UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS
ESCUELA DE INGENIERÍA INFORMATICA

Proyecto de graduación

Para optar por el grado de Bachillerato en Ingeniería en Sistemas de Información

Propuesta de una Guía de Ciberseguridad Preventiva básica en empresas Pymes de Costa Rica

Isaac José Villalobos Torres

AUTOR

Carlos Humberto Aguilar Mora

TUTOR

Daniel Álvarez Garro

LECTOR

San José, Costa Rica

Noviembre, 2023

CONTENIDO

TABLAS

FIGURAS

RESUMEN EJECUTIVO

El presente proyecto se enfocó específicamente a empresas Pymes de Costa Rica, esta clase de empresas representa uno de los principales ingresos del país debido a su accesibilidad, tanto en precios como en ubicación, estas tienen diversos focos de negocio, como supermercados, cooperativas y empresas de desarrollo de *software*, diseños y de consultoría.

Actualmente uno de los principales problemas de las Pymes es que se van quedando rezagadas en temas de ciberseguridad, como la creación de políticas e inventariado de *software* y no cuentan con un debido asesoramiento o material accesible que les pueda servir como un punto inicial durante el proceso de desarrollo y crecimiento de la Pyme.

Debido a esto, se propuso la creación de una guía de ciberseguridad básica que pueda servir principalmente de marco de referencia y conocimiento en temas de ciberseguridad, basándose en el marco de referencia de NIST *CyberSecurity Framework*, el cuál gira entorno a la gobernanza de datos (Identificar, Proteger, Detectar, Responder y Recuperar).

Dentro de los temas abarcados en la guía se desarrollaron 33 controles o puntos claves basándose en aquellas debilidades que suelen identificarse en empresas de más alto nivel para que las Pymes puedan ir adoptando estas prácticas desde tempranas etapas de desarrollo, estos controles fueron distribuidos en siete secciones que indican la forma correcta de realizar ciertas acciones internamente.

A partir de los estudios y encuestas realizados en las Pymes se identificó que uno de los principales problemas relacionados con la ciberseguridad es la falta de conocimiento, se construyó la guía con una estructura comprensible, manteniendo una terminología simple dentro de lo posible y concisa para que sea accesible no solo para Pymes, si no para cualquier lector que busque instruirse en ciberseguridad, convirtiéndose así en una base de información fundamental.

Adicionalmente, se tomaron en cuenta todas aquellas debilidades detectadas comúnmente por medio de las evaluaciones de vulnerabilidades para crear un debido proceso que permita evitar la exposición a estas y se pueda construir un ambiente entorno a la ciberseguridad

CAPÍTULO I: INTRODUCCIÓN

Planteamiento del problema

Actualmente en Costa Rica se desarrollan cada vez más las microempresas o pymes, donde uno de los principales problemas que afectan a estas es la falta de conocimiento en ciberseguridad, debido a esto, las Pymes se convierten en un nuevo blanco para los atacantes ya que la mayoría de los ataques que estos puedan efectuar son detectados, tiempo después de la brecha inicial o inclusive pueden pasar completamente desapercibidos.

La falta de conocimiento y los elevados costos de una consultoría externa de ciberseguridad pueden llegar a generar problemas serios organizacionales como, por ejemplo, una mala asignación de tareas, registros indebidos, procesos para el manejo de datos y capacitaciones deficientes, permitiendo que en un escenario real esta clase de empresas no esté preparada para repeler o evitar un ataque.

Objetivos

Objetivo General

- Desarrollar una guía de ciberseguridad básica que establezca las políticas y procedimientos de ciberseguridad orientados a la protección de los activos, dirigido a las pequeñas y medianas empresas de Costa Rica.

