Las principales medidas mencionadas en las entrevistas fueron aquellas que se implementan en la mayoría de las empresas, y esto destaca pues muchos atacantes tienen como objetivo el robo de contraseñas a través de distintos ataques, además de que una de las recomendaciones más básicas en términos de ciberseguridad siempre ha sido el uso de contraseñas complejas para aumentar la protección. Cabe destacar que siempre se abre paso a la mejora por medio del uso de generadores de contraseñas u otros mecanismos que ayuden a reducir el error humano a la hora de su creación.

En cuanto al manejo de redes, este parece ser uno de los problemas que menos se busca atacar en las empresas entrevistadas. A pesar de que existen mecanismos para mejorar la seguridad a la hora de navegar por medio de internet, las empresas pequeñas en su mayoría no aplican ningún protocolo para navegar de manera segura. Si bien a veces se da el uso de VPN o herramientas implementadas para reducir la intervención de anuncios y una navegación más segura, son casos poco comunes en las empresas entrevistadas. En muchas ocasiones esto también se da pues como son empresas pequeñas, su nicho no ve relevante el uso de grandes infraestructuras tecnológicas para su funcionamiento, por lo que aspectos como la seguridad de red no son una prioridad o una preocupación que se considere a la hora de establecer los equipos tecnológicos. También se debe considerar que esta clase de seguridad puede implicar inversiones económicas que muchas pequeñas empresas no pueden costear debido a la falta de presupuesto.

Como punto final, y tomando como referencia las respuestas brindadas por los entrevistados, se da la impresión de que en las pequeñas empresas, inclusive si estas manejan cierta cantidad de equipos y sistemas de tecnología ya sean propios o de terceros, la ciberseguridad no es un factor al que se le toma mucha importancia dentro de las necesidades del negocio y lo que se busca es que las distintas operaciones sigan funcionando como deben más allá de si se presenta algún peligro en los sistemas informáticos. Un aspecto importante de esto es que las medidas también dependen de la cantidad de personas que operan en una empresa, hay que tomar en cuenta que la definición de pequeña empresa indica que puede ser cualquier empresa con una persona como mínimo o con un máximo que no debe exceder a más de cincuenta personas (Rimachi, 2019). Las necesidades con respecto al manejo de tecnología y el abordaje de la ciberseguridad pueden ser diferentes según sea la expansión de la empresa. También se debe tomar en cuenta el enfoque del negocio, no es comparable una pequeña empresa que brinda servicios de tecnología, con otra cuya área no esté concentrada en la tecnología y esta se utilice solamente en cuestiones operacionales.

Conclusiones y recomendaciones

A la hora de conocer las principales herramientas y mecanismos utilizados por algunas pequeñas empresas costarricenses, se deduce que estas utilizan los mecanismos más básicos que se ofrecen en cuanto a seguridad informática y además en algunas ocasiones se utilizan sistemas por parte de terceros por lo que no se está al tanto de la seguridad cibernética. Entre estos mecanismos y herramientas básicas, los más utilizados son los antivirus, firewall (la mayoría el integrado por defecto en los equipos de computación como Windows Firewall) y el respaldo de la información. Se recomienda con respecto a esto, primero que todo tomar en cuenta las mejores opciones atinentes a antivirus, firewall y respaldo de información como por ejemplo investigar sobre los dispositivos que mejor se adapten a las necesidades técnicas de la empresa y considerar que sean recomendados por las comunidades técnicas, especialmente si no se puede contar con herramientas de pago. En cuanto a los respaldos, la mejor opción es considerar el espacio en la nube y no utilizar mecanismos físicos que puedan dañarse o perderse. Otra recomendación es que, a medida de lo posible, se considere invertir en otras herramientas más allá de las anteriormente mencionadas, siempre y cuando se cuente con el presupuesto económico para este fin y en caso de tener sistemas manejados por terceros, estar pendiente sobre el uso de su información.

A su vez, a la hora de evaluar el tipo de ataques cibernéticos recibidos por las pequeñas empresas costarricenses en los años 2021 y 2022, se concluye que los ataques cibernéticos más comunes son aquellos derivados de la ingeniería social como estafas telefónicas y estafas por correo (también conocido como phishing). Para atacar este problema, se recomienda invertir o habilitar las opciones de reporte de phishing en lo que respecta a correos electrónicos y en cuanto a estafas telefónicas; es recomendable preparar al personal para que no brinde información de datos confidenciales a fuentes dudosas. Otro hallazgo con respecto a los ataques cibernéticos es que por la limitada infraestructura tecnológica de este tipo de empresas, los ataques más graves como ataques a servidores son poco comunes, sin embargo, se recomienda que para evitar estos posibles ataques —a pesar de no ser tan comunes—, se apliquen las buenas prácticas para mantener la seguridad en los servidores como respaldos, revisiones de sistema y

software, análisis de vulnerabilidades, entre otros mecanismos que se deben considerar acorde con las características de TI de la empresa.

