Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Evaluación de la Existencia de Políticas de Ciberseguridad en las Pymes y en las Organizaciones del Sector Público que no cuentan con Personal de Ciberseguridad en Costa Rica

Elaborado Por:

Solarte Castañeda, César

Setiembre de 2021

DECLARATORIA DE DERECHOS DE AUTOR

DEDICATORIA

Dedico este trabajo a mis padres: César Solarte Solarte, Pilar Castañeda Medina, a mi hermana Ángela Solarte Castañeda y a mi cuñado Aarón Bolaños Cuevas que han sido mi apoyo incondicional durante toda esta etapa de esfuerzo y sacrificio. Siempre brindándome la motivación y las fuerzas para seguir adelante a pesar de las dificultades. A Dios por darme sabiduría y las fuerzas para lograr este objetivo.

AGRADECIMIENTOS

Agradezco a mi familia por todo el apoyo y amor incondicional. Agradezco a los profesores de la Universidad Cenfotec por toda la instrucción recibida durante estos años de estudio. A mi tutor de Tesis Miguel Pérez por guiarme con su consejo e instrucción durante la elaboración del proyecto de graduación. A todas las personas que me han apoyaron de una u otra forma en todos los momentos difíciles y que nunca dejaron de creer en mí.

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: Maestría en Ciberseguridad, requisito para optar por el título de grado de Maestría, para el estudiante: Solarte Castañeda César.

MIGUEL PEREZ MONTERO (FIRMA)

M. Sc. Miguel Pérez Montero
Tutor

YAHAIRA ROCIO SOSA ARIAS (FIRMA)
Firmado digitalmente por YAHAIRA ROCIO SOSA ARIAS (FIRMA)
Fecha: 2021.10.08 10:24:32 -06'00'

M. Sc. Yahaira Sosa Arias
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2021.10.08 11:25:56 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 07 de octubre de 2021

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

Tabla de contenido

Capítulo 1. Introducción

1.1 Generalidades

El avance acelerado de las tecnologías de la información y la creciente dependencia hacia las herramientas tecnológicas de todas las áreas de la sociedad, en contraste con el limitado conocimiento que se tiene por parte de la mayoría de la población al respecto de los riesgos inherentes al mal uso de las herramientas, hacen que existan amenazas en el sector comercial de Costa Rica, particularmente en las pymes; pues se desconoce el nivel de importancia que la seguridad informática puede brindar a ese delicado problema, ya que la seguridad informática no tiene el nivel de importancia que debería tener.

1.2 Antecedentes del problema

Si bien es cierto, contar con unas columnas robustas en materia de seguridad informática en las empresas siempre ha sido necesario, a raíz de la coyuntura ocasionada por el COVID-19, este aspecto se ha vuelto sumamente crítico, ya que la dependencia de la tecnología para realizar actividades básicas de la sociedad se ha disparado, trayendo consigo a los cibercriminales que buscan aprovecharse de estos portillos.

Joaquín Martínez, gerente de Fortinet Costa Rica, menciona sobre el tema de los ataques cibernéticos en Costa Rica: “Vemos una creciente actividad cibercriminal hacia objetivos en Costa Rica a medida que los *hackers* continúan lanzando métodos de ataque sofisticados dirigidos a víctimas desprevenidas, independientemente de su ubicación. El año 2020 demostró la capacidad de los delincuentes para invertir tiempo y recursos en ataques más lucrativos, como el *ransomware*. Además, se están

adaptando a la nueva era del trabajo remoto con acciones más sofisticadas para engañar a las víctimas y acceder a las redes corporativas". La firma estadounidense Fortinet detectó casi 32 millones de intentos de ciberataques durante el mismo periodo del año en Costa Rica, mediante el envío de códigos maliciosos del tipo, los cuales se intensificaron durante marzo con el inicio de la pandemia del COVID-19.

El Digital Trust Insights Pulse Survey Findings 2020 de la empresa Price Waterhouse Cooper indicó que en el 78 % de las firmas ya se había avanzado en términos de entrenamiento y concientización con sus colaboradores en materia de seguridad. Por su parte, Cecilia Pastorino, especialista en Seguridad Informática de ESET Latinoamérica, indicó: "Respecto al aumento de ataques y fraudes en línea se ha visto un incremento en toda Latinoamérica durante los últimos años, especialmente en las entidades financieras, no solo en Costa Rica; pasó también en Chile y en México. Es algo que ocurre porque el fin de los ciberdelincuentes ahora es obtener dinero, ya no es por fines ideológicos o activistas".

El Instituto Costarricense de Acueductos y Alcantarillados (AyA) sufrió un ataque informático durante la madrugada del sábado 1 de agosto del 2020 que afectó el funcionamiento de sus servicios digitales. "Una revisión preliminar permite establecer que la principal afectación del hackeo se centra, para efectos del usuario externo, en la afectación en el sistema que emplean los agentes recaudadores, por lo cual no es posible realizar los pagos en los agentes recaudadores o ejecutar consultas de facturación en nuestras plataformas digitales", dijo la entidad.

Por su parte, el sitio web Box Correos, de la institución estatal Correos de Costa Rica, sufrió un ataque de *ranswomware* el jueves 23 de julio de 2020, el cual fue dirigido a los servidores del proveedor de Correos de Costa Rica que administran la parte

operativa del servicio. “Estimamos una afectación de más de ¢50 millones, correspondientes al monto de las transacciones que debieron realizarse en este periodo que el sitio ha estado inactivo”, respondió Oscar Calderón, gerente de logística de Correos de Costa Rica.

1.3 Definición y descripción del problema

Según datos del Ministerio de Economía, Industria y Comercio, para el 2017 las pymes representaron el 97.5 % del parque empresarial a nivel nacional. Esto significa que la mayoría de industrias son pymes y comparten muchas características similares en cuanto a su gestión de la información. Si se toma como base que la prioridad de las pymes desde su constitución es producir un bien y posicionarse en el mercado, se ve que la seguridad de la información está muy lejos de ser considerada una prioridad. A esto se le suma que el grado de alfabetización digital por parte de los integrantes de las pymes reduce la conciencia de la necesidad de contar con conceptos de seguridad de la información desde el mismo nacimiento de las pequeñas empresas.

El estudio de la Contraloría General de la República de Costa Rica titulado *Medidas tomadas por las instituciones ante la derogatoria de las Normas Técnicas para la Gestión de las Tecnologías de Información*, publicado en agosto del 2021, destaca que 34 % de las instituciones tiene un bajo nivel de implementación del proceso de gestión de seguridad de la información y el 55 % no cuenta con personal dedicado a esta labor. Además, el 45 % no tiene un proceso de gestión de la ciberseguridad de la información y el 62 % no cuenta con personal dedicado en esta especialidad.

En cuanto a las instituciones que disponen de personal de seguridad y ciberseguridad de la información, el 93 % ha recibido capacitación en esos campos, la cual se ha gestionado directamente por la institución a nivel interno o externo; otros mediante el apoyo del Centro de Respuesta de Incidentes de Seguridad Informática de Costa Rica del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. La derogatoria de la Norma Técnica para la Gestión y el Control de las Tecnologías de Información, a partir de enero de 2022, implica la necesidad de declarar e implementar marcos de gestión de TIC a la medida de las instituciones, por lo tanto, su ausencia podría poner en riesgo la gestión y el control de las tecnologías; lo cual puede repercutir en forma negativa en la calidad y seguridad de la información, así como en los servicios que se brindan a la población.

1.4 Justificación

Existe una necesidad de crear conciencia sobre la importancia de la seguridad en el contexto de las pymes y en las organizaciones del sector público que no cuentan con personal de ciberseguridad en Costa Rica. Esto permitiría no solo una mejora desde el punto competitivo de los negocios, sino también en beneficio de toda la población; ya que al final es información personal la que circula de un lugar a otro en la red, porque el ciudadano es, en última instancia, el cliente de las pymes y las organizaciones del sector público.

1.5 Viabilidad

El desarrollo de un proyecto de investigación en un tema tan importante y necesario en la actualidad del país, cuyo costo de desarrollo no implica más que inversión de tiempo y que traería grandes beneficios para el sector de las pymes y las

organizaciones del sector público, hace que este proyecto sea viable desde todo punto de vista.

1.5.1 Punto de vista técnico.

Los conceptos aprendidos en la Maestría de ciberseguridad dan las bases técnicas para enumerar los puntos más importantes que se deben tomar en cuenta cuando se habla de seguridad informática en las pymes y las organizaciones del sector público. Enmarcar la importancia de conceptos como la disponibilidad, confidencialidad e integridad de la información gestionada en las pymes y las organizaciones del sector público brinda los lineamientos básicos, al igual que considera los conceptos de estándares como la IS0 27001 o el COBIT.

1.5.2 Punto de vista Operativo.

Para la ejecución de este proyecto, se realizan encuestas y entrevistas con diferentes encargados de tecnologías de la información que brindan sus servicios a pymes. Con la finalidad de ilustrar el panorama en el que se encuentran actualmente los sistemas que funcionan en las pymes, se aplican entrevistas virtuales, ya que, debido a la situación actual que vive el país a causa de la pandemia de COVID-19, se pretende minimizar el riesgo de exposición. También se cuentan los recursos en línea respecto a este tema.

1.5.3 Punto de vista económico.

Desde el punto de vista económico, el desarrollo de este proyecto implica inversión intelectual en la creación del proyecto. No implica gastos relacionados con compra de licencias, equipos de *hardware* ni ningún otro dispositivo. Existen los gastos mínimos que cualquier investigación tiene, sin embargo, no son representativos. Tomando en

cuenta estos factores, se puede decir que el proyecto es factible desde el punto de vista económico.

1.6 Objetivos

1.6.1 Objetivo general.

- Evaluar la existencia de políticas de ciberseguridad en las pymes y en las organizaciones del sector público que no cuentan con personal de ciberseguridad en Costa Rica.

1.6.2 Objetivos específicos

- Analizar las principales razones por las que no se contempla la seguridad informática como una prioridad en las pymes y organizaciones del sector público que no cuentan con personal de ciberseguridad.
- Describir los fundamentos de seguridad de la información en las pymes y organizaciones del sector público que no cuentan con personal de ciberseguridad, con el fin de contar con una base que se pueda utilizar.
- Identificar los principales estándares de seguridad informática que una pyme y organizaciones del sector público que no cuentan con personal de ciberseguridad pueden utilizar con el fin de dejar las bases para un mayor acercamiento con la seguridad informática.
- Identificar los diferentes modelos de seguridad que se pueden implementar en las pymes y organizaciones del sector público que no cuentan con personal de ciberseguridad de Costa Rica.
- Proponer un modelo de seguridad para las pymes y organizaciones del sector público que no cuentan con personal de ciberseguridad que contemple los aspectos más críticos y necesarios para alcanzar un grado alto de seguridad.

1.7 Alcances y limitaciones

1.7.1 Alcances.

- Documento que incluye los resultados de la investigación, recomendaciones y el modelo de seguridad que se puede aplicar en las pymes y organizaciones del sector público que no cuentan con personal de ciberseguridad, con el fin de tener un marco de conceptos de ciberseguridad que pueden ser aplicados por el encargado de TI.

1.7.2 Limitaciones.

- Para el desarrollo de este proyecto, solamente se contará con información relacionada a Costa Rica.
- No se pretende abarcar empresas que no sean consideradas pymes y organizaciones del sector público que cuentan con personal de ciberseguridad.

1.8 Marco de referencia organizacional y socioeconómico

Costa Rica fue conocido históricamente por ser exportador de café y banano. No obstante, en la década de los 90, con la llegada al país de la empresa Intel, se dio un cambio de modelo económico. Primero con la fabricación de microchips y luego hacia la exportación de servicios y tecnología avanzada, aprovechando el talento de una población educada y bilingüe. Debido a estas razones, el país ha podido seguir un camino muy distinto al de vecinos como Nicaragua, El Salvador u Honduras.

1.8.1 Historia.

Algunas de las grandes compañías extranjeras han establecido en Costa Rica sus sedes latinoamericanas, mientras que otras han traído al país operaciones en el área de servicios como atención al cliente, contabilidad, finanzas, soporte tecnológico y manejo de recursos humanos. Existen muchas empresas multinacionales que funcionan en zonas francas y que tienen una alta productividad. Estas empresas multinacionales son conscientes de la importancia de contar con altos estándares en cuanto al tema de la ciberseguridad. Sin embargo, son la minoría. El 95 % de las compañías de Costa Rica son empresas locales pequeñas o medianas y no tienen como prioridad el tema de la seguridad de su información.

Actualmente, en el contexto de la pandemia por COVID-19, se aceleró la digitalización con el teletrabajo, los servicios corporativos, el comercio electrónico, aprendizaje remoto, los eventos virtuales, la telemedicina, el desarrollo de aplicaciones y la comunicación, entre otros. Verónica Peña, directora regional de soluciones de trabajo moderno, seguridad y Surface de Microsoft, indicó que: “En dos meses se avanzó en la transformación digital lo que habría tomado 24 meses”.

De acuerdo con la investigación: 2020 Data Breach Investigations Report de Verizon, el 28 % de las violaciones de datos involucraron a víctimas de pequeñas empresas. Las pymes enfrentan un panorama diferente al de las grandes organizaciones que poseen la tecnología, equipo humano y procesos para afrontar los riesgos de seguridad. Algunas pymes no cuentan con el personal, presupuesto ni el conocimiento necesario para proporcionar ciberseguridad a su empresa y a sus clientes. “El primer paso para las pequeñas y medianas empresas es identificar. Es imposible proteger lo que no conocemos y por eso es necesario empezar por dónde

se encuentra mi información, qué dispositivos utilizo y cómo se comportan mis colaboradores. Identificar los activos de mi empresa permitirán definir el valor de la información y el por qué debo protegerla", dice Joey Milgram, gerente general de Soluciones Seguras Costa Rica.

1.9 Estado de la cuestión

Existen normativas e investigaciones que tienen por objetivo ampliar el panorama en cuanto a la seguridad informática en las empresas y las estrategias. La mayoría de las investigaciones realizadas en el tema de las pymes fueron realizadas en otros países. Sin embargo, la naturaleza y los retos que enfrenta una pequeña empresa son los mismos en Costa Rica que en cualquier parte del mundo. Contar con investigaciones internacionales permite identificar los puntos que también aplican para las industrias de Costa Rica y aplicar las recomendaciones.

Se han realizado búsquedas de información utilizando las palabras clave: *Cybersecurity* y *small business*. Los resultados se pueden observar en el anexo 1.
Uno de los marcos pioneros de seguridad cibernética fue creado por Ban y Heng (1995). Ellos propusieron crear medidas de seguridad en las pymes, pero solo las definieron como tareas: (i) emitir una política de seguridad informática; (ii) asignar responsabilidades en materia de seguridad; (iii) educar a todo el personal en temas de seguridad; y (iv) establecer un plan de ejecución simple y una estrategia de seguimiento para monitorear el cumplimiento de la seguridad.

En este capítulo, se presentan datos que indican que las estrategias que se utilizan para implementar políticas de ciberseguridad en las pymes son débiles y no cuentan con las especificaciones necesarias para reducir adecuadamente los riesgos inherentes del uso de tecnologías de información para realizar las labores básicas de una empresa.

A pesar de los innumerables beneficios y oportunidades, surgen retos cuando se adoptan las TIC, y las pequeñas y medianas empresas (PYMES) generalmente enfrentan mayores desafíos que los que encaran las compañías más grandes. El tener una infraestructura de TIC pobre, no saber cómo abordar adecuadamente las complejas amenazas de seguridad cibernética o subestimar la importancia de la protección de los datos personales son ejemplos de los desafíos para las pymes.

En la primera década del nuevo milenio, las organizaciones enfrentaron desafíos como los programas espía (*spyware*) y la detección de “suplantación de identidad (*phishing*) automática”, así como la detección de sitios intermediarios de derivación (*proxy bypass websites*); pero ahora son comunes retos más complejos como la detección de suplantación de identidad dirigido a un objetivo (*spear phishing*) (Symantec, 2018).

El nivel de conocimiento y preparación con respecto a la seguridad cibernética y la privacidad varía ampliamente según la pyme. Mientras que es posible que algunas hayan entendido y adoptado las medidas para proteger sus recursos y capacidades implementadas; otras tal vez no hayan implementado ninguna. De hecho, parte de esta problemática se debe a la falta de “cultura de seguridad”, definida como “actitudes, creencias y percepciones compartidas por los miembros del grupo, que definen normas y valores que, a su vez, determinan la forma en que actúan y reaccionan respecto al riesgo y al sistema de control de riesgos” (Lopes y Oliveira, 2014, p. 278).

El aspecto humano de la seguridad cibernética no debe subestimarse, dado su crucial importancia, por lo tanto, en este estudio se presentan algunas de las maneras en que este componente vital de la seguridad cibernética se puede fortalecer. Un estudio que intentó comprender los aspectos organizativos, tecnológicos y

psicológicos de la seguridad cibernética en las pymes encontró que la mayoría de los empleados (dos tercios) no informaron sobre sus errores a sus superiores (Zec y Kajtazi, 2015). Además, la “ausencia de políticas cibernéticas internas en las PYME” y las “bajas inversiones financieras” también fueron factores que pusieron a las pymes en una posición vulnerable (Zec y Kajtazi, 2015, p.237).

Los ciberdelincuentes se están volviendo cada vez más sofisticados en el uso de nuevos métodos y herramientas para los ciberataques, a medida que los métodos de ataque actuales se vuelven menos efectivos y una vez que las organizaciones comprenden las amenazas y tienden a mantener su sistema de seguridad actualizado y preventivo (Gostev,2012).

PricewaterhouseCoopers (PwC) realiza anualmente la encuesta sobre infracciones de seguridad de la información para el Departamento de Negocios, Innovación y Habilidades (BIS) en el Reino Unido, con el fin de evaluar el nivel de infracciones de seguridad de la información en empresas y organizaciones. Los resultados de la encuesta del 2015 muestran que, cuando se les preguntó a los encuestados si estaban de acuerdo con algunos de los conceptos erróneos más comunes sobre mantener su negocio seguro en línea, más de tres cuartas partes (78 %) de las pequeñas empresas creyeron al menos uno. Estos incluían los siguientes mitos: solo las empresas que aceptan pagos en línea corren el riesgo de cometer un delito cibernético (26%): todas las pymes están en riesgo y, aunque la piratería del *software* de procesamiento de pagos es una táctica obvia, los delincuentes son muy oportunistas y pueden beneficiarse de robar una amplia gama de datos de empresas. Las pequeñas empresas no son un objetivo para los piratas informáticos (22 %); de hecho, las pequeñas empresas son un objetivo más grande que nunca, porque normalmente tienen muchos más datos que el consumidor medio, pero a menudo no

tienen más medidas preventivas establecidas para protegerse. En el 2014, el 33 % de las pequeñas empresas sufrieron un ciberataque de alguien ajeno a su negocio. El 24 % de las pequeñas empresas piensan que la seguridad cibernética es demasiado cara de implementar y el 22 % admite que “no saben por dónde empezar” (Bradley y Vaizey, 2015).

Las tendencias recientes muestran que los ciberataques dominan entre las pymes en comparación con las grandes empresas (Verizon, 2012; Symantec, 2014). Numerosos artículos periodísticos muestran la incapacidad de las pymes para hacer frente a las medidas de seguridad que reflejan su desconocimiento en este dominio.