Objetivos Específicos

- Definir el proceso adecuado para crear una campaña de concientización y capacitación para ataques orientados a ingeniería social.
- Analizar distintos marcos de referencia y las buenas prácticas, políticas y procedimientos organizacionales de seguridad informática incluidos en ellos.
- Diseñar un plan de recuperación y respuesta para las Pymes en caso de un ataque informático.
- Establecer los conocimientos y buenas prácticas que los desarrolladores de *software* de las Pymes deben tener en cuenta durante el proceso de desarrollo de una aplicación web o móvil.

Justificación

Muchas de las empresas a las que los costarricenses suelen acudir diariamente (ventas de ropa, pulperías, panaderías, entre otras…) corresponden a emprendimientos y microempresas,

estas al estar aún en etapas de desarrollo suelen contar con múltiples fallas en su estructura, datos, políticas y procedimientos en general, en un mundo cada vez más digital, lo que las convierte en uno de los principales vectores para los atacantes, no solo en Costa Rica si no que en todo el mundo. Pese a que algunas optan por soluciones externas, sigue existiendo el problema del entrenamiento y concientización del personal, específicamente con la forma en la que se debe de manejar apropiadamente la información e incluso a que pueden estar expuestas las personas como colaboradores de la empresa

Tomando lo anterior como referencia, el desarrollo de una propuesta para una guía de seguridad informática básica que pueda ser completamente accesible para esta clase de empresas y para la población en general, puede llegar a marcar la diferencia en el posible escenario de un ataque real o una brecha de información. Todo esto con el fin de que estas puedan utilizarlo para implementar políticas y procedimientos de ciberseguridad, para agregar una capa de protección adicional a sus sistemas y demás activos que sean considerados como prioritarios, según su foco de negocio o intereses.

Viabilidad técnica

Se considera que implementar esta guía en una Pyme es técnicamente viable debido a que principalmente se ven aspectos administrativos simples, siendo en su gran mayoría la creación de nuevas políticas y procedimientos, siempre considerando que en dicha empresa haya al menos una persona con capacidades administrativas y una que tenga conocimientos destacables en temas de tecnología para abordar todas aquellas soluciones y procesos que impliquen configuraciones o demás en los activos tecnológicos de la empresa.

Tabla 1.

Recursos de hardware.

Recurso	Detalle
Equipo/*Laptop*	Marca Dell – Modelo Latitud
Procesador	Intel(R) Core (TM) i7-1265U CPU @ 1.80 GHz
Memoria RAM instalada	32 GB
Almacenamiento	512 GB SSD
Sistema Operativo	*Windows 10 P*ro

Fuente: elaboración propia.

Una vez definido el *hardware* por utilizar para la creación de la propuesta, es importante mencionar que para el *software* únicamente se utilizará el *software de Microsoft Office 365* para la creación del documento como tal.

Viabilidad operativa

Al concluir con esta propuesta, es importante recalcar que esta no necesariamente implica que se deba seguir completamente tal cual se indica, esto debido a que lo que se pretende y como su nombre lo indica es "guiar" a las Pymes en cómo realizar ciertos procesos que les pueden ser completamente desconocidos, especialmente enfocado en las áreas administrativas y de tecnologías de información (TI).

La ciberseguridad es un área en constante cambio, por lo tanto, una vez concluida y publicada esta guía, es necesario llevar a cabo un proceso de actualización y revisión periódica para adaptarse a las condiciones, cambios y nuevas vulnerabilidades que puedan afectar a los sistemas digitales.

El principal propósito de esta guía es que se convierta en un marco de referencia que pueda facilitarle a las Pymes una lista de acciones mínimas que deberían realizar e implementar para crear una cultura de ciberseguridad y concientización desde tempranas etapas de desarrollo, sin embargo; queda en decisión de cada una el poder utilizarla a su favor, buscando la mejor opción económica y operativa para poder llevar al funcionamiento óptimo del proceso de seguridad informática.