Igualmente, al analizar el nivel de conciencia que se tiene sobre la seguridad tecnológica se concluye que las pequeñas empresas, especialmente a la hora de implementar el trabajo remoto, no están muy precavidas con asuntos como el robo de la información o el descuido de los equipos. Se recomienda en estos casos, señalar al personal todos los posibles peligros a los que pueden estar expuestos los sistemas y la información. Otra conclusión con respecto a este tema es que además del personal de TI, los demás empleados no están plenamente informados sobre los posibles peligros o en sí la seguridad cibernética de la empresa, en este caso se recomienda distribuir el conocimiento sobre estrategias de protección y precaución a los empleados para que estos estén al tanto y evitar posibles riesgos contra la seguridad que podrían significar pérdidas para la empresa o daños irreversibles. Si se encuentran en la capacidad de tiempo y personal, se recomienda llevar a cabo un taller relacionado con las mejores prácticas de ciberseguridad cada cierto tiempo para mantener la línea de aprendizaje con respecto a este tema. En la guía adjunta en el Anexo B se puede obtener más información con respecto a esto.

De igual manera, se concluye que las pequeñas empresas no tienen un vasto conocimiento sobre los ataques cibernéticos recibidos y cómo evitarlos, sin embargo, detentan un conocimiento general en tecnología y los conceptos básicos que se pueden explotar ya que esto da paso a que se genere una retroalimentación para estas empresas; se demuestra que existe una trascendencia respecto al tema de la información y los sistemas. Se recomienda que, a nivel de empresa, se continúe leyendo y aprendiendo sobre temas relevantes a la tecnología y las implicaciones de reforzar la seguridad en esta para que así, a futuro, sea más sencillo aplicar mejores mecanismos de refuerzo de ciberseguridad. También se concluye que si bien las empresas no poseen un conocimiento de marcos como el NIST sí cuentan con los conceptos generales de tecnología. Como recomendación se propone tratar de seguir el modelo de 5 etapas del NIST o al menos implementar alguna de las etapas a la hora de crear planes para mejorar la ciberseguridad. Es preferible que estas empresas lean el manual para su implementación de la mejor manera, sin embargo también se pueden guiar por las 5 etapas y crear sus propias estrategias para adaptarlas.

Finalmente, se concluye que las pequeñas empresas sí muestran cierto nivel de interés por mejorar sus situaciones en cuanto al tema de ciberseguridad en sus sistemas tecnológicos, esto ya que se mostraron dispuestas a recibir el manual de información (Anexo B) para informarse mejor sobre los temas expuestos. En este caso se recomienda que la información expuesta en el manual se adapte acorde a la situación de la empresa y sus respectivas necesidades o capacidades. Además, se determina que la mejor manera de distribuir el manual es por medio de los datos de contacto brindados por las pequeñas empresas como los correos electrónicos y números de teléfono. Se recomienda asegurarse de que el manual sea accesible y continuar con su uso cada cierto período, aunado a esto también se recomienda que las pequeñas empresas se sigan manteniendo informadas con respecto a temas de ciberseguridad, especialmente noticias importantes del país relacionadas con este tema, y que a medida de lo posible estén dispuestas a seguir mejorando sus medidas de seguridad. El manual informativo queda abierto para ser compartido con pequeñas empresas fuera de aquellas entrevistadas y, en caso de que alguna de

las empresas participantes decida unirse a la distribución de este material, queda la anuencia para seguir mejorando la ciberseguridad en las pequeñas empresas costarricenses.

Referencias

Aguilar, J.(2021).Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior.https://www.scielo.cl/scielo.php?pid=S0719-37692021000100169&script=sci_arttext#t1

Apuy,E.(2022)Caracterización del uso y necesidades potenciales de ciberseguridad..http://sistemas.procomer.go.cr/DocsSEM/166A6143-2E5E-405D-BC19-4AE058A45E2B.pdf

Banco Interamericano de Desarrollo y Organización de los Estados Americanos. (2020) .*Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en America Latina y el Caribe*. https://publications.iadb.org/en/2020-cybersecurity-report-risks-progress-and-the-way-forward-in-latin-america-and-the-caribbean

Beltrán Aldás, J. L. (2022). *Programa de concientización en seguridad de información para pequeñas empresas en la ciudad de Puyo (Master's thesis, Pontificia Universidad Católica del Ecuador).*

Cabezas Juárez, I. C. (2020). Implementación de un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima.