James Lyne, director global de investigación de seguridad en Sophos y partidario de la campaña Cyber Streetwise, dijo: “las pequeñas empresas tienen una gran cantidad de datos, pero muchas no se dan cuenta de lo valiosos que son estos datos y de lo grave que podrían ser las consecuencias si cayeran en las manos equivocadas. Por ejemplo, la propiedad intelectual de una empresa podría venderse a un competidor e incluso las direcciones de correo electrónico se pueden vender a los *spammers* para obtener ganancias”.

Existen varios marcos de ciberseguridad muy prestigiosos que son utilizados por las grandes empresas, como lo son la NIST, el ISO 27001 y el COBIT; en Costa Rica: la Norma Técnica de la Contraloría General de la República. (N-2-2007-CO-DFOE). NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés) dependiente del Departamento de Comercio de EE. UU. El Marco de Ciberseguridad del NIST ayuda a las pymes a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, así como proteger sus redes y datos. Creado a través de la colaboración entre la industria y el gobierno, el Marco voluntario consta de estándares, pautas y

prácticas para promover la protección de la infraestructura crítica. El enfoque priorizado, flexible, repetible y rentable del Marco ayuda a los propietarios y operadores de infraestructura crítica a gestionar los riesgos relacionados con la ciberseguridad. Proporciona un conjunto de actividades y resultados de ciberseguridad deseados utilizando un lenguaje común que es fácil de entender. La NIST guía a las organizaciones en la gestión y reducción de sus riesgos de ciberseguridad de una manera que complementa los procesos de ciberseguridad y gestión de riesgos existentes de una organización.

La Organización Internacional de Estandarización (ISO), a través de las normas recogidas en ISO / IEC 27000, establece una implementación efectiva de la seguridad de la información empresarial desarrollada en las normas ISO 27001 / ISO 27002. ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2017 y ahora su nombre completo es ISO/IEC 27001:2017. La primera revisión se publicó en 2005 y fue desarrollada con base en la norma británica BS 7799-2.ISO 27001; se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

COBIT es un marco para la gestión de la tecnología y la información, y para el gobierno de la empresa, aplicable a cualquier tipo de compañía. Se entiende como I&T toda la tecnología y el tratamiento de información que aplica la empresa para conseguir sus objetivos, con independencia del departamento donde se aplique. COBIT (Objetivos de control para la información y tecnologías relacionadas) apareció por primera vez en 1996 como un conjunto de elementos que tenían la finalidad de ayudar a los auditores financieros a conocer mejor el entorno tecnológico a través de un control de estas tecnologías.

En 1998, se aprueba una nueva versión donde se amplía a otros ámbitos distintos de la auditoría. La tercera versión fue lanzada en el año 2000 y en ella se incluyen nuevos métodos de gobernanza y gestión de la información y las tecnologías. En 2005, aparece COBIT 4 y en 2007 COBIT 4.1. Ambos contienen una mayor información sobre la gestión de las tecnologías de información y comunicaciones.

En 2012 ISACA aprueba COBIT 5, actualizado en 2013. Aquí también se añade más información para el gobierno de la tecnología e información por las empresas. Finalmente, en noviembre de 2018 surge COBIT 2019. Este nuevo marco es mucho más completo y coherente. Establece nuevos planteamientos que pretenden adaptar el sistema de gobierno a las distintas necesidades de la empresa. Las áreas de enfoque establecidas son prácticamente ilimitadas, ya que pueden unir elementos de gobierno comunes con otros diferentes. Dentro de esas áreas de enfoque están: seguridad, organización de pymes, reguladores, desarrollo y gestión de *software*.

La Contraloría General de la República de Costa Rica creó en el 2007 las Normas técnicas para la gestión y el control de las tecnologías de información que fueron recientemente derogadas para enero del 2022, pero que hasta ese momento

las instituciones públicas costarricenses debían acatar. Estas normas técnicas brindan lineamientos en torno a la gestión de TI, si bien es cierto, la norma técnica ya no es de cumplimiento obligatorio por las instituciones del Estado, provee lineamientos de ciberseguridad que pueden ser utilizados por cualquier institución de Costa Rica. El Capítulo I Normas de aplicación general, en el inciso 1.4 Gestión de la seguridad de la información, habla puntualmente en lineamientos en temas de la ciberseguridad que pueden ser utilizados por cualquier pyme o institución del Estado como referencia.

A pesar de que existen muchos marcos de ciberseguridad, el problema que presentan para las pymes y pequeñas instituciones del sector público es que estos marcos fueron diseñados para organizaciones grandes y maduras, por lo que son complejos y difíciles para implementar y mantener. Esto no permite que puedan ser aprovechados por las organizaciones pequeñas que no cuentan con todos los recursos para implementar estos sistemas, pero que siempre necesitan contar con una guía en materia de ciberseguridad. No obstante, estos estándares proporcionan una excelente fuente de partida para que una pyme o institución pequeña del Estado pueda iniciar a familiarizarse con temas de ciberseguridad y la importancia para empezar a aplicarla en las organizaciones.

Por esta razón, a pesar de que estos marcos de ciberseguridad no están adaptados para estas organizaciones pequeñas, siempre resultan de gran utilidad y no deben desecharse por este hecho. El presente estudio busca crear un manual de ciberseguridad basado en estos marcos ya existentes, pero que sea aplicable a una de estas pequeñas organizaciones. Siendo este manual un primer paso en el acercamiento hacia la culturización de la ciberseguridad.

El Centro Nacional de Seguridad Cibernética (NCSC) es una organización del Gobierno del Reino Unido que brinda asesoramiento y apoyo al sector público y privado sobre cómo evitar las amenazas a la seguridad informática. Con sede en Londres, entró en funcionamiento en octubre de 2016. Este centro de seguridad cibernética cuenta con un programa de concientización y educación en materia de seguridad de la información llamado Cyber Aware.

La campaña Cyber Aware, anteriormente Cyber Streetwise, brinda al público el asesoramiento que necesita para protegerse de los ciberdelincuentes. La mensajería dirigida a través de las redes sociales y la publicidad, en asociación con las empresas promueve: el uso de tres palabras al azar para crear una contraseña segura y siempre descargando las últimas actualizaciones de *software*. La adopción de estos comportamientos brindará a las pequeñas empresas y a las personas protección contra los delitos cibernéticos. Cyber Aware cuenta actualmente con el apoyo de 128 socios intersectoriales, incluida la policía y las empresas de los sectores minorista, de ocio, de viajes y de servicios profesionales. Según la estrategia de ciberseguridad nacional del Renio Unido, en 2016 aproximadamente diez millones de adultos y un millón de pequeñas empresas declararon que tenían más probabilidades de mantener o adoptar comportamientos clave de seguridad cibernética como resultado de la campaña Cyber Aware.

1.9.1.1 Formulación de la pregunta

Con el fin de focalizar los esfuerzos de búsqueda, es necesario formular una pregunta que sea precisa y permita obtener la mayor cantidad de artículos altamente relacionados con el tema.

1.9.1.1.1 Foco de la pregunta

Es necesario enfocarse en artículos técnicos que especifiquen los lineamientos de ciberseguridad necesarios para la implementación en empresas pequeñas y verificar que sean documentos que estén actualizados y brinden pautas.

1.9.1.1.2 Amplitud y calidad de la pregunta

Se requiere que la formulación de la pregunta se enfoque en la ciberseguridad de pymes menores a 40 empleados, ya que es necesario limitar su tamaño, porque siempre existen diferencias que pueden hacer que la implementación de un modelo de ciberseguridad sea totalmente diferente entre una y otra pyme.

1.9.1.1.3 Problema

El bajo grado de alfabetización tecnológica por parte del liderazgo de las pequeñas y medianas empresas en Costa Rica hace que no se cuente con una cultura que le dé importancia a la seguridad informática, lo que hace que estas empresas sean vulnerables ante ataques informáticos que tienen como objetivo el robo de información y la extorsión, entre otros.

1.9.1.1.4 Pregunta

¿Qué trabajos se han realizado en el tema de políticas de ciberseguridad en empresas pequeñas?

1.9.1.1.5 Palabras clave y sinónimos

Al ser un tema en el que la mayoría de información se encuentra en inglés, las principales palabras claves y sinónimos se buscarán en este idioma.

Tabla 1: Principales palabras claves

Palabras	Equivalente en inglés

Ciberseguridad	*Cybersecurity*
Pequeña empresa	*Small Business*
Políticas	*Policies*
Seguridad	*Security*
Información sensible	*Sensitive information*
Respaldos	*backups*
Contraseñas	*Passwords*
Amenazas de seguridad	*security threats*

1.9.1.2 Selección de fuentes

Tabla 2: Fuentes utilizadas

Autor(es) o Autora(s)	Año	Título	URL
Brian Little	2014	Small Business Security	http://www.cs.lewisu.edu/mathcs/msisprojects/papers/SMBSecurity_BrianLittle.pdf
Donald A. Heier, Guy W. Garrett	2014	A Study of Small Business Information Security in Rural America	https://www.una.edu/sobie/proc2014.pdf#page=31
Stephen Pritchard	2010	Navigating the black hole of small business security	https://www.sciencedirect.com/science/article/abs/pii/S1754454810700851
John Edwards Vail	2012	Small Business Information Security	https://thescholarship.ecu.edu/bitstream/handle/10342/3889

			/Vail_ecu_0600M_10664.pdf?sequence=1&isAllowed=y
Camila Trujillo Chavarro	2019	Casos de Estudio de Cibercrimen para el Mejoramiento de la Seguridad Informática en pymes y medianas empresas	https://repository.unad.edu.co/bitstream/handle/10596/30220/ctrujilloch.pdf?sequence=1&isAllowed=y
Wilson Jiménez Castillo	2017	Seguridad Informática o de la Información en pymes	http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4929/51183%20-%20Jim%C3%A9nez%20Castillo%20Wilson.pdf?sequence=1&isAllowed=y

El artículo *Small Business Security* de Brian Little proporciona una introducción fácil para implementar la seguridad de las pequeñas empresas. La meta es mostrar a las pequeñas empresas cómo mantener seguros sus datos presentando el material de una manera que pueda ser entendido por cualquier persona, independientemente de su formación técnica. Se mencionan temas para la seguridad de pequeñas empresas en los siguientes aspectos: contraseñas, internet y uso del correo electrónico, seguridad informática, seguridad de datos y seguridad de la red e información actual sobre estos. Los temas que se tratan deben considerarse como la línea de base para cualquier pequeña empresa. La investigación futura puede desarrollar estas sugerencias de seguridad introductorias al ofrecer opciones más avanzadas para pequeñas empresas.

El artículo *A Study of Small Business Information Security in Rural America* de Donald A. Heier, Guy W. Garrett analiza una metodología de investigación propuesta

para determinar la postura de las pequeñas empresas respecto a la seguridad de la información y las limitaciones de las prácticas de seguridad de la información. Se propone una metodología de estudio de caso cualitativo que incluye una encuesta cuantitativa y criterios de selección para los participantes del estudio.

Por su parte, el artículo *Small Business Information Security* de John Edwards Vail menciona el hecho de que, si bien se han realizado muchos estudios de seguridad en organizaciones a escala empresarial, la investigación similar sobre pequeñas empresas en los EE. UU. es limitada. Una pequeña empresa fue evaluada por una auditoría de seguridad de la información para determinar si su información, los recursos y la red eran suficientemente seguros. Los resultados se usaron como un caso de prueba para identificar un enfoque que una pequeña empresa típica puede tomar para proteger sus redes y datos, con el fin de evitar la exposición de responsabilidad innecesaria.

Al examinar los factores de riesgo específicos en este estudio de caso, el autor cree que otras pequeñas empresas pueden establecer paralelismos como punto de partida para examinar sus propios factores de riesgo. Además, este estudio proporciona una serie de procesos de mitigación para mejorar la seguridad de la red de las pequeñas empresas que pueden adoptar otras pymes en circunstancias similares.

El artículo *Casos de Estudio de Cibercrimen para el Mejoramiento de la Seguridad Informática en pymes y medianas empresas* de Camila Trujillo Chavarro consiste en el estudio de casos de cibercrímenes, presentados a nivel mundial, para proponer pautas de mejoramiento de la seguridad informática en pymes de Colombia. Estas organizaciones se ven muy afectadas por sus escasos controles, además de considerar que el solo hecho de tener un antivirus evita un ataque cibernético, que se

ha visto en crecimiento por su gran rentabilidad y fácil ejecución. También hay que recordar que, detrás de este delito, no solo se encuentra un *hacker* aficionado en busca de probar sus conocimientos, sino que ahora es un crimen organizado que mejora los malvares antiguos haciéndolos eficientes y menos detectables. El artículo tiene como función principal informar sobre un tema puntual basado en documentos periodísticos y científicos de interés para la comunidad.

El artículo *Seguridad Informática o de la Información en Pymes* de Wilson Jiménez Castillo menciona que, debido al auge de la tecnología y a la masificación en el mundo, las empresas la han adoptado como un medio significativo e importante de evolución y crecimiento. La tecnología junto con la información se han convertido en uno de los activos más importantes de las empresas, al contribuir en un alto grado en la evolución y ejecución del núcleo de negocio. Por esta razón, es de vital importancia preservar y salvaguardar la información en cualquier tipo de empresa, más aún en empresas pymes, por ser las que se ven expuestas o son más vulnerables a posibles eventos infortunados sobre su información.

Capítulo 2. Marco conceptual

2.1 Conceptos sobre contenido

Figura 1: Nube de palabras. Elaboración propia.

Figura 2: Mapa conceptual. Elaboración propia.

2.1.1 Definición de pymes

Según el Ministerio de Economía, Industria y Comercio, se entiende por pequeñas y medianas empresas (PYMES) toda unidad productiva de carácter permanente que disponga de los recursos humanos, los maneje y opere, bajo las figuras de persona física o de persona jurídica, en actividades industriales, comerciales, de servicios o agropecuarias que desarrollen actividades de agricultura orgánica.

Las empresas se clasifican según actividad empresarial como industriales, comerciales y de servicios, utilizando la Clasificación Industrial Internacional Uniforme de todas las Actividades Económicas (CIIU).

2.1.2 Ciberseguridad

La definición de ciberseguridad por parte de la Asociación de Auditoría y Control sobre los Sistemas de Información (Information Systems Audit and Control Association, ISACA) es la: “Protección de activos de información, a través del

tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

2.1.3 Amenazas de seguridad

Según el Dictionary of Computing de Oxford, amenaza de seguridad es cualquier acción destinada a violar la seguridad de la información almacenada en un sistema: (a) obteniendo acceso no autorizado a esa información generalmente sin alertar al usuario autorizado; (b) denegación de servicio al usuario autorizado; (c) suplantación, que tiene como objetivo confundir introduciendo información falsa, generalmente sobre la identidad del usuario. Algunas amenazas tienen una intención maliciosa premeditada, pero otras son oportunistas, por ejemplo, navegando o durante un accidente.

2.1.4 Políticas de seguridad

Las políticas de seguridad son la declaración de las medidas, especialmente operativas, por tomar para defender un sistema frente a las amenazas postuladas. La política puede especificar el modo de procesamiento de seguridad junto con el modelo de seguridad y su relación con los controles de seguridad física y personal. Por ejemplo, la política de seguridad generalmente especificará la forma en que se asignarán las contraseñas y los arreglos para la auditoría, etc.

2.1.5 Seguridad de la información

La seguridad de la información, según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. Estos pueden ser electrónicos, en papel, audio y vídeo, etc. Los gobiernos, las instituciones

financieras, los hospitales y las organizaciones privadas tienen enormes cantidades de información confidencial sobre sus empleados, productos, investigación, clientes, etc. La mayor parte de esta información es reunida, tratada, almacenada y puesta a disposición de las personas que deseen revisarla.

2.1.6 Información sensible

La Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales 8968 define los datos sensibles como información relativa al fuero íntimo de la persona, por ejemplo, los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

2.1.7 Cibercrimen

Según Adrián Acosta, oficial del crimen digital de Interpol, el cibercrimen cuenta con una definición aceptada como la capacidad de acceder sin previo consentimiento a información y datos que son propiedad de gobiernos, personas o empresas. Todo el mundo relaciona al cibercrimen con delitos tecnológicos, o sea, el uso de la tecnología para cometer crímenes. Sin embargo, hoy en día es mucho más amplio que eso, dado que muchos delitos se cometen a través del uso de la tecnología sin distinguir un crimen específico. Por otro lado, la evidencia digital que es algo que abarca en forma transversal a todas las investigaciones en estos momentos y puede llevar a confusión dado que todas las áreas llevan a cabo este procedimiento.

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

Siendo el objetivo de este proyecto evaluar la eficacia de los criterios que se utilizan para implementar las políticas de ciberseguridad en las pymes y

organizaciones del sector público que no cuentan con personal de ciberseguridad en Costa Rica, el tipo de investigación correspondiente es la evaluativa. Se espera generar como resultado de la investigación, recomendaciones prácticas sobre lineamientos de ciberseguridad y cómo aplicarlos en el contexto de una pyme u organización del sector público que no cuenta con personal de ciberseguridad en Costa Rica.

3.2 Alcance investigativo

Según indica Sampieri, sobre la investigación descriptiva se busca especificar las propiedades, características y los perfiles de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre las variables a las que se refieren.

Basados en esta definición, se puede afirmar que el alcance investigativo del presente trabajo es descriptivo, ya que, durante la revisión de literatura, mostró bastante información sobre el tema, lo que facilita la posibilidad de mostrar situaciones y contextos enfocados al ámbito de Costa Rica.

3.3 Enfoque

Esta investigación sigue la orientación del enfoque alternativo. Como define Naranjo (2020), el enfoque alternativo se ubica en el paradigma pragmático. Para alcanzar este fin, se hacen explícitas las dimensiones epistemológica, ontológica y axiológica de la investigación. Este apego al pragmatismo permite al investigador una enorme flexibilidad en el uso de diseños cuantitativos, métodos cualitativos o diseños mixtos, ampliamente documentados en las fuentes bibliográficas. La ganancia de ello

es que no se ve obligado a encuadrarse dentro de un enfoque con diseños o métodos predefinidos, por el contrario, utiliza lo necesario para alcanzar sus objetivos.

3.4 Diseño

El diseño de la investigación es mixto, utilizando el modelo imbricado, ya que la investigación abarca algunos aspectos que se pueden analizar de manera cuantitativa; mientras hay otros aspectos que se deben de manera cualitativa. Al ser un diseño que mezcla los diferentes conjuntos de datos en el nivel de diseño, se puede obtener un máximo aprovechamiento de los diferentes datos que se encuentran disponibles relacionados a la ciberseguridad en las pymes.

3.5 Población y muestreo

Según la definición de población proporcionada por Pita Fernández S, Pértega Díaz, S (2001), la población representa el conjunto grande de individuos que se desea estudiar y generalmente suele ser inaccesible. Es, en definitiva, un colectivo homogéneo que reúne unas características determinadas. Con respecto a la definición de *muestra*, los mismos autores plantean la siguiente definición: la muestra es el conjunto menor de individuos (subconjunto de la población accesible y limitado sobre el que se realizan las mediciones o el experimento con la idea de obtener conclusiones generalizables a la población). Por su parte, el individuo es cada uno de los componentes de la población. La muestra debe ser representativa de la población y con ello se quiere decir que cualquier individuo de la población en estudio debe haber tenido la misma probabilidad de ser elegido.

Con relación a las definiciones anteriores, se puede determinar que la población del estudio abarca la totalidad de las pymes en Costa Rica, y la muestra

por obtener será un estudio de 17 pymes ubicadas en Costa Rica. También se toma un estudio de la Contraloría General de la República de Costa Rica que abarca 161 instituciones del sector público costarricense.