Viabilidad económica

Esta guía tiene como meta evitar el gasto excesivo de recursos para implementar los controles, además de estar pensada para que sea utilizada por empresas que actualmente se encuentren en este proceso de desarrollo, por lo que se buscaría reducir dentro de lo posible, gastos de producción o implementación y mejorar la postura de la empresa en estos temas.

Adicionalmente, esta guía está diseñada para que sea completamente gratuita y esté disponible para todo aquel que quiera seguirla, inclusive esta puede ser utilizada para sabes cómo medir la efectividad los controles internos y externos de su organización, siendo así un marco de referencia completamente accesible para la población costarricense.

Se realizó un análisis de los costos de un programador y analista en computación sin título universitario para realizar un costo aproximado del trabajo del analista según la lista de

salarios publicados por el Ministerio de Trabajo, al tipo de cambio de hoy este monto corresponde a $27.78 por hora, en la siguiente tabla se detallarán estos resultados.

Tabla 2.

Cotización de las actividades por realizar.

Actividad	Tiempo en días	Horas laboradas	Costo total
Análisis del mercado	10	1	$277.8
Análisis de distintos estándares y controles	15	1	$416.7
Entrevistas y asesoría de profesionales costarricenses	7	1	$193.46
Creación de la propuesta y redacción inicial	123	1	$3416.94
Revisión inicial	7	1	$277.8

Fuente: elaboración propia.

Viabilidad legal

La viabilidad legal de crear una guía de ciberseguridad basada en estándares reconocidos como el NIST (*National Institute of Standards and Technology*), CIS (*Center for Internet Security*) y CompTIA (*Computing Technology Industry Association*) es alta. Estas organizaciones y sus marcos de referencia son ampliamente aceptados, reconocidos y utilizados en la industria de la ciberseguridad por lo que es importante tener en cuenta que, al crear una guía basada en estos estándares, se cumplen con las licencias y términos de uso establecidos por cada organización, tomando en consideración también las siguientes leyes de la legislación costarricense:

- Ley 8148: Esta ley se refiere a la adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal. Estos artículos amplían el marco legal para abordar delitos relacionados con la explotación sexual de personas menores de edad, el turismo sexual y la trata de personas.
- Ley 4573: Esta ley, promulgada en 2001, tiene como objetivo reprimir y sancionar los delitos informáticos. Establece disposiciones para combatir actividades como el acceso no autorizado a sistemas informáticos, el sabotaje informático, el fraude electrónico y el uso indebido de información personal.

- Ley de Derechos de Autor 6683: Esta ley, aprobada en 1982, regula la protección de los derechos de autor en Costa Rica. Establece los derechos y obligaciones de los creadores y propietarios de obras literarias, artísticas y científicas, y proporciona un marco legal para su protección y explotación.
- Ley 8968: Esta ley trata sobre la protección de la persona frente al tratamiento de sus datos personales. Establece los principios y requisitos para el manejo y protección de la información personal por parte de entidades públicas y privadas en Costa Rica, con el objetivo de salvaguardar la privacidad y los derechos de las personas en relación con sus datos personales.

Proyecciones

Se espera que esta propuesta pueda convertirse en un marco de referencia de ciberseguridad para las Pymes de Costa Rica en general, ya que muchos de los temas abarcados en esta guía se verán de forma general para alcanzar y contemplar a la mayor cantidad de Pymes posibles, entre sus beneficios el principal sería servir de apoyo para agregar una capa de seguridad adicional a esta clase de empresas y servir de fuente de conocimiento para el entendimiento de algunos conceptos utilizados en el área de la ciberseguridad optimizando y reforzando su forma de pensar y de actuar.

Adicionalmente se busca que las Pymes creen una cultura de seguridad informática y de riesgos cibernéticos desde etapas tempranas de desarrollo, aprendiendo a valorar la información utilizada internamente y el daño que puede realizar una simple acción desinteresada o descuidada, así como incentivar la aplicación de capacitaciones obligatorias y de interpretación de las políticas, entre otras.