Cando-Segovia, M.R. & Medina-Chicaiza, P. (2021). PREVENCIÓN EN CIBERSEGURIDAD: ENFOCADA A LOS PROCESOS DE INFRAESTRUCTURA TECNOLÓGICA. (Spanish). 3C TIC, 10(1), 17–40. https://doi.org/10.17993/3ctic.2021.101.17-41

Carnero Garay, D. F., Armas-Aguirre, J., Antonio, M., Ramos, C., & Madrid Molina, J. M. (2020). Modelo de gestión de riesgos de seguridad de información para mitigar el impacto en las PYMEs en Perú. (Spanish). CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings, 1–6.

Cano Jeilyn.(2020). Pronósticos de seguridad/ciberseguridad 2021. https://peruciberseguro.org/pronosticos-de-seguridad-ciberseguridad-2021/

Cedeño Gómez, M. V. (2022). Marco de referencia para la implementación de controles de seguridad informática en una empresa de fabricación, comercialización y exportación de muebles.

Cordero-Robles, H. Y. (2021). Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST–Cybersecurity Framework,

para el mejoramiento y estandarización de las evaluaciones tecnológicas del área de auditoría de TI que apoya las auditorías financieras de los clientes de HCR.

Cortés, S. y Sáenz, R. 2022.MAYO 2022 CRONOLOGÍA DE LA PROTESTA SOCIAL.https://www.repositorio.iis.ucr.ac.cr/bitstream/handle/123456789/946/Crono_MAY22.pdf?sequence=1&isAllowed=y

Donadei Marta.(2019).APORTACIONES PARA LA DEFINICIÓN DE UNA METODOLOGÍA PARA LA INVESTIGACIÓN CUALITATIVA EN EL URBANISMO.https://idus.us.es/bitstream/handle/11441/95774/4313-16174-3-PB%20%281%29.pdf?sequence=1&isAllowed=y

Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). Methodology Based on the Nist Cybersecurity Framework as a Proposal for Cybersecurity Management in Government Organizations. 3C TIC, 10(2), 123–141. https://doi.org/10.17993/3ctic.2021.102.123-141

Grosser, S.(2020).Denuncias por fraude aumentaron 21.8% en 2019.https://delfino.cr/2020/03/denuncias-por-fraude-aumentaron-21-8-en-2019

IBIS.(2021).5 prácticas de ciberseguridad para pymes en 2021.https://www.ibiscomputer.com/blog/128-5-practicas-de-ciberseguridad-para-pymes-en-2021

INEC.(2019).Encuesta Continua de Empleo al primer trimestre de 2019.https://www.inec.cr/sites/default/files/documetos-biblioteca-virtual/reeceit2019.pdf

Landázuri Quintero, A. C. (2019). Técnicas de estudio en la comprensión lectora del subnivel elemental (Bachelor's thesis, Universidad de Guayaquil. Facultad de Filosofiía, Letras y Ciencias de la Educación.).

Lemaitre,R.(2021).Actividad programada dentro de la celebración del mes de la Ciberseguridad Año 2021.https://www.facebook.com/micitcr/videos/estado-de-ciberseguridad-en-costa-rica/248182280654795/

Marques,M.(2021).Ciberseguridad. ¿Por qué las pymes sufren la mayor parte de los ataques informáticos?.https://www.finanzarel.com/blog/ciberseguridad-pymes-sufren-la-mayor-parte-de-los-ataques-informaticos/

MEIC.(2021).Estado de Situación PYME en Costa Rica 2021.http://reventazon.meic.go.cr/informacion/estudios/2021/pyme/DIGEPYME-INF-038-2021.pdf

MEIC.(2020).Impacto de la pandemia por Covid-19 en las PYME.costarricenses.http://reventazon.meic.go.cr/informacion/estudios/2020/pyme/covid19.pdf

Méndez, A. E. L. (2021). Propuesta de estrategias de seguridad cibernética. Aproximaciones teórico–prácticas hacia el aprestamiento en países latinoamericanos. Dominio de las Ciencias, 7(1), 1186-1207.