Capítulo 4. Análisis del diagnóstico

4.1 Presentación

Con el fin de tener una perspectiva con respecto a la posición de las pymes en materia de ciberseguridad, se aplicó una encuesta a 17 jefes de pymes, en la que se les realizaron preguntas relacionadas con el uso de la ciberseguridad. En el análisis del diagnóstico, también se observaron los resultados del estudio realizado por la Contraloría General de la República de Costa Rica: *Medidas tomadas por las instituciones ante la derogatoria de las Normas Técnicas para la Gestión de las Tecnologías de Información*, que se publicó en agosto del 2021 y menciona temas relacionados a la implementación de la seguridad informática en las instituciones del sector público costarricense.

En el estudio realizado a 161 instituciones, 72 son las que cuentan con seguridad de TI y 61 instituciones cuentan con ciberseguridad. En el contexto de la Contraloría General de la República, seguridad de la TI corresponde a cualquier lugar donde esté la información, incluyendo hasta la información en formatos físicos. Ciberseguridad es la información que se expone a Internet. Con estos estudios se pretende analizar las principales razones por las que no se contempla la seguridad informática como una prioridad en las pymes.

4.2 Aplicación de cuestionarios

Los cuestionarios se distribuyeron selectivamente a jefes de pymes de Costa Rica, con el fin de procurar que los resultados fueran lo más precisos posible y que, de esta manera, mostraran un panorama acerca de la situación de la ciberseguridad en las pequeñas empresas de Costa Rica.

4.3 Análisis e interpretación

1. ¿En su empresa se generan respaldos de seguridad de la información relacionada con sistemas de información clave e información vital para su operación?

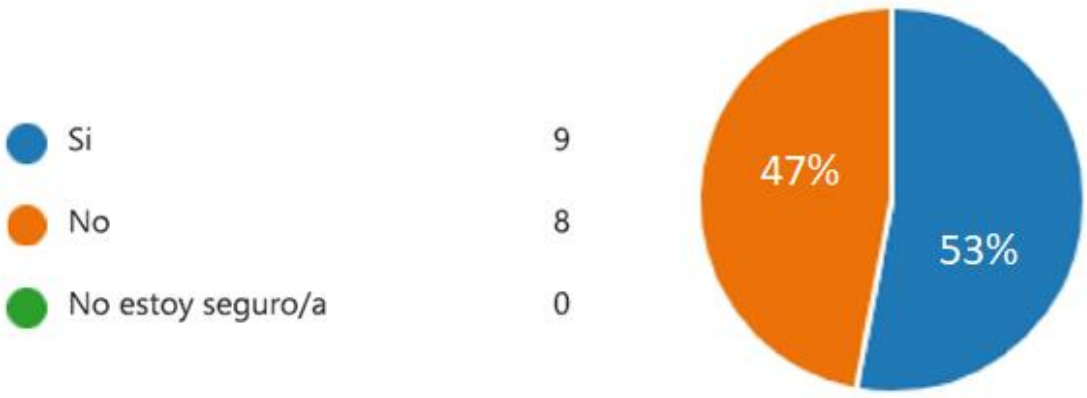


Figura 3: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

En relación con los respaldos, cabe resaltar el porcentaje tan alto (47 %) de pymes que no cuenta con un plan de respaldo de la información. Esto indica que la generación de respaldos de información del negocio no se encuentra generalizada en las pymes. Lo anterior pone en evidencia la vulnerabilidad de muchas de estas ante un ataque cibernético, por ejemplo, de *ransomware*, el cual obligaría a las pymes a pagar un rescate por la información corriendo el riesgo de que esta no sea del todo recuperable. También pone en una situación vulnerable a las pymes frente a un daño

físico como el de un disco duro o bien un desastre natural que imposibiliten a la organización a continuar operando.

2. ¿En su organización se procura la utilización de contraseñas seguras para el correo electrónico oficial?

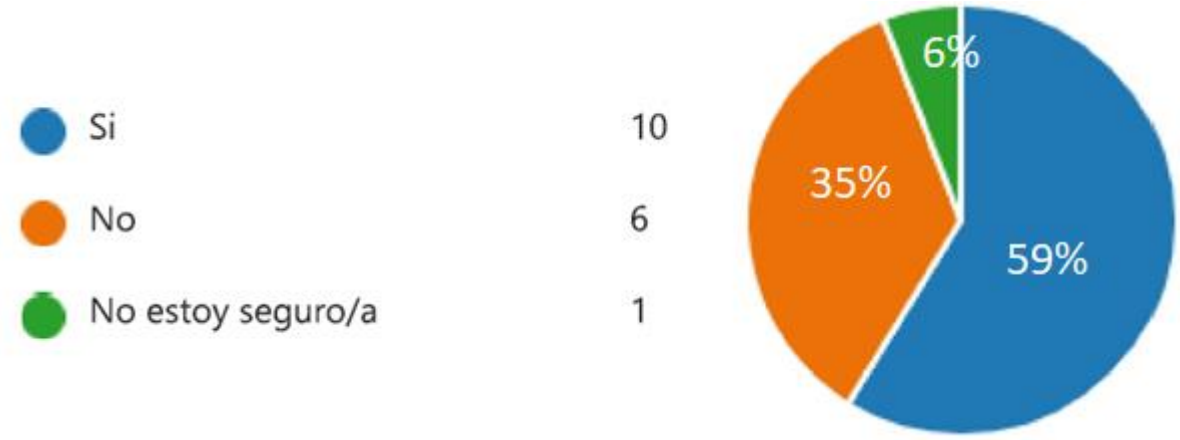


Figura 4: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

En la pregunta anterior, se puede ver que, aunque exista un porcentaje alto de pymes que procuran tener contraseñas seguras para el correo electrónico (59 %), existe un alto porcentaje que no utiliza contraseñas seguras (35 %) o no sabe (6 %). Es importante resaltar que la mayoría de ataques cibernéticos comienzan con una explotación de una contraseña débil, lo que le da acceso inicial a la organización y esto les permite ir explorando y adentrándose aún más en los sistemas de la organización. El no contar con una contraseña segura para el correo es una vulnerabilidad que pone en evidencia que las pymes se encuentran desprotegidas frente a ataques de fuerza bruta que buscan explotar las contraseñas débiles.

3. ¿Se tienen políticas o controles que establezcan que las contraseñas, tanto de los correos electrónicos del trabajo como las de los sistemas empresariales, sean diferentes entre sí?

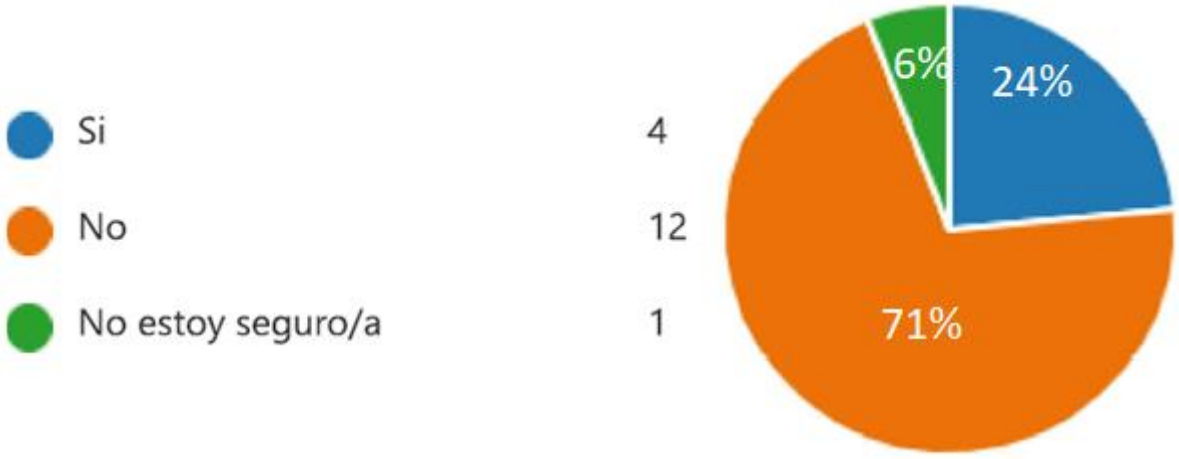


Figura 5: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

El gráfico anterior muestra que la mayoría de las pymes encuestadas (71 %) no cuenta con una política que haga que las contraseñas sean diferentes entre los diferentes sistemas. Esto permite que los empleados puedan utilizar la misma contraseña para todos los sistemas, lo que sería un riesgo en caso de que un actor malicioso pudiera obtener una contraseña de un usuario. Este podría acceder a los diferentes sistemas a los cuales tiene acceso el empleado. Cabe mencionar que existe el sistema de inicio de sesión único (*Single Sign-On*) que permite la gestión de las diferentes cuentas empresariales con una única contraseña de forma segura. Sin embargo, la implementación de este sistema de inicio único requeriría un gran esfuerzo en término de recursos por parte de la organización.

4. ¿Conoce si en su empresa está activada la autenticación de dos factores (ya sea por contraseña, huellas digitales, algún otro aspecto biométrico, tarjetas inteligentes, contraseñas temporales enviadas al correo o al celular, entre otros) para el acceso a los sistemas principales y a la información sensible de la empresa?

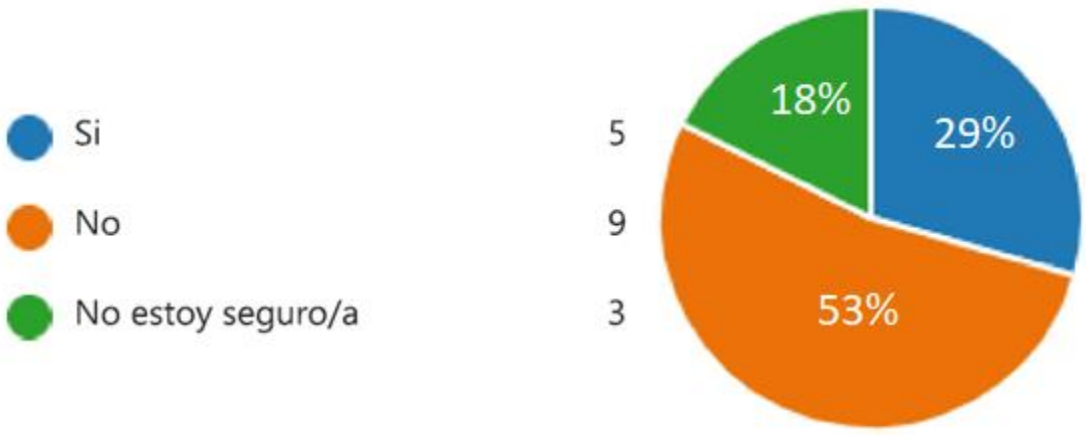


Figura 6: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Como muestra la pregunta anterior, más de la mitad de las pymes (53 %) no cuenta con un elemento adicional de seguridad como la autenticación basada en dos factores y el 18 % no está seguro, por lo cual es más probable que no tengan este tipo de autenticación. La autenticación de dos factores ha tomado popularidad en los años recientes, dado su gran efectividad, al no confiar exclusivamente en un factor como la contraseña; sino que, al contar con otro factor como un toquen, hace que, en caso de que la contraseña de un usuario haya sido vulnerada, no significa que ya el atacante tenga acceso al sistema, lo cual proporciona un nivel superior de protección. La configuración de los sistemas de dos factores no es sencilla y requiere conocimiento técnico. Sin embargo, ante la popularidad de este sistema, existen soluciones más accesibles como el uso del celular como un factor de autenticación.

5. ¿Qué dispositivos se utilizan dentro de su empresa para el entorno laboral?

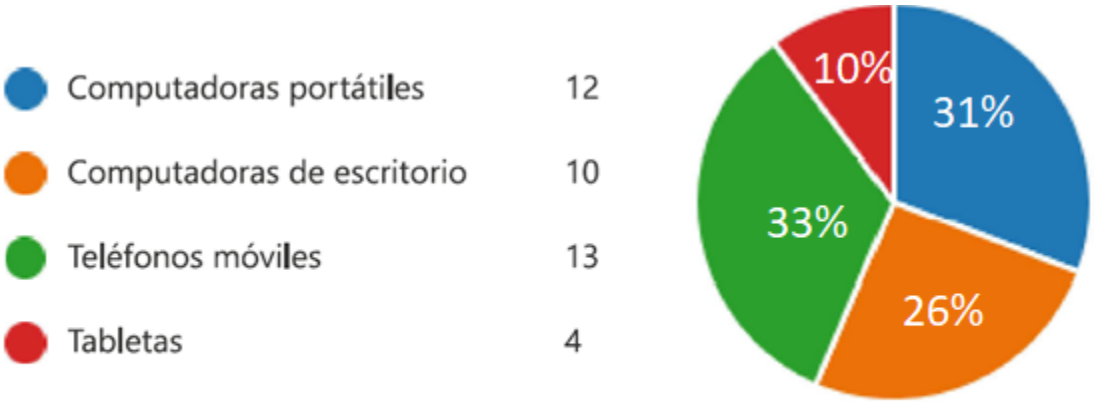


Figura 7: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Como se observa en la gráfica anterior, existe una gran diversidad de dispositivos que son actualmente utilizados en las pymes. Según los resultados de la encuesta, el más utilizado es el teléfono celular, seguido por las computadoras portátiles y de escritorio. El uso extendido de dispositivos móviles en el ambiente de trabajo significa que gran cantidad de información relacionada con la organización corre el riesgo de perderse o ser expuesta en caso de robo de los dispositivos electrónicos en el transporte cotidiano de los empleados, ya sea de la casa al trabajo o aquellos que tienen que estar constantemente desplazándose debido a las funciones de su puesto. Por esta razón, es de vital importancia que las organizaciones cuenten con políticas para el respaldo de información en dispositivos móviles, así como contar con funciones de borrado de información remota y uso de claves en los dispositivos, con el objetivo de minimizar el riesgo de robo de la información sensible de la empresa.

6. ¿Conoce si se tienen las siguientes funciones de seguridad activadas para los dispositivos de trabajo principales, siempre que sea posible?

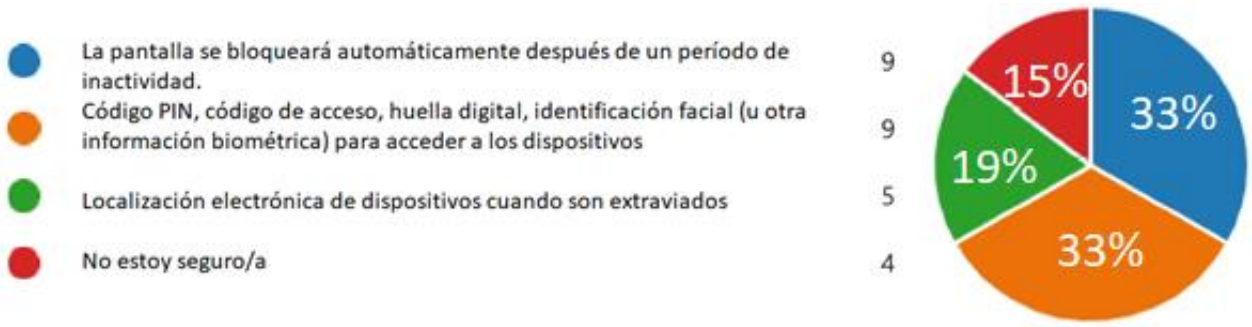


Figura 8: Gráfico de resultados de encuesta a pymes. Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

En relación con los controles de acceso para los dispositivos móviles, la mayoría de las pymes encuestadas cuentan con algún tipo de funcionalidad de acceso. Es muy importante contar con los controles básicos de acceso, pero no hay que perder de vista que se debe contar con otros niveles de protección. Cuando se trata de la seguridad de un dispositivo móvil, lo más importante que puede hacer el propietario es bloquear el dispositivo con un PIN único de cuatro dígitos. Usar un PIN o una contraseña única es lo más importante que debe hacer como usuario de un teléfono inteligente para proteger el dispositivo, los datos y su reputación.

Se puede afirmar que hoy en día los datos de los dispositivos móviles son más valiosos que los de la computadora de escritorio. En parte porque tiene la información más reciente. No es que una contraseña evite un robo rápido en la calle o la reventa ilegal del dispositivo, pero puede proteger los datos altamente personales en el teléfono, incluidos los mensajes privados, la información de contacto e incluso los datos bancarios móviles.

7. ¿Conoce si en las computadoras portátiles o de escritorio de su empresa se tiene activado el cortafuegos y habilitado el antivirus? El cortafuegos y el antivirus son funciones de seguridad que están integradas en Windows y macOS, y se pueden encontrar en la configuración de su computadora. Sin embargo, es posible que también haya optado por comprar un producto que proporcione estas o características adicionales, de un tercero.

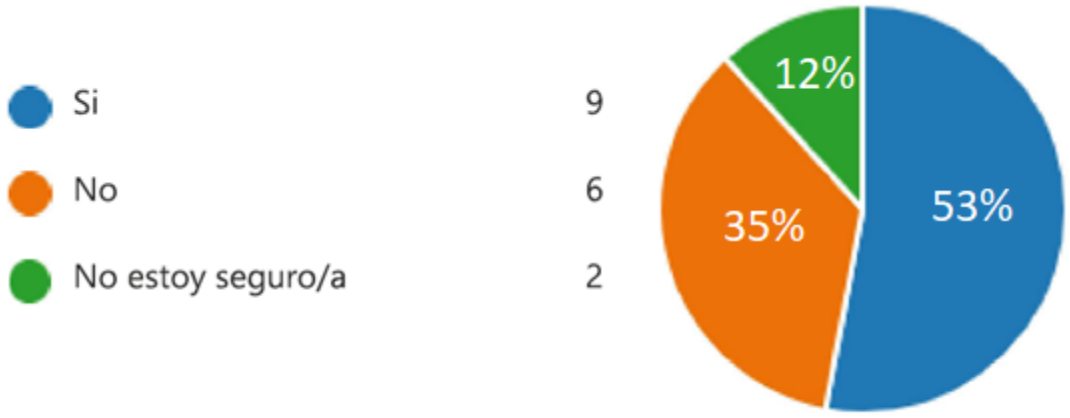


Figura 9: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Como se observa en el gráfico anterior, existe un alto porcentaje de jefaturas de pymes que no están seguras de contar con cortafuegos (35% + 12%). Esto pone en evidencia el desconocimiento de las jefaturas de las PYMES con respecto a la importancia de contar con elementos como cortafuegos que proporcionan un elemento básico de protección para los dispositivos presentes en las PYMES. El papel de los cortafuegos en la seguridad informática es crucial. La mayoría de las veces, evitan que los sistemas informáticos reciban correos electrónicos no deseados que a veces pueden contener troyanos y *malware*. Los cortafuegos personales operan en segundo plano e impiden que los códigos informáticos peligrosos penetren en el

sistema. Por lo tanto, protege la integridad del sistema. Es de vital importancia para las organizaciones mantener seguros sus datos y los de sus clientes. El cortafuegos proporciona una serie de funciones para garantizar la seguridad de los datos a gran escala con los que tratan las empresas.

8. ¿Conoce si se tienen políticas o directrices para que todos los dispositivos de trabajo principales cuenten con las últimas versiones de actualización del *software*? El *software* incluye: el sistema operativo del dispositivo (como Windows), cualquier aplicación en el dispositivo.