Alcance Funcional

En esta propuesta se encuentra la guía, que contiene información relevante sobre las políticas y procedimientos que pueden ser de utilidad en una pyme de Costa Rica, algunos de los apartados que se incluirán son:

- Manejo apropiado del riesgo de una amenaza informática: Se creará una matriz de riesgos que las Pymes puedan utilizar con el fin de clasificar riesgos a los que están expuestas, definiendo así un top 10 riesgos más comunes presentes en las Pymes y cómo responder apropiadamente, siguiendo las cuatro formas detalladas en *CompTIA*.

- Inventario de Tecnología y priorización de activos: Desarrollar una metodología para crear un inventario de *software* y *hardware* basado en el foco de negocio de la empresa que les permita determinar y priorizar los activos y datos críticos para el negocio que deben de ser protegidos.
- Responsables de gestionar la información: En este apartado se desarrollará una guía para crear una *matriz RASCI*, con el fin de definir los roles internos de las empresas para cada proceso que se realice.
- Plan de capacitaciones de ataques de ingeniería social: Definir un proceso de capacitación dirigido al personal de las Pymes a fin de que mediante la aplicación de las mejores prácticas estén en capacidad de identificar ataques de ingeniería social como *vishing*, *phishing* y otros que pongan en riesgo su operación.
- Respaldos de la información: Desarrollar la metodología de un proceso adecuado para el respaldo de la información, identificando:
    - ¿Quién debe de hacerlo?
    - ¿Cuándo debe de hacerse?
    - ¿Cómo debe hacerse?
    - ¿Qué debe de respaldarse?
- Legitimización de activos: Crear un procedimiento de adquisición y mantenimiento de *software* y *hardware* utilizado por las Pymes (Paquetes de Office 365 y máquinas como computadoras o servidores).
- El uso apropiado de cuentas de la pyme: Crear un procedimiento para manejar información confidencial de la empresa (contraseñas, PII, cuentas…) según NIST y definir políticas seguras de contraseñas y accesos implementando los principios de *least privilege* y *need-to-know de CompTIA.*
- Buenas prácticas informáticas: En este apartado se desarrollarán todas aquellas prácticas seguras utilizadas comúnmente en las áreas de TI, con el fin de mejorar la postura de ciberseguridad de las pymes.
- Evaluación de vulnerabilidades: Crear un proceso de evaluación de vulnerabilidades interno para las pymes, para evaluar la efectividad de los controles, políticas y procedimientos internos mediante cuatro fases:
    - Identificación de vulnerabilidades.

    - Análisis de las vulnerabilidades.
    - Priorización de activos (tomando en cuenta el inventario organizacional)
    - Remediación de vulnerabilidades.
- Plan de recuperación de ataques informáticos: Desarrollar un plan que permita a una pyme recuperarse de un incidente informático según el tipo de negocio al que esté orientado.
- Vulnerabilidades en *aplicaciones web* y móviles según OWASP: Crear parámetros defensivos para que el desarrollador los aplique en el desarrollo seguro de aplicaciones.
- Análisis de código estático y dinámico y su importancia: Desarrollar una metodología para la ejecución de pruebas sencillas para evaluar la seguridad del código dinámico y estático basándose en la *WSTG v4.2 de OWASP*, (donde se evalúan ataques como *Cross Site Scripting, SQL Injection, Clickjackin*g …).

Todos estos apartados o módulos son tomados en consideración debido a que son los principales fallos detectados en empresas más grandes y maduras, inclusive que una pyme, por lo que durante el desarrollo de la guía se procederá a detallar estos apartados con los pasos para que los mismos se puedan desarrollar con éxito durante el proceso de implementación por parte del ingeniero o el personal asignado para la tarea, además de mantenerse lo más simple posible para evitar posibles problemas de comprensión.