Mendivil Caldentey, J., Sanz Urquijo, B., & Gutierrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. Pixel-Bit, Revista de Medios y Educacion, 63, 197–225. https://doi.org/10.12795/pixelbit.91640

Microsoft. (2022, 19 abril). 9 de cada 10 pymes en Costa Rica consideran que la pandemia aceleró su proceso de transformación digital. Microsoft News Center Latinoamérica. https://news.microsoft.com/es-xl/9-de-cada-10-pymes-en-costa-rica-consideran-que-la-pandemia-acelero-su-proceso-de-transformacion-digital/

National Institute of Standards and Technology.(2018).Framework for Improving Critical Infrastructure Cybersecurity.https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NCSI.(2019).60.Costa Rica 53.25.https://ncsi.ega.ee/country/cr/412/#details

Piza Burgos, N. D., Amaiquema Márquez, F. A., & Beltrán Baquerizo, G. E. (2019). Métodos y técnicas en la investigación cualitativa. Algunas precisiones necesarias. Conrado, 15(70), 455-459.

Pruna, F. X. J., Jeada, P. V. Y., & Jumbo, J. L. C. (2020). Análisis de las características del sector microempresarial en Latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información. Revista Científica ECOCIENCIA, 7(1), 1-26.

Ramírez Mesa, C., & González López, J. C. (2020). Guía de Controles y Buenas Prácticas de Ciberseguridad para MiPymes.

René.E & Arce,Á & Romero,W & Soledispa,C.(2019).Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro.http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400487

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

Revista Summa.(2021).Ante ataques cibernéticos en Costa Rica: Esta es la guía de ciberseguridad que toda empresa debe contemplar.https://revistasumma.com/ante-ataques-ciberneticos-en-costa-rica-esta-es-la-guia-de-ciberseguridad-que-toda-empresa-debe-contemplar/

Rimachi Salazar, Z. (2019). El financiamiento, rentabilidad y tributación de la micro y pequeña empresa del sector servicios Consultor y Contratista Generales “Los Andes” SAC del distrito de Ayacucho, 2018.

Rodríguez Arroyo, H. A. Importancia de controlar todas las amenazas detectadas a través de Magerit v. 3 e ISO/IEC 27002 según análisis de ataques informáticos en Latinoamérica.

Rosa,J & Galán,J.(2019).“CIBERSEGURIDAD PARA PYMES”.https://core.ac.uk/download/pdf/250406325.pdf

Sánchez Flores, F. A. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. Revista digital de investigación en docencia universitaria, 13(1), 102-122.

Santaolalla,A.(2022).Seguridad informática: tipos, consejos y herramientas.https://www.beedigital.es/tendencias-digitales/seguridad-informatica-tipos-consejos-y-herramientas/

Solano Méndez, G. E. (2020). Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica.

Sulima,N & Mora,S.(2022).Ciberseguridad y la respuesta de Costa Rica a los ciberataques.https://www.elfinancierocr.com/opinion/ciberseguridad-y-la-respuesta-de-costa-rica-a-los/JUAOYAI2V5A2VED4C3WJ3TR2DE/story/

Trujillo Chavarro, C. (2019). Casos de estudio de cybercrimen para el mejoramiento de la seguridad informática en pymes y medianas empresas.

Tully,L.(2020).Automatización de edificios y ciberseguridad (I).https://www.acrlatinoamerica.com/202002158575/articulos/automatizacion-de-edificios/automatizacion-de-edificios-y-ciberseguridad-i.html

UCR.(2022).Debemos navegar en internet a la defensiva.https://www.ucr.ac.cr/noticias/2022/06/09/debemos-navegar-en-internet-a-la-defensiva.html

Ulloa-Mora, J. (2021). Automatización, ciberseguridad y ciencia de datos: la nueva estrategia empresarial.

Valverde,M.(2022).Las pequeñas y grandes empresas son el futuro de Costa Rica.https://delfino.cr/2022/01/las-pequenas-y-grandes-empresas-son-el-futuro-de-costa-rica

Anexo A. Propuesta de entrevista

Parte I.

Previo al inicio de la entrevista se le solicitará el consentimiento del entrevistado para que la sesión sea grabada por medio de la herramienta Zoom. Se le indicará al entrevistado el propósito de esta investigación, si desea brindar información extra de las preguntas es opcional, si hay preguntas que no desea responder se le respetará y se continuará con las siguientes preguntas.

Parte II.