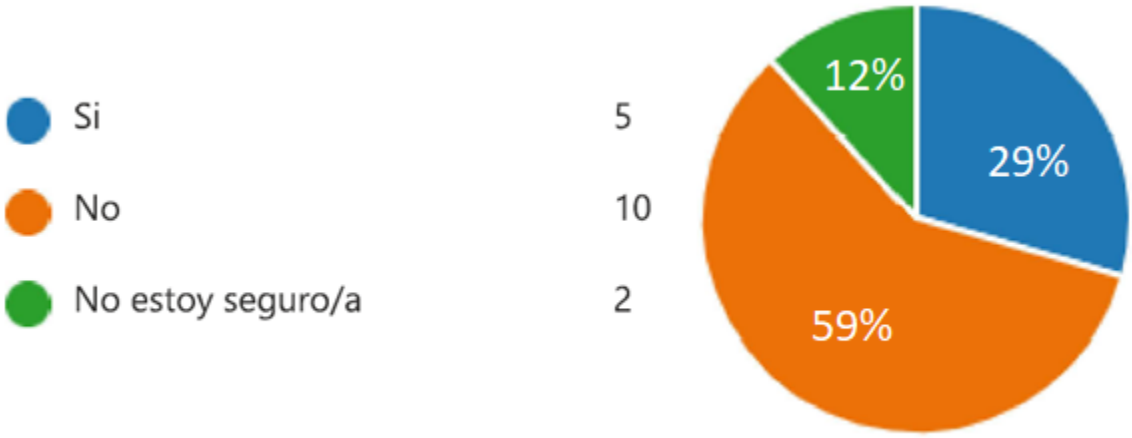


Figura 10: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Con respecto a esta pregunta, se puede observar que la mayoría de pymes encuestadas no cuentan con políticas para asegurarse de que el equipo cuenta con las últimas actualizaciones de *software*. Lo cual pone en gran peligro a estas organizaciones, ya que las actualizaciones de *software* son importantes, pues a menudo incluyen parches críticos para los agujeros de seguridad. De hecho, muchos de los ataques de *malware* más dañinos aprovechan las vulnerabilidades del *software* en aplicaciones comunes, como sistemas operativos y navegadores. Estos son grandes programas que requieren actualizaciones periódicas para mantenerse

seguros y estables. Es importante tomar conciencia de la importancia de estas y verlas como uno de los pasos más esenciales cuando se trata de proteger la información. Además de las correcciones de seguridad, las actualizaciones de *software* también pueden incluir funciones nuevas o mejoradas, o una mejor compatibilidad con diferentes dispositivos o aplicaciones. También pueden mejorar la estabilidad de su *software* y eliminar funciones obsoletas.

9. ¿Conoce si antes de instalar algún *software* en los principales dispositivos de trabajo se comprueba que sea de una fuente oficial? ¿Existen políticas o directrices en este sentido? Esto puede incluir verificar que sea de una marca conocida, realizar una búsqueda en la web o solo descargarlo de una tienda aprobada por el fabricante, como Apple App Store o Google Play.

Figura 11: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Como se observa en la gráfica anterior, el 35 % de las pymes encuestadas no tiene políticas con el objetivo de verificar la confiabilidad del *software* que se instala en los equipos de las pymes y un 24 % no está seguro. En total, las pequeñas

empresas que no tienen políticas o no están seguras hacen un 59 % de las pymes. Este número es muy alto y pone en evidencia el riesgo que corren.

El *software* gratuito es uno de los elementos más peligrosos con los que puede afectar seriamente a una organización. Esto no quiere decir que las ofertas de prueba o cualquier producto gratuito deba evitarse, si la empresa que los ofrece es legítima. Lo que se debe evitar son los paquetes de *software* gratuitos que se anuncian en internet. Estos *softwares* gratuitos de fuentes no confiables pueden contener *malware* que puede llegar a afectar seriamente un sistema. Antes de descargar una aplicación, es necesario asegurarse de que sea legítima. Muchas aplicaciones de fuentes no confiables contienen *malware* que, una vez instalado, puede robar información, instalar virus y afectar seriamente a una organización.

10. ¿Abre los correos electrónicos de los cuales desconoce quién es su remitente?

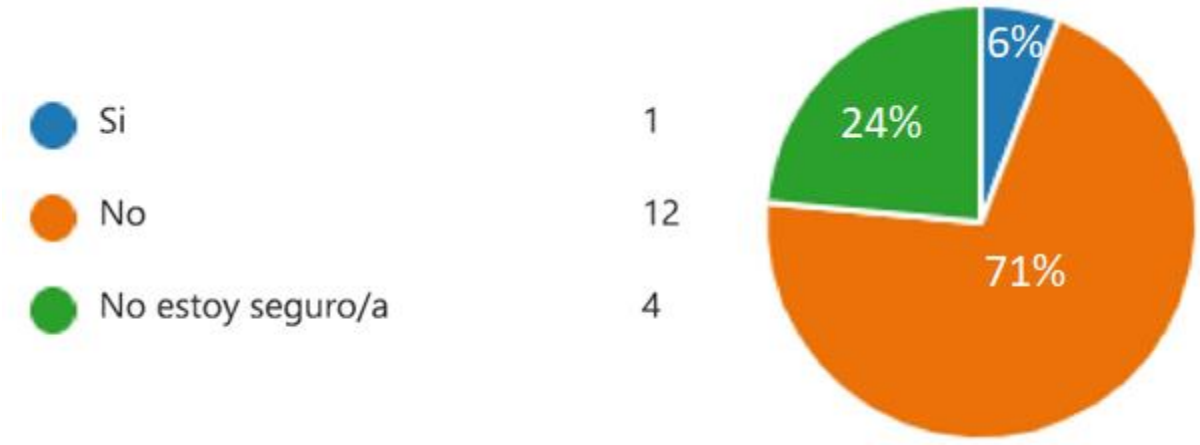


Figura 12: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Con relación al correo electrónico, se puede observar que la mayoría de los encuestados (71 %) muestra precaución al abrir correos electrónicos. Esta es una muy buena práctica, ya que los correos electrónicos no deseados suelen tener intenciones maliciosas y, por lo tanto, riesgos potenciales.

11. Seleccione la afirmación que considere más acertada:

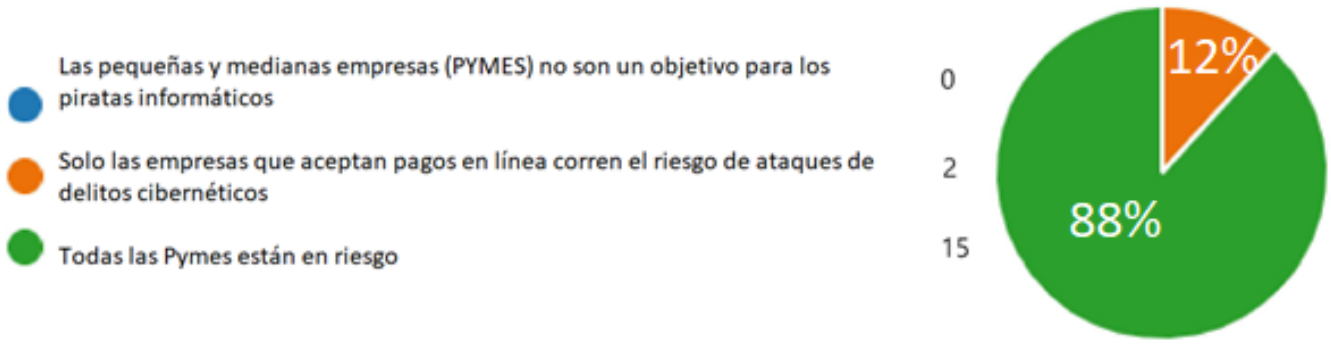


Figura 13: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Se puede observar que la mayoría de encuestados (88 %) concuerdan con que el riesgo de la ciberseguridad para las pymes es algo real. Sin embargo, como se ha podido observar en el análisis del diagnóstico, la mayoría de pymes encuestadas no cuenta con medidas activas para proteger su organización de los ataques, existiendo una clara contradicción entre lo importante que es la seguridad en oposición a las acciones que se toman por parte de las pymes, con el fin de reducir el riesgo de seguridad.

12. ¿En su empresa se realizan capacitaciones para el personal en temas de seguridad informática?

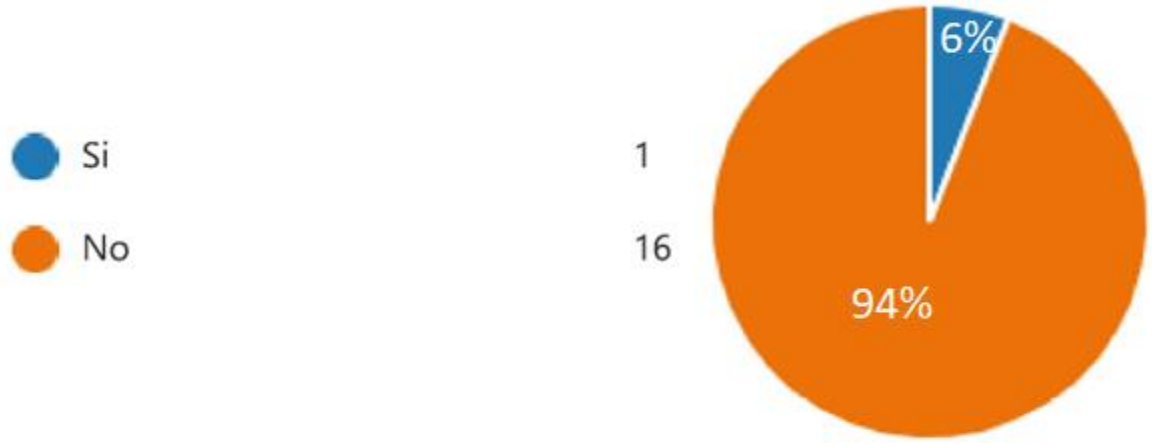


Figura 14: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Después de observar el gráfico relacionado a la respuesta anterior, queda muy claro que casi la totalidad de las pymes encuestadas (94 %) no ha incluido la capacitación en temas de ciberseguridad hacia sus colaboradores. Queda en evidencia la dicotomía que existe entre la importancia de la ciberseguridad por parte de los encuestados en oposición a las acciones que se toman en dirección de proteger la organización.

Hay muchas formas de reducir el potencial y el impacto de los ciberataques, pero requieren una acción y una planificación. Las empresas que ya han recibido formación sobre ciberseguridad están preparadas para afrontar un aumento continuo de las ciberamenazas. La educación juega un papel importante en impulsar el desarrollo de las capacidades organizacionales en materia de ciberseguridad.

El propósito principal del proceso de capacitación es crear un sentido de responsabilidad compartida y rendición de cuentas, para que la empresa esté a salvo de ataques por factores humanos. Los estudios han demostrado que la mayoría de los ataques digitales son intentos de explotar el factor humano a través de intentos de *phishing* muy creativos y atractivos, así como otros esfuerzos relacionados.

Los atacantes maliciosos buscan engañar a los usuarios. Por lo tanto, las personas pueden ser consideradas como el eslabón más débil en las defensas de ciberseguridad de cualquier organización. Esta es la razón por la que las personas son, en la mayoría de los casos, los principales objetivos de los ciberataques. Por estas razones resulta de vital importancia contar con un personal capacitado en materia de ciberseguridad.

13. ¿Conoce si en su empresa se mantiene un inventario de todos los equipos y *software* de TI?

Figura 15: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

La gráfica anterior indica que alrededor de la mitad de las pymes encuestadas no mantienen un inventario (35 %) o no están seguras (12 %). Esto representa 47 % del total de encuestados. Este porcentaje es muy alto y muestra que no es una práctica generalizada en las pymes el contar con un inventario actualizado de los equipos informáticos.

El inventario de activos constituye la primera parte de una cadena en el sistema de gestión de seguridad del sistema. No puede proteger lo que no sabe que tiene. Si no tiene un inventario de activos, se corre el riesgo de no saber qué está conectado al internet y, por ende, desconocer los riesgos de que ese dispositivo sea vulnerado, así como la organización.

La capacidad de rastrear y auditar el inventario es un requisito básico para la mayoría de los estándares de seguridad. Un inventario de activos es un elemento fundamental de su programa de seguridad. Puede ser tan simple como una hoja de cálculo de Excel que rastrea cada pieza de *hardware* (lo más importante, lo que está conectado a su red o almacena sus datos), la fecha en que se puso en servicio, el número de serie y una breve descripción.

14. ¿Conoce si su empresa cuenta con un plan de seguridad informática?

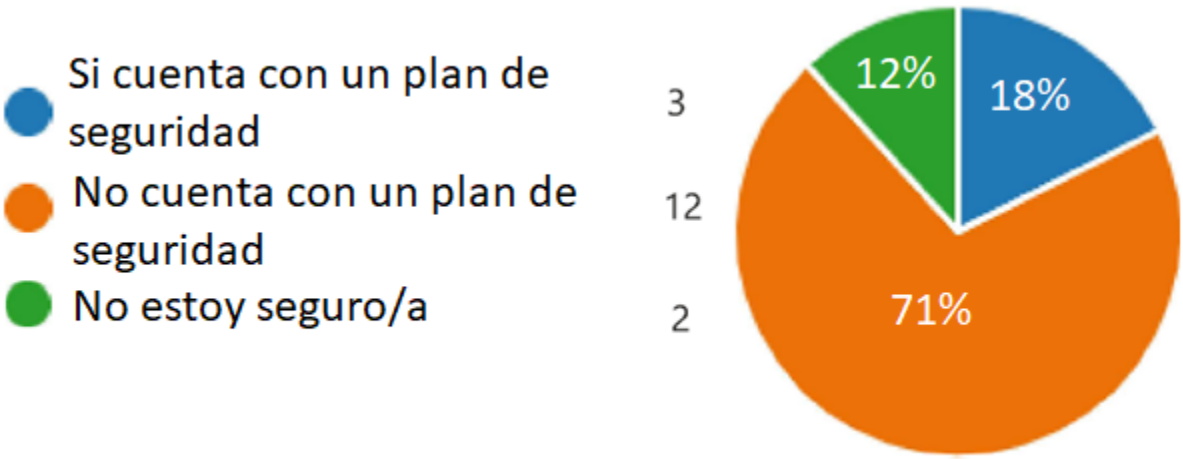


Figura 16: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Como se observa en el gráfico anterior, las pymes encuestadas no cuentan con un plan de seguridad (71 %) o no están seguras (12 %). Estos datos muestran que la

mayoría de las pymes encuestadas (83 %) se encuentran sin un plan de ciberseguridad, lo que evidencia que, a pesar de que las jefaturas son conscientes de que están en riesgo, como lo muestra la pregunta anterior, no existe una intención por enfocarse a concretar los esfuerzos de ciberseguridad en un plan. No solo es importante tener un plan de ciberseguridad para proteger la información interna de su organización, sino que también es importante para proteger la información del cliente.

15. Si su empresa no tiene un plan de seguridad informática, ¿cuál considera usted la razón principal?

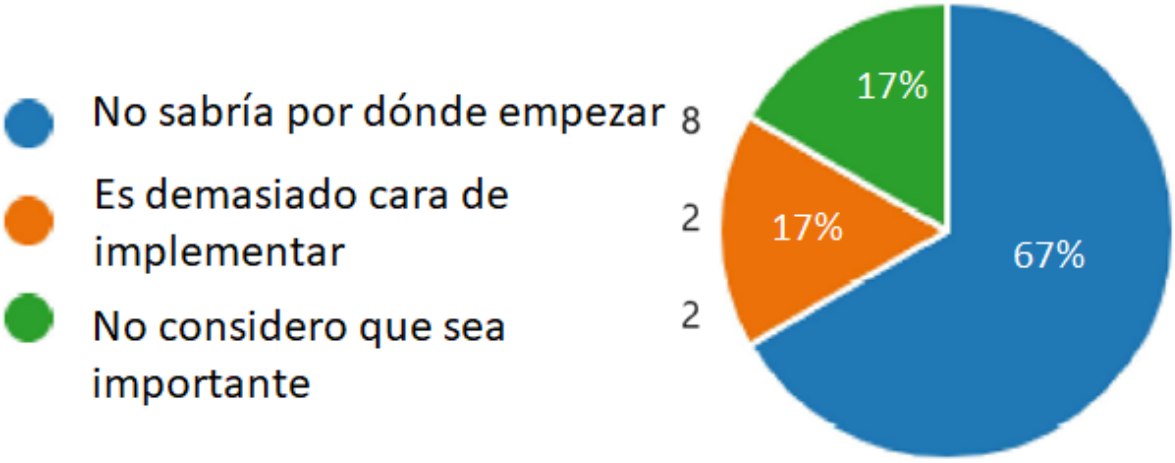


Figura 17: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Como muestra la pregunta anterior, la principal razón de las pymes encuestadas que no tienen un plan de seguridad informática es que consideran que no sabrían por dónde empezar (67 %). Se puede relacionar esta pregunta a la pregunta 12, la cual indica que el 88 % de las pequeñas empresas encuestadas considera que todas las pymes están en riesgo frente un ataque cibernético, pero el 71 % no cuenta con un plan de ciberseguridad (pregunta 15). Esto muestra que, aunque la mayoría de las pymes encuestadas está consciente del riesgo que corren, no han tomado acciones

para corregir esta situación debido al desconocimiento en el tema, que impide visualizar integralmente una estrategia de ciberseguridad que proteja a su organización. Esto indica que hay una gran área de mejora y de oportunidad de negocio que consiste en capacitar a las pymes en materia de seguridad informática.

4.4 Estudio de la Contraloría General de la República.

16. Instituciones del sector público costarricense que cuentan con seguridad de TI (en el contexto de la Contraloría General de la República, seguridad de TI corresponde a cualquier lugar donde esté la información, incluyendo hasta la información en formatos físicos)

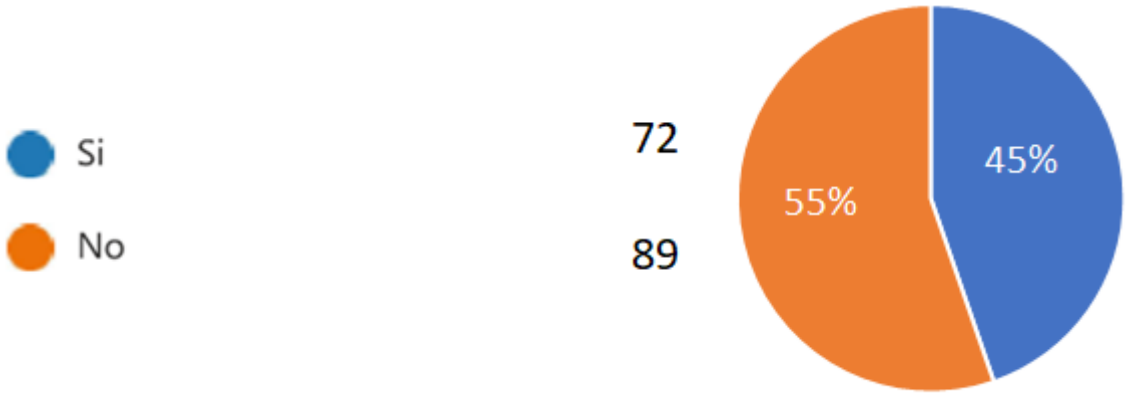


Figura 18: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Como se puede observar en el gráfico anterior, casi la mitad de las instituciones públicas no cuentan con seguridad de la información (45 %). Un porcentaje muy alto de instituciones públicas no contemplan la seguridad de la información en ningún aspecto, por lo que es necesario empezar a introducir los conceptos de la seguridad de la información en las instituciones públicas con el fin de cerrar brechas.