Alcance Metodológico

Los insumos utilizados para desarrollar la propuesta son marcos de referencia o estándares como *CIS, NIST* y para los conceptos a modo más general se utilizará un *e-book de CompTIA,* el cual incluye información relevante y actualizada, esto con el fin de obtener la mayor cantidad de información posible, adicionalmente se incluirán referencias a la ISO 27001 y 27002, estas con el fin de evaluar los controles indicados en el marco de trabajo de *NIST Cybersecurity Framework* y utilizarlos como referencia para evaluar su ajuste a una empresa Pyme.

Alcance Tecnológico

Para la implementación de esta propuesta, no se requiere alguna especie de requerimiento técnico, ya que la misma buscará trabajar con los recursos tecnológicos con los que cuenten estas

empresas, sin embargo, dentro de los sistemas y elementos utilizados más comúnmente en Pymes se encuentran:

- Sistemas POS (*Point of sale*), usualmente estas vienen acompañadas de un sistema de inventariado como lo es *Alegra*.
- Servidores EC2 de AWS.
- Computadoras de escritorio.
- *Laptops* y equipos de red.
- Licencias de *Microsoft y Office 365.*
- Licencias de antivirus como *Kaspersky, Avast, Sophos*.
- Una solución de *firewall, como PfSense o algún WAF* (*Web Application Firewall*) como los provistos por *cloudflare.*

CAPITULO II: MARCO REFERENCIAL

Para abordar en profundidad la propuesta, se deben de conceptualizar los temas más relevantes para esta investigación, la ciberseguridad es un tema complejo, en especial sin tener la comprensión de conceptos considerados como básicos en el área de tecnología y administración, en este capítulo se contemplarán todas aquellas definiciones que le permitirán al lector comprender la propuesta por desarrollar.

En el área de tecnología y ciberseguridad el concepto más básico corresponde a los activos, estos representan un valor y desempeñan un papel importante en el funcionamiento y éxito de una organización. Pueden ser tangibles o intangibles y tener diferentes niveles de importancia y sensibilidad para la organización.

Los activos informáticos corresponden a todos los elementos que componen el proceso de comunicación, es decir comprende la información, el emisor, el medio de transmisión y el receptor. En una forma detallada, además de la información comprende los elementos *hardware, software,* la organización y las personas que la utilizan. Comprende los elementos esenciales para garantizar el funcionamiento adecuado del sistema informática, de acuerdo con Ramos (et al.) (2017):

> Los activos informáticos hardware, comprenden la infraestructura, el cableado de red, los equipos de cómputo y los servidores, además los componentes relacionados con el software comprenden sistemas operativos, aplicaciones, programas de cómputo y por último la información que corresponde a bases de datos, paquetes de información, copias de información y claves. (pág. 92).

El *endpoint* se puede definir como un dispositivo o activo de una red, puede ser una computadora de escritorio, portátil, tableta, teléfono inteligente u otro dispositivo conectado a una red, principalmente son puntos de acceso y comunicación que permiten a los usuarios interactuar con una red o sistema (estos conceptos se contemplaran más adelante). Estos dispositivos pueden enviar y recibir datos, ejecutar aplicaciones y acceder a recursos de red, según (Pons, 2015):

> Un punto final o *Endopint* [sic.] es un dispositivo informático remoto que se comunica a través de una red a la que está conectado**.** Normalmente se refiere a los dispositivos que utilizamos a diario como ordenadores de escritorio, portátiles, teléfonos inteligentes, *tablets* o dispositivos de Internet de las cosas (IoT). (párr. 2).

En el ámbito de la ciberseguridad, los *endpoints* son considerados como puntos de vulnerabilidad potencial. Pueden ser atacados por *malware*, *hackers* u otras amenazas cibernéticas. Por esta razón, la protección de los *endpoints* y la implementación de medidas de seguridad en ellos son aspectos fundamentales para garantizar la seguridad de una red o sistema. Esto incluye el uso de soluciones de seguridad.