Guía de preguntas para la entrevista

1. ¿Qué entiende usted por Ciberseguridad? Desarrolle ampliamente su respuesta.
2. ¿Ha invertido durante el último año en algún tipo de seguridad tecnológica o instalado alguna herramienta de seguridad (Antivirus, antispyware, antimalware, firewalls)?
3. ¿Dentro de su empresa tienen personal encargado al área de TI o es solo su persona manejando cada área?
4. ¿Dentro de su empresa el personal de tecnología y personal de seguridad están unificados o están separados?
5. Por favor identifique qué métodos de seguridad tienen implementado en su empresa.
    a. Antivirus (Norton, AVG Antivirus, McAfee, entre otros)
    b. Antispyware
    c. Antimalware
    d. Firewall (WindowsFirewall, Linux Firewall, Netdefender, entre otros)
    e. Ninguna
    f. Otros
6. Durante la pandemia, ¿usted implementó alguna estrategia para que los colaboradores de la empresa trabajaran virtualmente desde sus hogares, algunas áreas de trabajo o la totalidad de su empresa?
7. ¿Qué modalidad de trabajo siguió usted al comienzo y durante toda la pandemia?
8. ¿Qué tipos de ataques cibernéticos han enfrentado en su empresa?
    a. Estafas Telefónicas
    b. Phishing (estafas por correo)
    c. Ransomware (malware que roba información encriptando)
    d. Virus
    e. Adwares (malware que proviene de anuncios)
    f. Troyanos (malware que elimina, copia, modifica, interrumpe computadoras)
    g. Gusanos/Worms (malware que se propaga en diversas computadoras)
    h. Suplantación o Modificación web (ataque que cambian la página web o roba información)
    i. No se ha recibido ningún ataque cibernético
    j. Otros: ¿Cuáles?
9. ¿Con respecto al 2020 ha mejorado su área de seguridad contra los ataques cibernéticos? Escala: Nada, Poco, Algo, Mucho
10. ¿Cada cuánto ustedes solicitan cambios de claves de usuario en su empresa?

11. ¿Qué tan complejo es su código de contraseña? Escala: Nada complejo, Poco complejo, Complejo, Muy complejo). Detalle por qué.
12. ¿Qué protocolos ustedes utilizan para loguearse de manera segura cuando navegan en internet? (Ej.: VPN u otros (¿cuáles?))

Anexo B. Manual informativo.

Pasos a tomar en cuenta a la hora de realizar una estrategia de ciberseguridad.	
Identificar	Realizar un análisis exhaustivo sobre los problemas de ciberseguridad a los que se encuentra expuesta la empresa para poder concentrarse en estos, además de los servicios principales que se puedan ver afectados por riesgos en la seguridad.
Proteger	A la hora de tener una idea sobre los posibles riesgos y las áreas afectadas, se debe identificar los mecanismos o herramientas necesarias para dar protección a los puntos afectados de la empresa.
Detectar	El monitoreo continuo de los sistemas ayuda a identificar la repetición de amenazas o descubrir nuevos riesgos en los sistemas tecnológicos de la empresa. Implementar planes de monitoreo en las funciones principales de la empresa ayuda a tener un mejor control a la hora de detectar posibles amenazas.
Responder	Una vez identificadas las posibles amenazas a la infraestructura o información de la empresa, esta debe implementar las medidas necesarias para poder mitigar estas amenazas y mantener el negocio corriendo. Cada protocolo de respuesta se adapta a los hallazgos y necesidades de la empresa según sus respectivos fallos en seguridad.
Recuperar	Las empresas deben implementar planes de restauración de servicios, equipos o información acorde a la infraestructura de esta. El NIST indica que las empresas deben contar con procedimientos de recuperación e implementar mejoras basadas en la experiencia conforme se vaya enfrentando casos de ciberseguridad.
Ataques comunes y posibles recomendaciones	
Ingeniería social	Los ataques por medio de ingeniería social pueden ser tanto las posibles estafas por llamadas o mensajes telefónicos, así como correos electrónicos que buscan suplantar a otras empresas o personas con el fin de engañar al receptor del ataque. Estos pueden venir en forma de simples preguntas sobre información