17. De las 72 instituciones del sector público costarricense que cuentan con seguridad de la información en TI (en el contexto de la Contraloría General de la República, seguridad de TI corresponde a cualquier lugar donde esté la información, incluyendo hasta la información en formatos físicos), los siguientes números reflejan cuáles instituciones cuentan con capacitación de seguridad de la información.

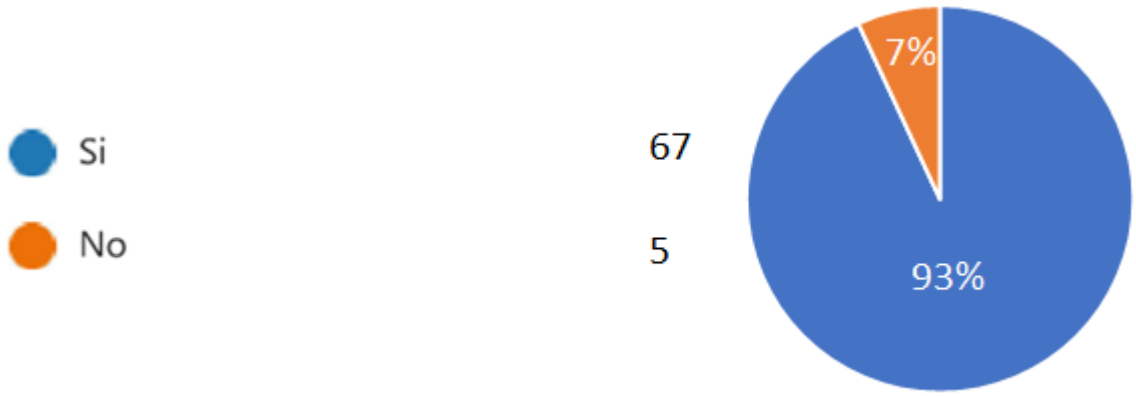


Figura 19: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

En el gráfico anterior, se observa que la mayoría de instituciones cuentan con seguridad de la información en TI, 93 % tiene capacitación en temas de seguridad de la información. Se puede observar que, entre las instituciones del Estado que sí cuentan con seguridad de TI, se he hecho conciencia sobre la importancia de la educación en temas de seguridad de la información. Esto contrasta con los números observados en las pymes, en las cuales solo un 6 % de los encuestados invierte en capacitación de seguridad de la información.

18. Instituciones del sector público costarricense que cuentan con ciberseguridad (en el contexto de la Contraloría General de la República, ciberseguridad es la información que se expone a internet).

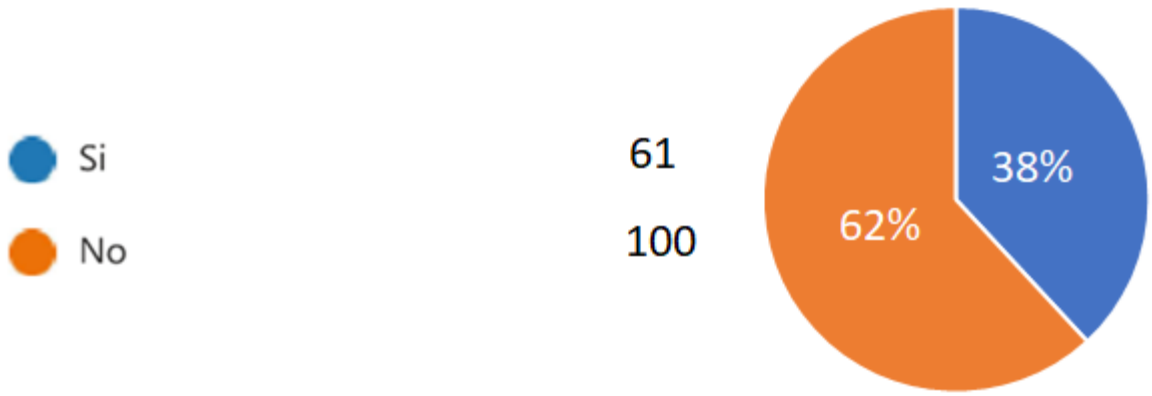


Figura 20: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

En esta gráfica se observa que el 62 % de las instituciones del Estado no cuentan con ciberseguridad. En el contexto de la Contraloría General de la República, se está hablando de la información que se expone al internet. Este porcentaje es muy elevado e indica que existe mucha información que no cuenta con ningún control de seguridad y que se encuentra expuesta al internet. Estas instituciones del Estado se encuentran en riesgo de recibir un ataque informático y que su información sea vulnerada. Por lo que es necesario que se pueda aumentar el número de instituciones públicas que cuenten con ciberseguridad.

19. De las 61 instituciones del sector público costarricense que cuentan con capacitación en ciberseguridad (en el contexto de la Contraloría General de la República, ciberseguridad es la información que se expone a internet), los siguientes números reflejan cuáles instituciones cuentan con capacitación en ciberseguridad.

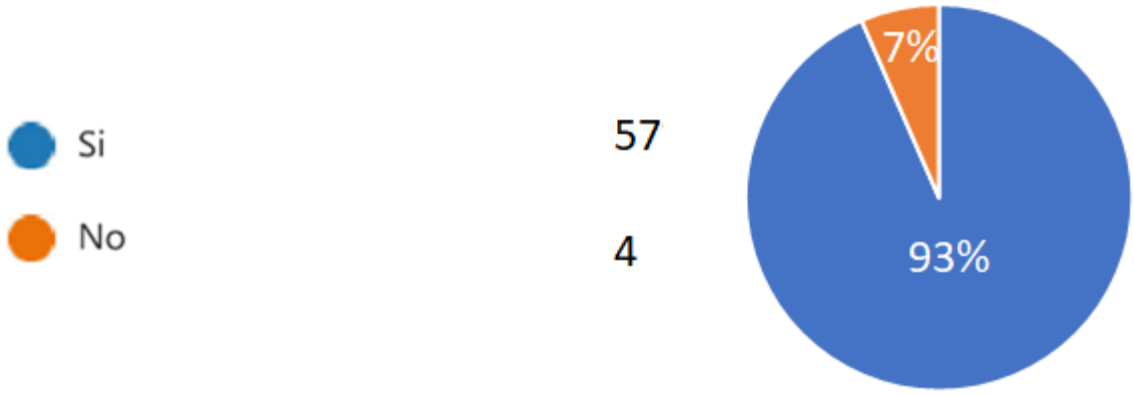


Figura 21: Gráfico de resultados de encuesta a pymes Fuente: elaboración propia a partir del cuestionario aplicado a dueños de pymes en Costa Rica.

Se puede observar el alto porcentaje (93 %) de instituciones del Estado que cuentan con capacitación en temas de ciberseguridad. Sin embargo, estos números contrastan con la pregunta anterior, en la que solo el 38 % de las instituciones del Estado cuentan con ciberseguridad. Se puede observar un interés por parte de estas instituciones del Estado que ya cuentan con ciberseguridad, en las que sus colaboradores estén capacitados en dicho tema.

Capítulo 5. Propuesta de solución

El presente proyecto consiste en analizar, diseñar y proponer una guía de ciberseguridad para que pueda ser utilizada por las pymes e instituciones del sector público costarricense. El manual se basó en los controles de la ISO 27001. Se tomaron los controles que son indispensables para iniciar con lineamientos en una organización pequeña, debido a que este manual tiene como objetivo crear conciencia de la importancia de la seguridad de la información. Como se observó en el análisis del diagnóstico, la principal razón por la que las pymes encuestadas, aunque consideraban que su negocio está en riesgo con respecto a la seguridad de la

información, no han tomado acción, es porque no sabrían por dónde empezar. Este manual pretende ser ese primer paso que se puede tomar para que sea el inicio de una cultura de la ciberseguridad en la organización.

5.1 Etapa de diseño

El Manual de Ciberseguridad contempla tres partes. La primera parte es de educación en conceptos de seguridad de la información. La segunda parte incluye los lineamientos técnicos que una organización pequeña debe velar por tener, con el objetivo de poseer bases de ciberseguridad que luego puedan ir aumentando. La tercera parte cuenta con un quiz de ciberseguridad que se puede hacer luego de haber leído la primera parte de conceptos de seguridad. Este quiz tiene como objetivo hacer una comprobación del conocimiento adquirido tanto por los líderes de la organización como por todos los colaboradores de esta.

5.2 Guía de conceptos básicos de ciberseguridad (Anexo 2)

La primera parte del manual cumple dos propósitos: el primero es educar al dueño de la pyme o el jerarca de la institución del sector público en conceptos básicos de ciberseguridad. También puede utilizarse como material didáctico para ser distribuido entre todos los colaboradores de la organización, con el fin de promover una cultura de la seguridad de la información.

5.3 Lineamientos técnicos (Anexo 3)

La segunda parte del manual contiene lineamientos técnicos básicos que deben ser tomados en cuenta con el fin de que la organización pueda empezar a tener bases sólidas en materia de ciberseguridad. El manual brinda una descripción general del lineamiento que se debe implementar, así como el porqué de este. Esto tiene como

fin ayudar a crear conciencia de la importancia de estos lineamientos y que no se están proponiendo sin ninguna utilidad práctica.

5.4 Quiz de ciberseguridad. ¿Qué tanto sabe usted de conceptos de ciberseguridad? (Anexo 4)

La tercera parte del manual cuenta con un quiz de comprobación de aprendizaje. Contiene los conceptos que se vieron en la primera parte del manual referente a los conceptos básicos de ciberseguridad. Este quiz puede ser realizado por los colaboradores de la organización antes de leer la Guía de Conceptos Básicos de Ciberseguridad, con el fin de evaluar los conocimientos previos en materia de seguridad de la información. Luego de leer la Guía, se puede realizar el quiz nuevamente con el objetivo de evaluar que los conceptos fueran aprendidos por los colaboradores.

Capítulo 6. Conclusiones y recomendaciones

Después del desarrollo del presente trabajo de investigación, se puede concluir que en las pymes de Costa Rica existe una conciencia de que están en riesgo en temas de seguridad de la información, pero el principal motivo por el que no se toma acción es porque existe un desconocimiento en el tema que genera un sentimiento abrumador de impotencia ante el mundo de la ciberseguridad. Por ende, existe una gran área de trabajo con respecto a la capacitación en materia de aspectos relacionados con la ciberseguridad, lo cual inclusive puede ser una oportunidad de negocio, ya que los líderes de las pymes están conscientes del riesgo, por lo que están abiertos a recibir ayuda en relación con temas de capacitación, así como de consultoría.

Es importante que el Estado costarricense se involucre en el proceso de creación de una cultura de seguridad de la información. El Centro Nacional de Seguridad Cibernética (NCSC) del Gobierno del Reino Unido es un excelente ejemplo de cómo el gobierno está involucrado en la educación y concientización de las organizaciones de todos los tamaños y también del ciudadano común. El programa Cyber Aware es un modelo que se puede adoptar por el gobierno costarricense, ya que en la investigación realizada no se encontró que existieran programas concretos que apoyen el proceso de alfabetización digital en la población, así como la concientización en temas de ciberseguridad.

En relación con las instituciones del sector público costarricense, se puede observar que la cultura organizacional en temas de ciberseguridad no se encuentra extendida uniformemente por todas las organizaciones, a pesar de que ha existido desde el 2007 la Norma Técnica para la Gestión y el Control de las Tecnologías de Información que recientemente fue derogada. Esta norma de cumplimiento obligatorio

por parte de las instituciones del Estado, que incluye lineamientos en temas de seguridad de la información, no fue suficiente para crear una cultura de seguridad de la información en todas las instituciones del Estado.

Es importante reconocer que el primer paso para el cambio cultural, tanto en las pymes como en las instituciones del sector público costarricense en materia de seguridad de la información, es la educación y concientización en todas las áreas de la entidad. Empezando por las jerarquías y continuando con todos los colaboradores. Este estudio tiene como objetivo crear conciencia acerca de que, como país, hace falta mucho recorrido todavía para poder hablar de un “alfabetismo digital”. Las empresas que ya han recibido formación sobre ciberseguridad están mejor preparadas para afrontar un aumento continuo de las ciberamenazas. Lo importante es reconocer las áreas de mejora, romper con esta parálisis de acción, que es la principal razón por la que no hay avances hacia este objetivo de crear una cultura de la seguridad de la información en las organizaciones.

La educación juega un papel importante en impulsar el desarrollo de capacidades nacionales de ciberseguridad. Además, se necesita una sólida cooperación entre los sectores público y privado para garantizar el pleno intercambio de conocimientos. Todos deben trabajar juntos con el objetivo de fortalecer la configuración actual de la arquitectura de seguridad, para desarrollar y aplicar medidas de seguridad entre empresas y organizaciones, a fin de garantizar la resiliencia colectiva.

Referencias bibliográficas

Castro, Johnny. (2020). “Más de 200 Millones de Intentos de Ciberataques Afectaron a Costa Rica En 2020.” *Www.larepublica.net*, 17 Mar. 2021, www.larepublica.net/noticia/mas-de-200-millones-de-intentos-de-ciberataques-afectaron-a-costa-rica-en-2020. Recopilado el 31 de agosto de 2021

Castro, Johnny. (2020). “Ticos Acechados Por Hackers Que Buscan Robar Sus Cuentas Bancarias.” *Www.larepublica.net*, 28 May 2020, www.larepublica.net/noticia/ticos-acechados-por-hackers-que-buscan-robar-sus-cuentas-bancarias. Recopilado el 31 de agosto de 2021

Chacón Jiménez, Krisia. (2020). “AyA Sufre Una Vulnerabilidad En Sus Sistemas Informáticos Y Causa La Suspensión Temporal de Su Página Web.” *El Financiero*, 1 Aug. 2020, www.elfinancierocr.com/tecnologia/aya-sufre-una-vulnerabilidad-en-sus-sistemas/REIBMY3AYVFXRHJZ7EU5D6Y4VE/story/. Recopilado el 31 de agosto de 2021

“COBIT.” *Ciberseguridad*, ciberseguridad.com/normativa/espana/sgsi/cobit Recopilado el 31 de agosto de 2021

Cordero Pérez, Carlos. (2020). “Sitio de Box Correos Sigue Sin Operar Tras Ataque a Equipos Del Servicio Con Un ‘Ransomware’; Pérdidas Se Estiman En ¢50 Millones Inicialmente.” *El Financiero*, 5 Aug. 2020, www.elfinancierocr.com/tecnologia/sitio-de-box-correos-sigue-sin-operar-tras-ataque/TIOW7L52BJEI7NVLV4HSMIPKJU/story/. Recopilado el 31 de agosto de 2021

Cordero Pérez, Carlos. (2020). “Más de 51 Millones de Ataques de ’Hackers’ Durante La Pandemia En Costa Rica: Empresas Siguen Basando Su Estrategia de Seguridad En La Educación.” *El Financiero*, 30 Aug. 2020,

www.elfinancierocr.com/tecnologia/mas-de-51-millones-de-ataques-de-hackers-durante/AXLI7EOQQZD7RA6X5O5DJPFNAA/story/. Recopilado el 31 de agosto de 2021

"Create Your Cyber Action Plan." *Www.ncsc.gov.uk*, www.ncsc.gov.uk/cyberaware/actionplan. Recopilado el 31 de agosto de 2021

Durango, Juan Esteban. (2019) "La Importancia de Una Política de Seguridad de La Información | ISO 27001." *MDP Soluciones*, 24 July 2019, mdpsoluciones.com/la-importancia-de-una-politica-de-seguridad-de-la-informacion/. Recopilado el 31 de agosto de 2021

Edwards, John. (2012). *Small Business Information Security*. https://thescholarship.ecu.edu/bitstream/handle/10342/3889/Vail_ecu_0600M_10664.pdf?sequence=1&isAllowed=y, 2012. Recopilado el 31 de agosto de 2021

Fishman, Tiffany. (2018 "Elevating Cybersecurity on the Higher Education Leadership Agenda." *Deloitte Insights*, 22 Feb. 2018, www2.deloitte.com/us/en/insights/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html. Recopilado el 31 de agosto de 2021

Heier, Donald, Guy Garrett. *A Study of Small Business Information Security in Rural America*. https://www.una.edu/sobie/proc2014.pdf#page=31 Recopilado el 31 de agosto de 2021

"ISO 27001 - Seguridad de La Información: Norma ISO IEC 27001/27002." *Normas ISO*, www.normas-iso.com/iso-27001/. Recopilado el 31 de agosto de 2021

"ISO 27002 A6 Organización de La Seguridad de La Información." *ISO 27001*, normaiso27001.es/a6-organizacion-de-la-seguridad-de-la-informacion/. Recopilado el 31 de agosto de 2021

Janofsky, Adam. “Small Companies Are Least Prepared for Cyberattacks.” *Wall Street Journal*, 22 June 2020, www.wsj.com/articles/small-companies-are-least-prepared-for-cyberattacks-11592606067. Recopilado el 31 de agosto de 2021

Jiménez Castillo, Wilson. *Seguridad informática o de la información en pymes*. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4929/51183%20-%20Jim%C3%A9nez%20Castillo%20Wilson.pdf?sequence=1&isAllowed=y Recopilado el 31 de agosto de 2021

Juan Esteban Durango. “Regulación Comercio Electrónico En Costa Rica - Abogado Derecho Digital.” *GoLegal*, 25 May 2020, golegalcr.com/regulacion-comercio-electronico-en-costa-rica/. Recopilado el 31 de agosto de 2021

“Las Pymes, El Blanco Perfecto de Los Cibercriminales En La Nueva Normalidad.” *Noticias de Guanacaste Y Costa Rica. Heraldo de La Región Chorotega*, 17 Sept. 2020, www.periodicomensaje.com/otras/tecnologia/5548-las-pymes-el-blanco-perfecto-de-los-cibercriminales-en-la-nueva-normalidad. /. Recopilado el 31 de agosto de 2021

Little, Brian. “Small Business Security.” *Http://Www.cs.lewisu.edu/*, www.cs.lewisu.edu/mathcs/msisprojects/papers/SMBSecurity_BrianLittle.pdf.

Los CISOs ante la prueba extrema de resiliencia. Plan para emerger más fuerte Digital Trust Insights Pulse Survey Findings 2020 https://www.pwc.com/ia/es/publicaciones/assets/CISO-Survey-Interam%C3%A9ricas.pdf Recopilado el 31 de agosto de 2021

Nicole Keller “Getting Started.” *NIST*, 5 Feb. 2018, www.nist.gov/cyberframework/getting-started. Recopilado el 31 de agosto de 2021.