Dentro de las "soluciones de seguridad" se encuentran algunos *softwares* de gran importancia y que son considerados como la primera línea de defensa contra un evento de seguridad, a modo general entre las más importantes y básicas en toda empresa o pyme corresponden a *firewalls* y antivirus.

Según Weiss (2020) un antivirus es un elemento de *software* que se encarga de analizar y escanear archivos, correos o actividad que pueda ser considerada como maliciosa, usualmente estos no son almacenados en archivos de facíl acceso, si no en archivos ocultos de programas que se ejecuten en la máquina o inclusive en su propia configuración, a su vez un antivirus puede bloquear la ejecución de ese archivo malicioso y evitar que un atacante o tercero tenga acceso al equipo y a sus archivos, conservando su confidencialidad.

Los *firewalls* o corta-fuegos por otro lado evitan que esta clase de archivos lleguen al *endpoint*, este se encarga especialmente de analizar todo el tráfico proveniente de internet para evitar distintos ataques o conexiones indebidas por parte de un atacante, agregando limitaciones geográficas o inclusive bloqueando direcciones IPs catalogadas como maliciosas.

Parte de los activos más importantes en el área de tecnologías de información y en ciberseguridad, son los servidores, un servidor usualmente contiene información altamente sensible y confidencial de las empresas, también son bien conocidos por albergar las aplicaciones y sistemas utilizados de forma diaria en los procesos internos, de acuerdo con *European Knowledge Center for Information Technology (2022):*

> Es un aparato informático que **almacena, distribuye y suministra información**. Los servidores funcionan basándose en el modelo "cliente-servidor". El cliente puede ser tanto un ordenador como una aplicación que requiere información del servidor para funcionar. Por tanto, un servidor ofrecerá la información demandada por el cliente siempre y cuando el cliente esté autorizado. (párr.1).

Dentro de sus usos más comunes podemos encontrarlos como centralizadores de correos, almacenamiento de aplicaciones o bien como simples puntos de almacenamiento para los

archivos organizacionales y como control y cerebro organizacional, siendo este último el más relevante, también denominado como *Active Directory*. Los servidores a su vez tienen dos tipos de implementación, locales (*on-premise*) y *cloud*.

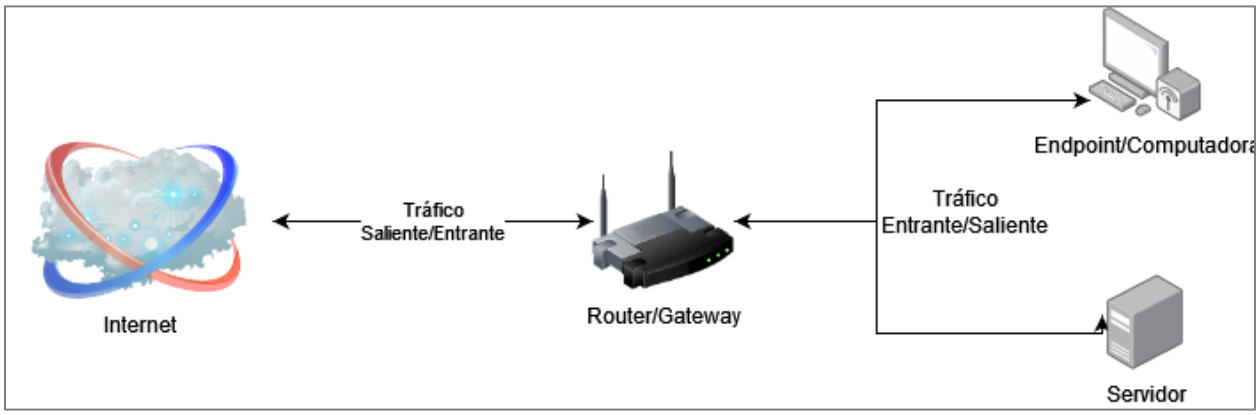
- Los servidores locales corresponden a aquellas piezas de *hardware* que se instalan de forma local o presencialmente dentro de un lugar especializado y acondicionado, dentro de alguna instalación empresarial también conocida como *datacenter*. Tomando en cuenta que para esta propuesta se contemplan pymes, no se espera que cuenten con este tipo de espacios debido al alto precio que conlleva el mantenimiento de estos sitios.
- Los servidores *cloud* son una solución bastante accesible para las pymes, ya que permiten trasladar los gastos de mantenimiento y personal a otra empresa dedicada a esto. En este caso, únicamente se paga por la cantidad de recursos que se deseen en el mismo. Además, estos se pueden integrar y acoplar perfectamente a las redes internas en caso de tenerlas.