	personal, o links que lleven a la descarga de programas maliciosos que pueden dañar los sistemas y robar la información. Existen varias recomendaciones que se pueden brindar con respecto a esto: - No exponer datos de confianza cuando no se tiene claro la fuente que trata de obtenerlos. Siempre se debe asegurar que al hablar con una empresa o demás, está lidiando con personal oficial y no con personas suplantando una identidad. - Si no está seguro de que está lidiando con personal oficial, siempre es recomendable comunicarse con las empresas por canales oficiales para asegurarse que la interacción es legal. - Informar al personal de la empresa con respecto a esta clase de ataques y mantenerlos informados con respecto a estas situaciones para que ellos puedan aprender. - A medida de lo posible, realizar simulacros de estos ataques para comprobar la reacción de la empresa y sus empleados con respecto a estos. - Activar mecanismos anti-phishing en las cuentas de correo de los empleados y asegurarse que posibles mensajes de spam no se reciban en la carpeta principal de recibidos. - Educar al personal sobre la lectura de nombres y direcciones de correo electrónicos en caso de recibir correos sospechosos para que estos no caigan en los engaños que estos representan. - Reportar cuando se reciben correos por parte de fuentes dudosas para así poder informar al resto de la empresa y evitar que exista una brecha de seguridad por descuido de algún empleado.
Ataques a los sistemas o equipos	Estos ataques se pueden dar por varias razones tal como la descarga de archivos dudosos, visita a sitios web restringidos, inserción de hardware malicioso a los equipos, entre otros. Las recomendaciones con respecto a estos casos pueden variar, a continuación, unas medidas básicas que se pueden tomar en cuenta: - Implementación de herramientas antivirus para la protección de los equipos. De preferencia realizar una inversión económica para implementar los mejores programas de este tipo, en caso de no ser posible, consultar las mejores opciones que se adapten al presupuesto de la empresa.

	- Realizar análisis de los equipos de manera constante para comprobar que no existe algún elemento malicioso en las computadoras o demás. - Educar a los empleados para que estos no utilicen mecanismos como dispositivos USB u otros de este tipo que no sean de la empresa para evitar posibles riesgos en los equipos. - Bloquear sitios maliciosos que puedan guiar a las personas a la descarga de archivos peligrosos en los equipos. - Intervenir en la navegación por la red de los empleados, esto se puede lograr por medio del uso del VPN y está adjunto al punto anterior. - En caso de tener que descargar software para los equipos, siempre asegurarse que este provenga de las fuentes oficiales. Además, siempre se debe controlar los programas que los empleados instalan en sus computadoras para comprobar que estos sean necesarios para sus funciones en la empresa. - Evitar el acceso a sitios como redes sociales pues estos también pueden representar un peligro a la integridad de los sistemas de la empresa. - Mantener los programas y sistemas operativos actualizados para así obtener los mejores parches de seguridad y evitar que se exploten las vulnerabilidades de versiones anteriores.

Otras recomendaciones

Las presentes son recomendaciones extra que también pueden complementarse con las recomendaciones brindadas en los puntos anteriores:

- Establecer un protocolo con respecto a las contraseñas donde estas deban tener características como distintas letras, números y caracteres especiales. Además, establecer un período de tiempo para reemplazar estas contraseñas por nuevas para evitar riesgos. Educar a los empleados sobre ciertas reglas a la hora de escoger sus contraseñas como el no hacer uso de fechas de cumpleaños, nombres fáciles de reconocer, nombres de mascotas, entre otros. En lo posible utilizar un software de generación de contraseñas.
- Educar a los empleados con respecto al cuido de la información y de los equipos. Aspectos como asegurarse que las computadoras siempre estén en lugares seguros, bloquear el acceso a éstas en caso de que el empleado se ausente por un momento, utilizar la posibilidad de encriptar archivos importantes para proteger la integridad de la información, no compartir información de la empresa a través de medios no autorizados por la empresa, entre otras medidas.
- A medida de lo posible, evitar que los empleados utilicen equipo que no pertenezca a la empresa para realizar actividades laborales o manipular información relevante a la empresa. Si es posible evitar el uso de computadoras personales para el trabajo pues esto puede implicar la afectación de elementos laborales por el uso de programas

personales y demás.

- Cuando se utilizan sistemas implementados por otras empresas (ejemplo sistemas de facturación de terceros y demás) asegurarse que la información brindada a estos sistemas está segura y no expuesta.
- Es importante siempre tener mecanismos de respaldo en caso de que exista pérdida de información.
- En caso de tener sistemas propios, asegurarse que a la hora de realizar código este siempre esté actualizado y se realicen las comprobaciones necesarias para evitar ataques a los servidores.
- Mantener los datos en bases de datos y demás encriptados para evitar el posible acceso a estas por parte de terceros maliciosos.