Pritchard, Stephen. “Navigating the Black Hole of Small Business Security.” *Infosecurity*, vol. 7, no. 5, Sept. 2010, pp. 18–21, 10.1016/s1754-4548(10)70085-1.

https://www.sciencedirect.com/science/article/abs/pii/S1754454810700851 Recopilado el 31 de agosto de 2021

TRUJILLO, CAMILA. Casos de estudio de cibercrimen para el mejoramiento de la seguridad informática en pymes y medianas empresas. https://repository.unad.edu.co/bitstream/handle/10596/30220/ctrujilloch.pdf?sequence=1&isAllowed=y , 2019. Recopilado el 31 de agosto de 2021

Ed Vaizey, Karen Bradley. "Cyber Security 'Myths' Putting a Third of SME Revenue at Risk." GOV.UK, 15 Feb. 2015, www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk. Recopilado el 31 de agosto de 2021

Víquez Alvarado, Jessica. "Medidas Tomadas Por Las Instituciones Ante La Derogativa de Las Normas Técnicas Para La Gestión Y Control de Las Tecnologías de Información." *Contraloría General de La República*, 3 Sept. 2021, cgrfiles.cgr.go.cr/publico/docs_cgr/2021/SIGYD_D/SIGYD_D_2021014759.pdf. Recopilado el 3 Sept. 2021

Anexos

Anexo 1. Imágenes de resultados de investigación

Figura 22: Resultado de la búsqueda intitle: “small business security”

Como resultado de la búsqueda anterior se obtienen 20 artículos.

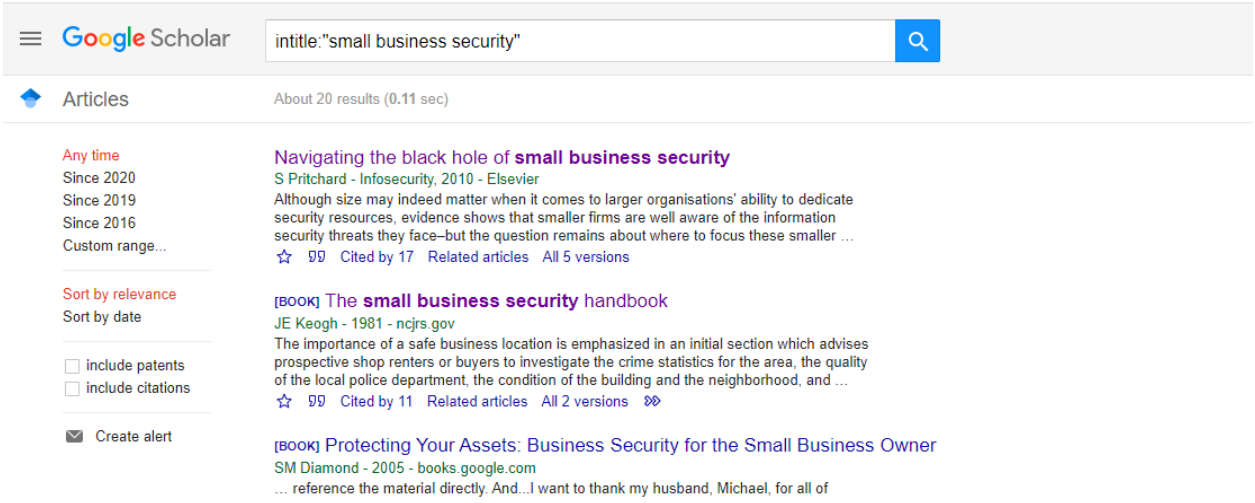


Figura 23: Resultado de búsqueda intitle “small business” + “security threats”

El resultado de búsqueda brinda 32 artículos.

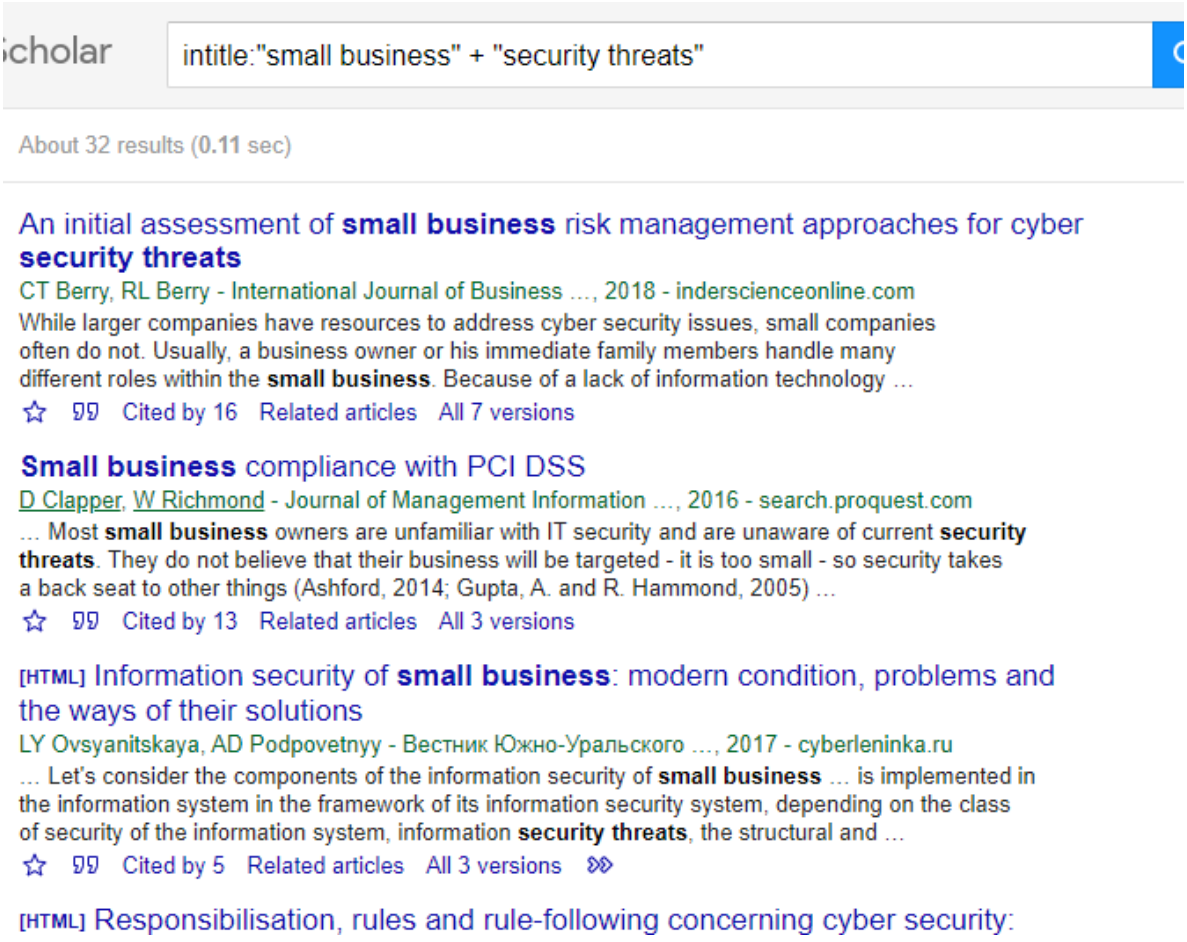


Figura 24: Resultado de búsqueda intitle:small business security” + “policies”

La búsqueda brinda 19 resultados.

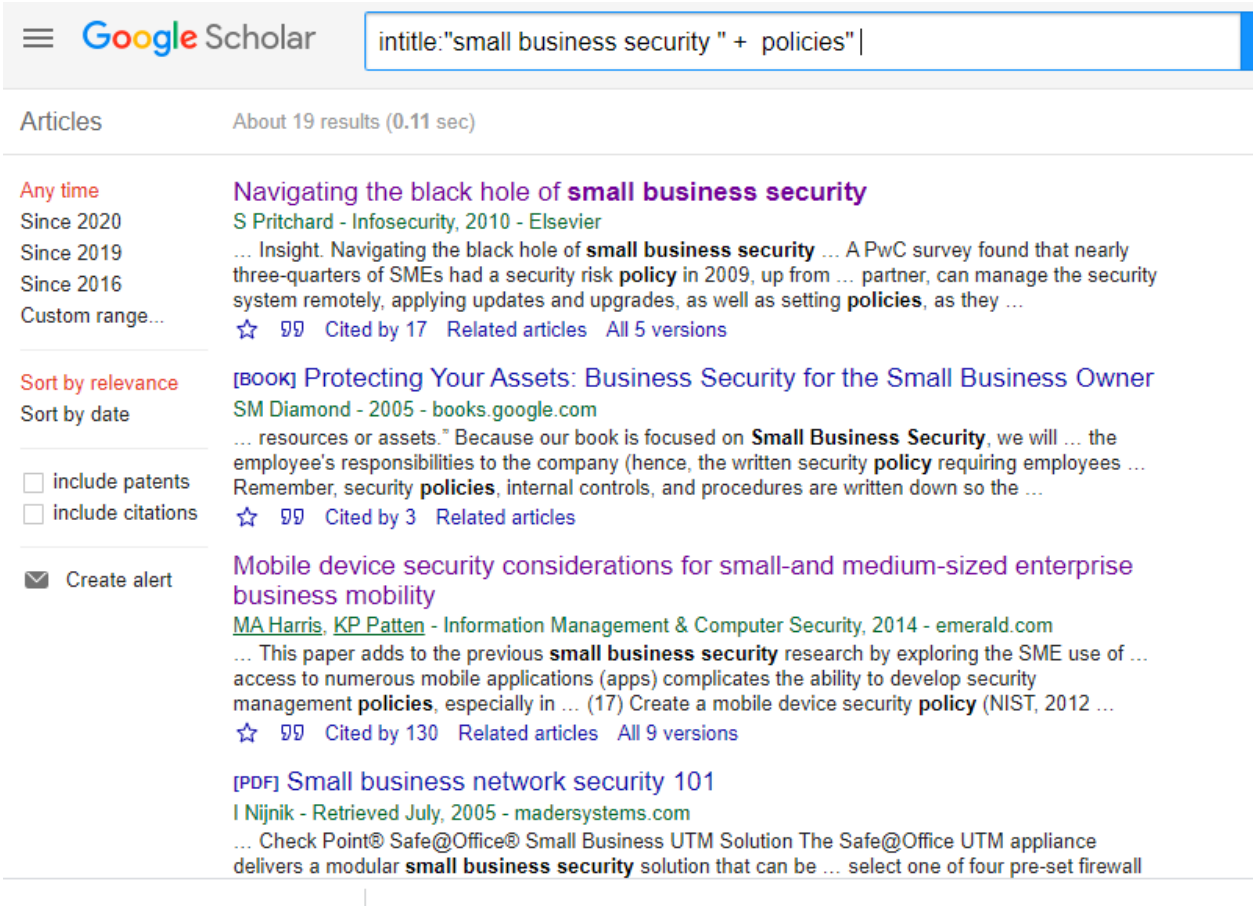


Figura 25: búsqueda: inline “pyme” + “seguridad informática

Resultados 422

Imagen de criterios de búsqueda

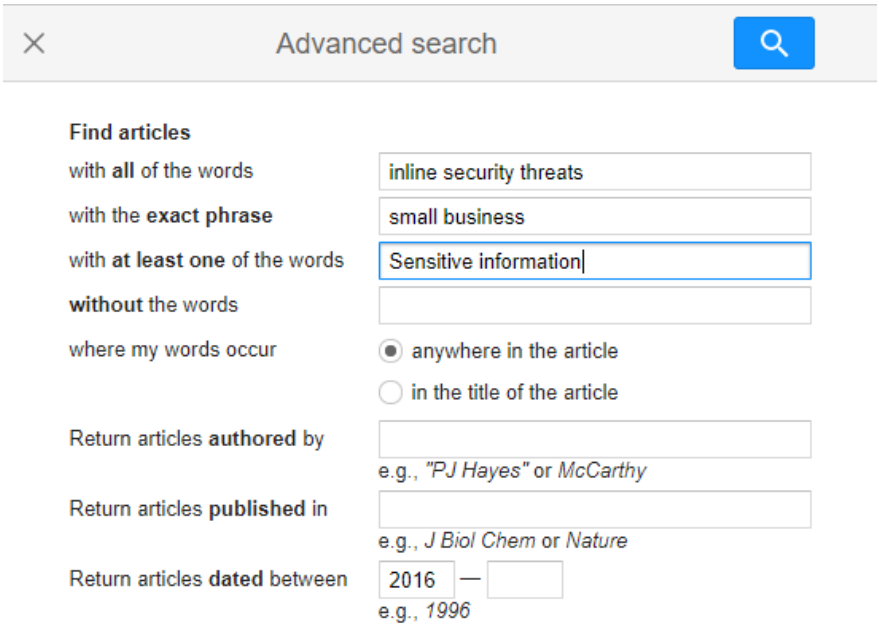


Figura 26: Resultado de búsqueda: artículo encontrado: Cybersecurity liability: How technically savvy can we expect small business owners to be

Anexo 2. Guía de conceptos básicos de ciberseguridad

Importancia de la ciberseguridad

Un reporte de la firma de ciberseguridad Fortinet, líder global en soluciones de ciberseguridad, indica que, en el primer semestre del 2020, se detectaron más de 51 millones de ataques informáticos contra sistemas y dispositivos institucionales, empresariales y personales en Costa Rica. El gerente de Fortinet para Costa Rica comenta lo siguiente: “Vemos una creciente actividad cibercriminal hacia objetivos en Costa Rica a medida que los hackers continúan lanzando métodos de ataque sofisticados dirigidos a víctimas desprevenidas, independientemente de su ubicación”.

El Instituto Costarricense de Acueductos y Alcantarillados y el servicio Box Correos, de Correos de Costa Rica, sufrieron caídas en sus plataformas, lo que imposibilitó la prestación de servicios durante un tiempo considerable. Esto debido a los ataques perpetrados por delincuentes conocidos como *hackers*, que sufrieron sus sistemas. La caída del sistema de Correos de Costa Rica en julio 2020 duró 15 días y la pérdida económica se estimó en más de 50 millones de colones. Desde el inicio de la pandemia del COVID-19 (primeros meses del 2020), los especialistas en ciberseguridad advirtieron que los *hackers* estaban intentando ingresar a los sistemas corporativos, aprovechando las vulnerabilidades en las redes domésticas de los empleados trasladados a teletrabajo.

La ciberseguridad se trata de proteger los equipos computarizados e información, de accesos no permitidos ni deseados, así como el cambio, robo o destrucción de información. Las buenas prácticas de ciberseguridad pueden mejorar la reputación de las empresas y abrirlas a nuevas oportunidades.

La mayoría de los ataques se pueden prevenir o detectar con prácticas básicas de seguridad para los colaboradores, procesos y sistemas de tecnologías de la información (TI). Estas prácticas de seguridad son tan importantes como ponerle seguro a las puertas o depositar el dinero en la caja fuerte. Se debe manejar la seguridad en línea de la misma manera como se protegerían otros aspectos de su negocio.

Entender de riesgos. ¿Qué está en riesgo?

- En las empresas está en juego el dinero, la información, la reputación, el equipo de TI y los servicios basados en TI. La información es un activo que puede tomar muchas formas: listas de clientes, bases de datos de clientes, los detalles financieros de la empresa y de los clientes, acuerdos que se están haciendo o considerando, información de precios, diseños de productos o procesos de fabricación. Existe un riesgo para los servicios e información de TI donde sea que estén almacenados, ya sea en los propios sistemas y dispositivos, o en sistemas alojados en infraestructura de terceros.

¿Quién puede ser una amenaza a estos activos?

- Empleados actuales y antiguos o personas con las que se hace negocio. Pueden comprometer la información por accidente o por negligencia o con un fin malicioso.
- Criminales. Quieren robar, comprometer la información valiosa o parar el negocio por múltiples razones, desde el propio beneficio financiero de los atacantes hasta que no les gusta lo que hace la empresa.
- Competidores. Quieren ganar una ventaja económica.

¿Qué forma tomaría un ataque?

- Robo o uso no autorizado de las computadoras, tabletas o móviles.
- Ataque remoto al sistema de TI o al sitio web.
- Ganar acceso a la información a través del personal.

¿Qué impacto podría tener un ataque?

- Pérdidas financieras derivadas del robo de información, detalles financieros y de información bancaria.
- Pérdidas financieras por el impedimento de hacer negocios, especialmente si se depende de hacer negocios en línea.
- Pérdida de negocios por mala publicidad y daño en la reputación base del cliente.
- Costos de arreglar los sistemas afectados y ponerlos en funcionamiento nuevamente.
- Costos de multas si la información personal de una persona es perdida o comprometida.
- Daño a otras compañías con las que se está conectado.
- Un solo ataque podría dañar seriamente al negocio

Phishing. ¿Qué es phishing?

El *phishing* es un intento que se realiza generalmente a través del correo electrónico para robar información personal. Los cibercriminales están tratando de hacer que se les entregue datos de tarjetas de crédito, que se brinde una contraseña o se entregue algo personal. Todos han recibido correos no deseados en algún momento y se cree que se pueden identificar fácilmente. Sin embargo, hay ataques inteligentes de

phishing. Parece que provienen del banco, la municipalidad, del gobierno, de las empresas proveedoras de servicios básicos. Parecen correos electrónicos legítimos, pero en realidad son ataques de *phishing* que están tratando de engañar para que se haga clic en un enlace sospechoso o que se proporcione información personal.

¿Cómo detectar un ataque de phishing?

No hay que caer en las redes del *phishing* respondiendo a preguntas, como las que aparecen a continuación, cuando se recibe un correo electrónico o un mensaje de texto inusual, especialmente si contiene enlaces o documentos adjuntos:

- ¿Conoce al remitente?
- ¿Esperaba recibir este mensaje?
- ¿Es demasiado bueno o muy poco probable para ser verdad?
- ¿El remitente pide que se tome algún tipo de medida, por ejemplo, introducir una contraseña?
- ¿Una ventana emergente o una página web sospechosa pide que se actúe o proporcione información?
- En ese contexto, ¿tiene sentido este mensaje?
- Nunca se va a pedir su contraseña o su información personal por correo.
- No se deben abrir correos que tienen documentos adjuntos si se desconoce quién los envía.
- Elimine correos sospechosos.

Ingeniería social

La ingeniería social es cuando una persona intenta manipular a alguien para obtener información o acceder a un área no autorizada. Pueden ser contraseñas,

nombres de usuario o información con privilegios. Es mucho más fácil explotar la confianza de alguien que *hackear* una computadora. Esta técnica explota la confianza humana natural. El delincuente pretende ser alguien o una entidad en la que confía. La ingeniería social suele producirse a través del correo electrónico, pero puede llevarse a cabo por otros medios como por teléfono.

Un cibercriminal puede suplantar la identidad de casi cualquier persona, incluso alguien que trabaja en la empresa. Los atacantes saben que, si hablan elegantemente y utilizan siglas de la compañía, es más probable que se confíe en ellos y se les dé lo que desean.

El robo de identidad es una técnica fraudulenta empleada por ciberdelincuentes utilizando internet. Los ataques de robo de identidad usan varias formas y la más común es el correo electrónico. Los ataques están aumentando y se están volviendo más sofisticados, haciéndose más difíciles de detectar.

Por su parte, el robo de identidad es un fraude que usa comunicaciones falsas para robar información o instalar programas malintencionados en los dispositivos corporativos. Luego los ladrones de identidad usan esa información para cometer robo de identidad, generalmente por una ganancia financiera, pero a veces para fines políticos. Los fraudes por robo de identidad son una amenaza real. Además de la pérdida financiera directa hay que considerar los costos para restaurar las reputaciones dañadas, reparar las violaciones de seguridad y volver a ganar la confianza del cliente.

¿Cómo funciona el robo de identidad?

El ladrón de identidad envía un correo masivo falso pero convincente, que parece venir de una fuente confiable. Los ejemplos incluyen correos de instituciones financieras, amigos y colegas, minoristas en línea y sitios de redes sociales.

Después de enviar un mensaje falso, los ladrones de identidad esperan para ver quién cae en la trampa incitando a la víctima a que confirme su nombre de usuario, contraseña, número de cuenta bancaria u otra información personal. Generalmente el robo de identidad requiere interacción humana para que funcione, ya que cuando se hace clic en un enlace, se descarga e instala *software* malicioso oculto difícil de detectar y eliminar. Un correo de robo de identidad puede parecer inofensivo, pero solo se necesita un clic que sea el inicio de un ataque que perjudique gravemente a la organización.

Contraseñas

Es muy común que las personas guarden sus contraseñas alrededor de su escritorio. Los lugares más comunes para mantener las contraseñas son el monitor, esquina inferior izquierda o derecha, nota adhesiva debajo del teclado o el cajón superior del escritorio. Muchas organizaciones almacenan las contraseñas en un documento de Word o en algún tipo de hoja de Excel. Esto es una mala práctica.

Las contraseñas comprometidas permiten a otros enviar correos malintencionados, acceder a información o recursos, cometer fraude o delitos, haciéndose pasar por la víctima. Nunca se debe compartir la contraseña verbalmente o de otro modo. Las contraseñas deben ser recordadas en vez de escribirlas. Si es

necesario guardarlas, se pueden escribir al revés, o agregando caracteres en medio para confundir a los usuarios no autorizados.

La mayoría de las personas usa solo una o dos contraseñas para todas las cuentas de las aplicaciones. Reutilizar contraseñas para cuentas importantes es peligroso. Si alguien obtiene la contraseña para una cuenta, podría acceder al correo electrónico, dirección e incluso al dinero guardado en cuentas electrónicas.

La fuerza de la contraseña proviene de la longitud, la fuerza es igual a la longitud y la longitud es mucho mejor que la complejidad. Las contraseñas largas son más seguras. Estas deben tener al menos 12 caracteres.

Los siguientes consejos pueden ayudar a crear contraseñas más largas que sean más fáciles de recordar: usar la letra de una canción o un poema, una cita significativa de una película o un discurso, una frase de un libro, una serie de palabras que son significativas únicamente para su dueño. Se debe evitar elegir contraseñas que puedan adivinarse por personas que conocen al usuario o que puedan buscar información de fácil acceso (como el perfil de redes sociales). Es recomendable usar una diferente para cada una de las cuentas importantes, como el correo electrónico y la banca en línea. 12345678 es una de las contraseñas más comunes. Cuando un atacante intenta ingresar a un sistema, primero usará estas comunes para ver si puede entrar, por lo que no se deben usar contraseñas comunes.

Un impedimento para conservar contraseñas seguras es tener muchas que recordar, pues no es fácil realizar un seguimiento de todas. Una solución para esto es un *software* llamado administrador de contraseñas. El principal beneficio de usar un administrador de contraseñas para aumentar la seguridad cibernética es que no se necesita tener una buena memoria. Solamente es necesario tener una contraseña

maestra para ingresar al administrador donde están seguras todas las demás. Se puede imaginar que un administrador de contraseñas es como una caja fuerte. Solo necesita una clave para ingresar a la caja fuerte donde se pueden guardar todos los objetos valiosos. En este ejemplo, los objetos valiosos a guardar son las contraseñas. Los administradores de contraseñas se encargan de crear contraseñas únicas y seguras. Esta es una de las mejores formas para mantenerlas seguras.

Navegar en Internet de forma segura

Cuando se navega en Internet se quiere estar seguro de que se tiene una conexión segura. ¿Qué es una conexión segura? Las páginas en internet se categorizan en dos tipos: HTTP y HTTPS. Esto se puede ver en la barra de direcciones del navegador. Esta es la primera parte de la dirección web del sitio que se quiere visitar. La S al final de HTTPS es sinónimo de seguridad. Siempre se quiere una conexión segura. Si se está en un sitio web que requiere que se inicie sesión como cualquiera de los sitios web de redes sociales, es necesario que sea una página de tipo HTTPS. También se quiere tener una conexión segura cuando se ingresa al banco y se tiene que ingresar la información de la tarjeta de crédito; de igual manera, cuando se está comprando por internet, se debe asegurar que se esté usando https. Si no se usa https, no se debe ingresar información personal como el nombre de usuario, contraseña, información de tarjeta de crédito o cualquier dato sensible.

Muchos sitios web en Internet todavía usan HTTP. Se puede navegar en una página HTTP, pero si no se ingresa ninguna contraseña o información de tarjeta de crédito. Leer las noticias, buscar una receta o leer un blog son ejemplos de cuando se puede navegar en un sitio HTTP. En estos casos, no es una preocupación demasiado grande porque no se está enviando información a ese sitio web. Lo más

adecuado es que todas las páginas fueran HTTPS para que la navegación sea privada.

De igual manera, hay que tener cuidado cuando se conecta al internet inalámbrico gratuito o público como en un centro comercial o un aeropuerto. No se debe ingresar a un sitio web de un banco o a ningún lugar donde se tenga que poner las contraseñas, si se está conectado en una red pública.

Dispositivos personales

Los dispositivos personales como celulares tabletas o relojes inteligentes contienen información personal, que no se quiere que se haga pública. Se usa el celular para tomar fotografías, se hace descarga de archivos, estos dispositivos mantienen mucha información personal. Perder el celular o ser víctima de robo es algo muy incómodo. También existen riesgos de seguridad en estos casos. La persona que encuentre el teléfono ahora podría enviar correos electrónicos en nombre de la víctima. Se podrían revisar todos esos documentos confidenciales. Se podrían encontrar mucha información personal. Si se tenían datos de trabajo en el teléfono eso es una fuga de datos, porque otra persona tiene acceso al dispositivo y ahora tiene acceso a documentos de trabajo de la organización.

¿Cómo se puede proteger un dispositivo personal, ya sea un teléfono, tableta o computadora portátil? Mucho de esto podría evitarse si se tuviera una contraseña segura para ingresar al teléfono y tenerlo siempre bloqueado, al igual que las computadoras portátiles. Estos equipos se deben configurar para que se bloqueen después de un cierto período de tiempo, después de tal vez 60 segundos, que se apague la pantalla y bloquee el dispositivo. Se debe asegurar que esté protegido con una contraseña, por lo que cada dispositivo portátil debe tener una.

Las tiendas para iPhone y Android pueden contener programas maliciosos o una gran cantidad de correo no deseado o anuncios. Hay que tener mucho cuidado con las aplicaciones que se descargan al dispositivo, aunque sean de una tienda oficial. Si se tiene información confidencial en el teléfono, hay que preguntarse si realmente se necesitan esos documentos allí, como documentos de trabajo que pueden descargar, tal vez se esté viajando y se quiera revisar algunos mientras tanto. Una vez que tenga esos documentos, se debe recordar que ahora están almacenados en el dispositivo y se tiene información del trabajo en el teléfono personal. Si se ha terminado con estos, es mejor eliminarlos.

Cuando se compra un dispositivo nuevo, se debe asegurar que la información sensible no quede en el celular antiguo, si es que se quiere vender o darlo a alguien más. Todos los dispositivos tienen la opción de limpiar el teléfono por completo. Hacer esto evita que la información personal quede disponible para el nuevo dueño del dispositivo.

Elementos básicos de seguridad

Los siguientes son lineamientos básicos para mantener seguros los sistemas. Si se tienen dudas de que estos puntos se cumplen, se debe consultar con el encargado de TI de la organización. Si alguno de estos puntos no se cumple, se debe tomar acciones para garantizar la seguridad de la información.

- Asegurarse de instalar las actualizaciones de *software* de computadoras, tabletas y celulares.
- Usar un antivirus en la computadora, tableta y el celular.
- Entrenar a los colaboradores sobre la importancia de la ciberseguridad.

- Realizar copias de seguridad de los archivos periódicamente: garantizar que se realice con regularidad una copia de seguridad de los archivos y las carpetas esenciales para los negocios es una parte importante de la protección contra programas maliciosos. Si una estación de trabajo resulta infectada, es posible que los archivos de seguridad sean la única forma de recuperar los datos almacenados en ella. Se pueden tener diferentes formas de realizar respaldos:
    - Unidades de red compartidas
    - Discos duros externos
    - *Software* de seguridad para realizar respaldos
- Proteger las áreas de trabajo: un área segura minimiza el riesgo de pérdida, robo y destrucción de los documentos impresos, los archivos electrónicos y el equipo.
- Mantener limpio el escritorio, guardar bajo llave los documentos y el equipo.
- Saber cuándo y dónde desechar los documentos que ya no sean necesarios.
- Bloquear las pantallas de las computadoras siempre que se aleje del escritorio y asegurarse de que todos los documentos impresos estén seguros.
- Recoger de inmediato los documentos luego de imprimirlos o copiarlos.
- Mantener los documentos sensibles en lugares seguros.
- No dejar las contraseñas escritas en la oficina.
- No compartir las contraseñas con nadie.
- Cambiar de contraseñas periódicamente (cada 30 a 60 días).
- Usar un administrador de contraseñas.
- Usar contraseñas de más de 12 caracteres.
- No usar contraseñas comunes como 12345678 o 123clave.

- Usar una contraseña diferente para cada una de las cuentas importantes, como el correo electrónico y banca en línea.

Anexo 3. Lineamientos técnicos

Documentar política de seguridad de información

Se debe contar con un documento de política de seguridad de la información. Se puede tomar este manual como base e ir agregando políticas conforme se identifiquen las necesidades. Independientemente del tamaño, es importante que la organización cuente con políticas de seguridad de TI documentadas, para ayudar a proteger los datos de la organización y otros activos valiosos.

La Política de Seguridad de la Información debe contemplar directivas y controles para asegurar características tan sencillas como la longitud y dificultad de contraseñas, el respaldo periódico de la información, el uso de dispositivos no seguros dentro de la organización (equipos móviles personales sin protección o antivirus).

Revisión de las políticas de seguridad de la información.

Es importante revisar las políticas semestral o anualmente, con el fin de hacerle ajustes según sea necesario. También se debe comunicar las políticas de seguridad de la información a los colaboradores periódicamente, para garantizar que estén al tanto de estas, así como familiarizar a colaboradores nuevos que no tienen conocimiento de ellas.

Asignación de responsabilidades de la seguridad de la información.

Asignar el rol y responsabilidades de la seguridad de la información con el fin de velar por el cumplimento de las políticas, así como cualquier mejora que haya que hacerle. Este rol se puede asignar al encargado de TI o a la empresa proveedora de servicios de TI. De no existir encargado de TI o empresa proveedora de servicios de

TI, se debe procurar capacitar a algún colaborador de confianza en temas de seguridad de la información. El encargado de la seguridad de la información debe identificar la sensible con el fin de protegerla. Esta es información cuya divulgación haría que la entidad se viera expuesta a demandas o a pérdidas de clientes.

Acuerdos de confidencialidad

En caso de que un tercero tenga acceso a la información de la empresa, se debe tener un acuerdo de confidencialidad con el fin de evitar la divulgación de la información sensible de la empresa de parte del tercero.

Inventarios de activos

Mantener una lista de activos como computadoras, tabletas y celulares, donde se tenga información de la empresa. Se debe actualizar esta lista de manera periódica, puede ser semestral o anualmente. Es necesario que esta lista cuente con el responsable de cada activo. Por ejemplo, en caso de que se haya identificado una computadora, se debe indicar cuál colaborador es el responsable de ese activo.

Uso aceptable de los activos

Tener un documento en el cual se exprese el uso adecuado de cada activo y el colaborador debe expresamente dar su consentimiento. El documento debe indicar la consecuencia del incumplimiento de este acuerdo. Además, debe ser firmado por el colaborador y guardado de forma segura. En caso de un incumplimiento por parte del colaborador, este documento puede ser utilizado como base para cualquier sanción. Además, se debe comunicar a los empleados para evitar el uso indebido.

El objetivo del documento de uso aceptable de activos es asegurar que el personal comprenda que los activos de información, tales como los equipos (computadoras, tabletas, celulares etc.), el acceso a Internet, las aplicaciones y los servicios de mensajería electrónica son exclusivamente para fines laborales. Se pretende que el personal conozca las pautas y tomen las medidas necesarias para proteger los activos. Las siguientes son recomendaciones de lineamientos que puede tener el documento:

- Respetar y seguir las normas establecidas.
- Respetar las condiciones de uso y protección de activos de información.
- No instalar, cambiar o eliminar componentes de la plataforma tecnológica sin autorización.
- Solicitar la configuración y entrega de estaciones de trabajo y computadoras portátiles.
- Devolver los equipos de trabajo según la pauta definida.
- Evitar utilizar los recursos tecnológicos de la empresa para fines personales o ajenos a las labores de la empresa.
- Proteger la imagen y propiedad de la empresa, al usar los recursos de forma ética, cumpliendo las leyes y reglamentos vigentes.
- Utilizar solo el *software* propietario de la empresa o aquel *software* que esté autorizado.

Selección del personal

En la medida de lo posible, se debe llevar a cabo una revisión de antecedentes de los postulantes que van a manejar la información que ha sido catalogada como sensible, con el fin reducir el riesgo de que sea divulgada con algún fin económico o

delictivo. La organización debe hacer una comprobación mucho más detallada de los antecedentes, cuando una persona concurse por un puesto de trabajo en el que se va a manejar información sensible, por ejemplo, información financiera. Comprobar si existen referencias satisfactorias tanto en el ámbito profesional como en el personal. Comprobar la veracidad del currículum vitae del postulante. Confirmar las calificaciones académicas y profesionales declaradas. Comprobar de forma independiente la identidad (cédula de identidad, pasaporte). Comprobaciones en detalle: deudas, antecedentes penales etc.

Capacitación y educación en seguridad de la información

Proporcionar capacitación al personal sobre las buenas prácticas en materia de la seguridad de la información. Actualmente existen cursos digitales, los cuales se pueden acceder desde una computadora o celular. Esta capacitación deberá ser recibida por todos los colaboradores una vez al año. Se puede contar con un programa de educación, el cual puede incluir varias actividades de concientización, por ejemplo, un “día de la seguridad de la información”. Con el avance de los ataques cibernéticos enfocados en los trabajadores, hoy es más importante que nunca, garantizar que los empleados sepan cómo reconocer cuándo están siendo atacados. La capacitación de los empleados en temas de seguridad puede incluir los siguientes temas:

- Los malos actores detrás de los ataques y qué los motiva.
- Los métodos utilizados para los ataques.
- Cómo protegerse y cómo proteger la información a la cual tienen acceso.
- Términos de ciberseguridad clave.

Terminación o cambio del empleo

Contar con un procedimiento para la terminación de la relación laboral con un empleado, con el fin de que asegurar que salgan de la organización de una manera ordenada. Con el paso del tiempo las relaciones existentes entre las personas y las organizaciones cambian. Es un proceso natural, por lo que las condiciones laborales cambian también.

Las empresas normalmente tienen procesos para acomodar a las personas en estas nuevas situaciones, aunque a menudo se descuida cuál es el nivel de conocimiento e información que maneja el empleado en cuestión para poder realizar sus tareas, lo que puede representar riesgos inaceptables para la organización. Cuando una persona deja la empresa, todos sus privilegios deben ser cancelados de inmediato, dado que cualquier activo o información que estuviera bajo su control puede ser utilizado para su beneficio propio y la organización no podría tomar medidas.

Devolución de activos

Al finalizar la relación laboral, el empleado debe devolver todos los activos que estén en su poder. Para esto es necesario revisar la lista de activos y corroborar que efectivamente el empleado esté devolviendo todos los que tenía bajo su responsabilidad y no se deje ninguno sin devolver.

Eliminación de derechos de acceso

Revisar que todos derechos de acceso a la información sean removidos. En caso de que el empleado tenga un correo electrónico de la organización, se debe

desactivar la cuenta para que este no pueda enviar correos de parte de la organización una vez terminada la relación laboral.

Protección contra *software* malicioso y actualización de *software*

Las computadoras, tabletas y celulares que sean activos de la organización deben contar con un antivirus actualizado y realizar escaneos de virus al menos una vez al mes. Existen muchos antivirus gratuitos en el mercado que se pueden utilizar, no obstante, las licencias anuales de este tipo de *software* no son onerosas y se puede contar con respaldo del proveedor. Es muy importante asegurarse de que el antivirus siempre esté actualizado y activado. Por ninguna razón se debe permitir el desactivar el antivirus. Se deben mantener actualizados los sistemas operativos, antivirus y aplicaciones que se vayan a utilizar. Además, aplicar los parches de seguridad que recomiendan los fabricantes de sistemas operativos y equipos.

Respaldo de la información

Se deben realizar copias de respaldo de la información. Las computadoras, tabletas o celulares donde la información se encuentra almacenada pueden dañarse sin previo aviso, poniendo en peligro el acceso a la información importante de la empresa. Por lo cual, se deben realizar copias de respaldo regularmente. Existe información que debe ser respaldada a diario, otra puede ser respaldada dde manera semanal, dependiendo de su criticidad.

Es importante determinar el tiempo con el que se va a respaldar la información en relación con la importancia de esta. Los respaldos pueden ser realizados en discos duros externos, idealmente almacenados en otra ubicación física distinta a la de la oficina. Esto porque, si llegara a ocurrir un accidente, llámese incendio o inundación,

si la información se encuentra respaldada únicamente en la oficina, no serviría de nada porque también se perdería. Existen soluciones de respaldo de información en la nube, esta opción brinda una mejor alternativa, ya que, si por algún motivo hay un daño en la oficina, la información se puede acceder desde cualquier dispositivo conectado a Internet. Si se va a utilizar está opción de respaldo, es necesario asegurarse de que la empresa proveedora de este servicio cuente con todos los estándares de seguridad para garantizar que la información va a estar protegida.

Comercio electrónico

En caso de que la organización realice comercio electrónico, es necesario asegurarse de que cumple todos los reglamentos de la normativa establecida en el Código de Comercio, el Código Civil y las relativas a la defensa del consumidor como la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, Ley 7472, entre otras. Al ser el comercio electrónico realizado en Internet, este requiere una normativa especial para tratar de proteger de manera especial al consumidor, el cual se considera la parte débil en la relación de consumo. Por esta razón, y a falta de una ley emitida por la Asamblea Legislativa, el Poder Ejecutivo en el año 2017 reformó el Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor 7472 N.º 37899-MEIC y creó el capítulo X sobre la protección al consumidor en el contexto del comercio electrónico.

Uso de contraseñas

No dejar las contraseñas escritas en la oficina y no compartirlas con nadie. Cambiar contraseñas periódicamente (cada 30 a 60 días). De ser posible, usar un administrador de estas. Usar contraseñas de más de 12 caracteres y que no sean comunes como 12345678 o 123clave.

Se debe usar una contraseña diferente para cada una de las cuentas importantes, como el correo electrónico y banca en línea. Además, las computadoras, tabletas y celulares activos de la empresa deben contar con una contraseña para poder acceder a estos. Las siguientes son recomendaciones para el uso de contraseña:

- Permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores en los ingresos.
- Imponer una elección de contraseñas de calidad (Complejidad de contraseñas).
- Imponer cambios de contraseñas (cada 30 a 60 días).
- Forzar a los usuarios a cambiar las contraseñas temporales en el primer registro de inicio de sesión.
- Evitar la reutilización de las contraseñas por lo menos de los dos tres o cuatro últimos periodos.

Equipo de usuario desatendido

Cuando un colaborador se levante de su escritorio, debe bloquear la computadora con contraseña. La computadora no debe quedar desatendida, ya que esto podría permitir que otro colaborador haga una acción maliciosa en nombre del responsable de la computadora. Así mismo, un actor malicioso podría robar información sensible.

Política de pantalla y escritorio limpio

Se debe adoptar una política de escritorio limpio. Esta establece que los escritorios necesitan estar limpios de información, no dejar usuarios o contraseñas,

información de clientes, acuerdos, principalmente porque podrían ser accesibles por personas no autorizadas. La mayoría de los proyectos requieren confidencialidad y todos en la oficina manejan documentos que contienen información confidencial, por lo que todos deben proteger los documentos y los datos, ya sean internos o de personas externas. Entonces, mantener una política de escritorio limpio reduce el riesgo.

Política de teletrabajo

La pandemia a raíz del COVID-19 ha originado que la mayoría de las empresas se hayan visto obligadas a implementar el teletrabajo y este hecho está siendo aprovechado por los ciberdelincuentes para robar datos e información. En la actualidad, el teletrabajo es una actividad muy difundida en todo tipo de organizaciones, por lo que la seguridad de la información es un aspecto clave para garantizar la protección de la actividad de la empresa. Se debe tener por escrito una política de teletrabajo, en la que contengan los reglamentos que necesariamente deben ser acatados por los colaboradores de la organización. Se deben tener en cuenta los siguientes puntos:

- El suministro de equipo adecuado y mobiliario de almacenamiento para las actividades de teletrabajo, donde no se permite el uso de equipo de propiedad privada, que no se encuentra bajo control de la organización.
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede realizar, así como los sistemas y servicios internos a los que el teletrabajador se encuentra autorizado a acceder.
- El suministro de equipo adecuado de comunicación, incluyendo los métodos para asegurar el acceso remoto.

- Asegurarse de que los activos de la organización se encuentren en un lugar resguardado y protegido.
- Las reglas y directrices del acceso de la familia, visitas al equipo y la información.
- Tener previsto el soporte técnico del equipo y mantenimiento de *hardware* y *software*, en caso de que sea necesario para que el teletrabajador pueda realizar sus funciones correctamente.
- Los procedimientos para el respaldo de la información.

Anexo 4. Quiz de ciberseguridad. ¿Qué tanto sabe usted de conceptos de ciberseguridad?

Marque con una X la respuesta correcta.

1. ¿Cuál es la forma más segura de hacer clic en los enlaces de un correo electrónico?

( ) Haga clic en él, espere y vea lo que dice en su navegador.

( ) Copie y pegue el enlace en el navegador.

( ) Coloque el cursor sobre el enlace para ver lo que dice.

2. Si un correo electrónico comienza con 'Estimado cliente valioso', es muy probable que se trate de una estafa de *phishing.*

( ) Verdadero

( ) Falso

3. ¿Qué enlace de abajo es el enlace real?

( ) WWW.FACEB00K.COM

( ) www.facebook.com

( ) www.facedook.com

( ) www.fasebook.com

4. Los ataques de *phishing* suelen ocurrir a través del correo electrónico, pero también pueden ocurrir por teléfono.

( ) Verdadero

( ) Falso

5. ¿En qué circunstancias su banco o empleador se comunicará con usted para obtener su contraseña?

( ) Si su cuenta fue comprometida.

( ) Si hay una promoción en curso.

( ) Nunca.

( ) Si necesitan verificar su identidad.

6. Si alguien lo llama y quiere información sobre su cuenta, ¿qué información debe proporcionarle?

( ) Siempre que proporcionen su fecha de cumpleaños.

( ) Solo cierta información, si conocen su nombre, apellido y fecha de nacimiento.

( ) Ninguna, lo mejor es llamar directamente a la institución.

7. Los empleados son la parte más débil del vínculo de seguridad para las empresas.

( ) Verdadero

( ) Falso

8. Verificar las redes sociales de alguien es una forma segura de verificar quiénes son.

( ) Verdadero

( ) Falso

9. ¿Qué acciones ayudan a mantener seguras las contraseñas de su negocio? Seleccione todas las que correspondan.

( ) Use las mismas contraseñas para los sistemas de su negocio que las que utiliza para sus cuentas personales, de modo que las pueda recordar con mayor facilidad.

( ) Use contraseñas diferentes para cada sistema, incluida su cuenta personal.

( ) Use contraseñas que pueda recordar o almacénelas utilizando una herramienta de administración de contraseñas segura.

( ) Use un trozo de papel del escritorio para anotar sus contraseñas.

10. ¿Cuál contraseña es más segura?

( ) 53gur!dad

( ) EstaContraseñaesSegura

11. Una contraseña complicada, como L3@rn!Ng, significa que es compleja y difícil de descifrar.

( ) Verdadero

( ) Falso

Una contraseña como 0123456789 es segura porque tiene 10 caracteres.

( ) Verdadero

( ) Falso

12. ¿Cuándo es seguro utilizar HTTP?

( ) Cuando escribe su nombre de usuario o contraseña.

( ) Cuando escribe solo su información de pago.

( ) Cuando está leyendo un artículo.

( ) Cuando HTTPS no está disponible.

13. El sitio usa HTTPS, pero el navegador aún le dice que es una conexión que no es de confianza. ¿Qué debería hacer?

( ) Ignore la advertencia, ya ha visitado los sitios muchas veces antes.

( ) Evite ir al sitio web hasta que desaparezca la advertencia.

( ) Dígale al navegador que agregue una excepción a este sitio.

14. ¿Cuándo debería actualizar su navegador?

( ) Tan pronto como le notifique que hay una actualización disponible.

( ) La próxima vez tiene que reiniciar su computadora.

( ) Solo cuando compra una computadora nueva.

15. Hacer que su navegador recuerde sus contraseñas es conveniente, pero ¿cuáles son los riesgos?

( ) Si le roban su computadora, sus contraseñas se almacenan en la computadora.

( ) Si deja su computadora desbloqueada, cualquiera puede obtener sus contraseñas guardadas.

( ) Si alguien toma prestada su computadora o la usa brevemente, podría ingresar a sus cuentas sin su permiso.

( ) Todo lo anterior.

16. Está vendiendo su teléfono celular viejo a un amigo, ¿qué debe hacer?

( ) Desconecte su correo electrónico del teléfono y véndalo.

( ) Dele el teléfono, una vez que su amigo instale su información, la suya se borrará.

( ) Borre todo en su teléfono al menos una vez y luego véndalo.

( ) Elimine su historial de navegación y luego venda el teléfono.

17. Eliminar un correo electrónico con datos confidenciales garantiza que los datos desaparezcan

( ) Verdadero

( ) Falso

18. Una de las formas más fáciles de proteger su teléfono es tener un código de acceso

( ) Verdadero

( ) Falso

19. Si descarga una aplicación de la App Store, es 100% seguro.

( ) Verdadero

( ) Falso

Respuestas a quiz de ciberseguridad

1. ¿Cuál es la forma más segura de hacer clic en los enlaces de un correo electrónico?

( ) Haga clic en él y espere y vea lo que dice en su navegador.

( ) Copie y pegue el enlace en el navegador.

R/ Coloque el cursor sobre el enlace para ver lo que dice.

2. Si un correo electrónico comienza con 'Estimado cliente valioso', es muy probable que se trate de una estafa de phishing.

R/ Verdadero

( ) Falso

3. ¿Qué enlace de abajo es el enlace real?

( ) WWW.FACEB00K.COM

R/ www.facebook.com

( ) www.facedook.com

( ) www.fasebook.com

4. Los ataques de *phishing* suelen ocurrir a través del correo electrónico, pero también pueden ocurrir por teléfono.

R/ Verdadero

( ) Falso

5. ¿En qué circunstancias su banco o empleador se comunicará con usted para obtener su contraseña?

( ) Si su cuenta fue comprometida.

( ) Si hay una promoción en curso.

R/ Nunca

( ) Si necesitan verificar su identidad.

6. Si alguien lo llama y quiere información sobre su cuenta, ¿qué información debe proporcionarle?

( ) Siempre que proporcionen su fecha de cumpleaños.

( ) Solo cierta información, si conocen su nombre, apellido y fecha de nacimiento.

R/ Ninguna, lo mejor es llamar directamente a la institución.

7. Los empleados son la parte más débil del vínculo de seguridad para las empresas.

R/ Verdadero

( ) Falso

8. Verificar las redes sociales de alguien es una forma segura de verificar quiénes son.

( ) Verdadero

R/ Falso

9. ¿Qué acciones ayudan a mantener seguras las contraseñas de su negocio? Seleccione todas las que correspondan.

( ) Use las mismas contraseñas para los sistemas de su negocio que las que utiliza para sus cuentas personales, de modo que las pueda recordar con mayor facilidad.

R/ Use contraseñas diferentes para cada sistema, incluida su cuenta personal.

R/ Use contraseñas que pueda recordar o almacénelas utilizando una herramienta de administración de contraseñas segura.

( ) Use un trozo de papel del escritorio para anotar sus contraseñas.

10. ¿Cuál contraseña es más segura?

( ) 53gur!dad

R/ EstaContraseñaesSegura

11. Una contraseña complicada, como L3@rn!Ng, significa que es compleja y difícil de descifrar.

( ) Verdadero

R/ Falso

12. Una contraseña como 0123456789 es segura porque tiene 10 caracteres.

( ) Verdadero

R/ Falso

13. ¿Cuándo es seguro utilizar HTTP?

( ) Cuando escribe su nombre de usuario o contraseña.

( ) Cuando escribe solo su información de pago.

R/ Cuando está leyendo un artículo.

( ) Cuando HTTPS no está disponible.

14. El sitio usa HTTPS, pero el navegador aún le dice que es una conexión que no es de confianza. ¿Qué debería hacer?

( ) Ignore la advertencia, ya ha visitado los sitios muchas veces antes.

R/ Evite ir al sitio web hasta que desaparezca la advertencia.

( ) Dígale al navegador que agregue una excepción a este sitio.

15. ¿Cuándo debería actualizar su navegador?

R/ Tan pronto como le notifique que hay una actualización disponible.

( ) La próxima vez tiene que reiniciar su computadora.

( ) Solo cuando compra una computadora nueva.

16. Hacer que su navegador recuerde sus contraseñas es conveniente, pero ¿cuáles son los riesgos?

( ) Si le roban su computadora, sus contraseñas se almacenan en la computadora,

( ) Si deja su computadora desbloqueada, cualquiera puede obtener sus contraseñas guardadas,

( ) Si alguien toma prestada su computadora o la usa brevemente, podría ingresar a sus cuentas sin su permiso.

R/) Todo lo anterior.

17. Está vendiendo su teléfono celular viejo a un amigo, ¿qué debe hacer?

( ) Desconecte su correo electrónico del teléfono y véndalo.

( ) Dele el teléfono, una vez que su amigo instale su información, la suya se borrará.

R/ Borre todo en su teléfono al menos una vez y luego véndalo.

( ) Elimine su historial de navegación y luego venda el teléfono.

18. Eliminar un correo electrónico con datos confidenciales garantiza que los datos desaparezcan.

( ) Verdadero

R/ Falso

19. Una de las formas más fáciles de proteger su teléfono es tener un código de acceso.

R/ Verdadero

( ) Falso

20. Si descarga una aplicación de la App Store, es 100% seguro.

( ) Verdadero

R/ Falso

Anexo 5. Cuestionario aplicado a directores de pymes

Preguntas

Respuestas

17

Cuestionario Seguridad Informática PYMES

Este cuestionario es parte de un estudio realizado en la Universidad Cenfotec con el objetivo de analizar el conocimiento con el que cuentan los directores de pymes en Costa Rica con relación a la Ciber Seguridad. Gracias por tomarse el tiempo para responder.

1. ¿En su empresa se generan respaldos de seguridad de la información relacionada con sistemas de información clave e información vital para su operación?

- Sí
- No
- No estoy seguro/a

2. ¿En su organización se procura la utilización de contraseñas seguras para el correo electrónico oficial?

- Sí
- No
- No estoy seguro/a

3. ¿Se tienen políticas o controles que establezcan que las contraseñas, tanto de los correos electrónicos del trabajo como las de los sistemas empresariales, sean diferentes entre sí?

- Sí
- No
- No estoy seguro/a

4. ¿Conoce si en su empresa está activada la autenticación de dos factores (ya sea por contraseña, huellas digitales, algún otro aspecto biométrico, tarjetas inteligentes, contraseñas temporales enviadas al correo o al celular, entre otros) para el acceso a los sistemas principales y a la información sensible de la empresa?

- Sí
- No
- No estoy seguro/a

5. ¿Qué dispositivos se utilizan dentro de su empresa para el entorno laboral?

- [ ] Computadoras portátiles
- [ ] Computadoras de escritorio

- [ ] Teléfonos móviles
- [ ] Tabletas

6. ¿Conoce si se tienen las siguientes funciones de seguridad activadas para los dispositivos de trabajo principales, siempre que sea posible?

- [ ] La pantalla se bloqueará automáticamente después de un período de inactividad.
- [ ] Código PIN, código de acceso, huella digital, identificación facial (u otra información biométrica) para acceder a los dispositivos.
- [ ] Localización electrónica de dispositivos cuando son extraviados.
- [ ] No estoy seguro/a.

7. ¿Conoce si en las computadoras portátiles o de escritorio de su empresa se tiene activado
el cortafuegos y habilitado el antivirus?
El cortafuegos y el antivirus son funciones de seguridad que están integradas en Windows y macOS, y se pueden encontrar en la configuración de su computadora. Sin embargo, es posible que también haya optado por comprar un producto que proporcione estas, o características adicionales, de un tercero.

- ○ Sí
- ○ No
- ○ No estoy seguro/a

8. ¿Conoce si se tienen políticas o directrices para que todos los dispositivos de trabajo principales cuenten con las últimas versiones de actualización del software?
El software incluye:
El sistema operativo del dispositivo (Como Windows)
Cualquier aplicación en el dispositivo

- ○ Sí
- ○ No
- ○ No estoy seguro/a

9. ¿Conoce si antes de instalar algún software en los principales dispositivos de trabajo se comprueba que sea de una fuente oficial? ¿Existen políticas o directrices en este sentido?
Esto puede incluir verificar que sea de una marca conocida, realizar una búsqueda en la web o solo descargarlo de una tienda aprobada por el fabricante, como Apple App Store o Google Play.

- ○ Sí
- ○ No
- ○ No estoy seguro/a

10. ¿Abre los correos electrónicos de los cuales desconoce quién es su remitente?

- Sí
- No
- No estoy seguro/a

11.Seleccione la afirmación que considere más acertada:

- Las pequeñas y medianas empresas (PYMES) no son un objetivo para los piratas informáticos.
- Solo las empresas que aceptan pagos en línea corren el riesgo de ataques de delitos cibernéticos.
- Todas las pymes están en riesgo.

12. ¿En su empresa se realizan capacitaciones para el personal en temas de seguridad informática?

- Sí
- No

13. ¿Conoce si en su empresa se mantiene un inventario de todos los equipos y software de TI?

- Sí se mantiene un inventario.
- No se mantiene un inventario.
- No estoy seguro/a.

14. ¿Conoce si su empresa cuenta con un plan de seguridad informática?

- Sí cuenta con un plan de seguridad.
- No cuenta con un plan de seguridad.
- No estoy seguro/a.

15.Si su empresa no tiene un plan de seguridad informática, ¿cuál considera usted la
razón principal?

- No sabría por dónde empezar.
- Es demasiado cara de implementar.
- No considero que sea importante.

Anexo 6. Resultados de encuesta a jefes de pymes

Cuestionario Seguridad Informática PYMES

17	02:47	Active
Responses	Average time to complete	Status

1. ¿En su empresa se generan respaldos de seguridad de la información relacionada con sistemas de información clave e información vital para su operación?

Si	9
No	8
No estoy seguro/a	0

2. ¿En su organización se procura la utilización de contraseñas seguras para el correo electrónico oficial?

Si	10
No	6
No estoy seguro/a	1

3. ¿Se tienen políticas o controles que establezcan que las contraseñas, tanto de los correos electrónicos del trabajo como las de los sistemas empresariales, sean diferentes entre si?

Si	4
No	12
No estoy seguro/a	1

4. ¿Conoce si en su empresa está activada la autenticación de dos factores (ya sea por contraseña, huellas digitales, algún otro aspecto biométrico, tarjetas inteligentes, contraseñas temporales enviadas al correo o al celular, entre otros) para el acceso a los sistemas principales y a la información sensible de la empresa?

Si	5
No	9
No estoy seguro/a	3

5. ¿Qué dispositivos se utilizan dentro de su empresa para el entorno laboral ?

Computadoras portátiles	12
Computadoras de escritorio	10
Teléfonos móviles	13
Tabletas	4

6. ¿Conoce si se tienen las siguientes funciones de seguridad activadas para los dispositivos de trabajo principales, siempre que sea posible?

La pantalla se bloqueará auto...	9
Código PIN, código de acceso...	9
Localización electrónica de dis...	5
No estoy seguro/a	4

7. ¿Conoce si en las computadoras portátiles o de escritorio de su empresa se tiene activado el cortafuegos y habilitado el antivirus?
   El cortafuegos y el antivirus son funciones de seguridad que están integradas en Windows y macOS, y se pueden encontrar en la configuración de su computadora. Sin embargo, es posible que también haya optado por comprar un producto que proporcione estas, o características adicionales, de un tercero.

Si	9
No	6
No estoy seguro/a	2

8. ¿Conoce si se tienen políticas o directrices para que todos los dispositivos de trabajo principales cuenten con las últimas versiones de actualización del software?
   El software incluye:
   El sistema operativo del dispositivo (Como Windows)
   Cualquier aplicación en el dispositivo

Si	5
No	10
No estoy seguro/a	2

9. ¿Conoce si antes de instalar algún software en los principales dispositivos de trabajo se comprueba que sea de una fuente oficial? ¿Existen políticas o directrices en este sentido?
   Esto puede incluir verificar que sea de una marca conocida, realizar una búsqueda en la web o solo descargarlo de una tienda aprobada por el fabricante, como Apple App Store o Google Play.

Si	7
No	6
No estoy seguro/a	4

10. ¿Abre los correos electrónicos de los cuales desconoce quién es su remitente?

Si	1
No	12
No estoy seguro/a	4

11. Seleccione la afirmación que considere más acertada:

Las pequeñas y medianas em...	0
Solo las empresas que acepta...	2
Todas las Pymes están en riesgo	15

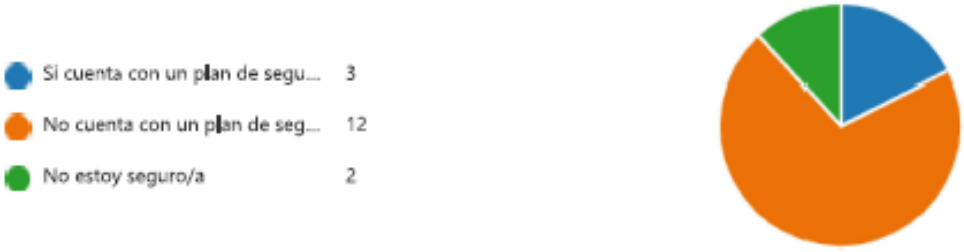
12. ¿En su empresa se realizan capacitaciones para el personal en temas de seguridad informática?

Si	1
No	16

13. ¿Conoce si en su empresa se mantiene un inventario de todos los equipos y software de TI?

Si se mantiene un inventario	9
No se mantiene un inventario	6
No estoy seguro/a	2

14. ¿Conoce si su empresa cuenta con un plan de seguridad informática?



15. Si su empresa no tiene un plan de seguridad informática, ¿cuál considera usted la razón principal?