Una vez definidos los activos tecnológicos es importante mencionar que estos convergen en un punto especifico llamado red y se puede definir como un espacio donde *endpoints* y servidores tienen una comunicación entre sí, todo *endpoint* conectado a la red se considera como un miembro de la infraestructura de redes, uno de los dispositivos más importantes a nivel de infraestructura es el comúnmente conocido como *router*/*Gateway* o puerta de enlace, esta es la que permite realmente que los dispositivos se puedan conectar entre sí y asignar una especie de "identificador" denominado IP (*Internet Protocol*) al equipo el cual es un protocolo de identificación, que le permite al dispositivo disponer de los demás protocolos para comunicarse con otros *endpoints* o bien, conectarse a internet.

Esta comunicación también se conoce como tráfico y se realiza a través de protocolos, los cuales pueden ser catalogados como los canales por los que se distribuye el tráfico y la información, en la siguiente imagen se ilustrará más detalladamente cómo se compone una red, y cómo interactúan sus componentes.

Figura 1.

Arquitectura básica de redes



Fuente: Elaboración propia.

Las redes mantienen un estándar especifico, el modelo OSI (*Open Systems Interconnection*), este es un modelo conceptual que describe cómo se comunican los sistemas de red. Se compone de siete capas funcionales y secuenciales las cuales se pueden definir como:

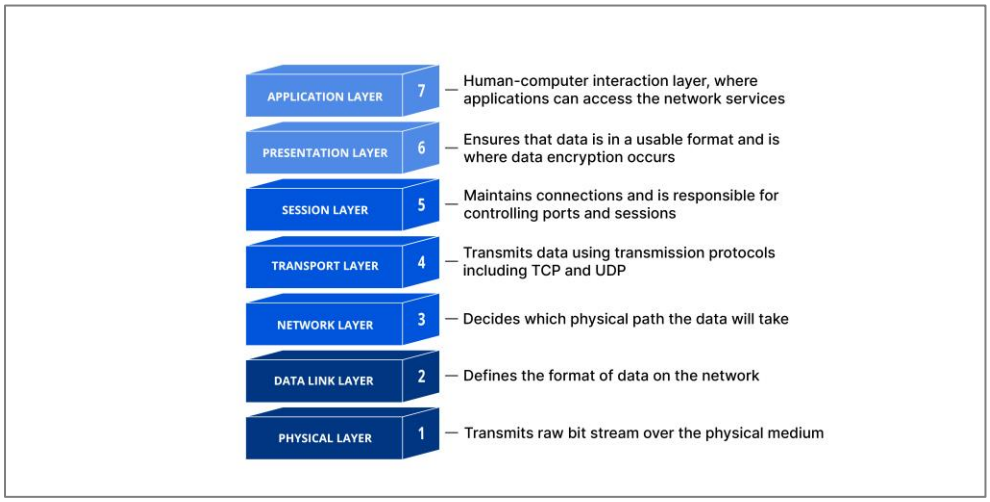
1. Capa física: Esta capa se encarga de la transmisión de bits de datos a través de un medio físico, como lo son los cables de ethernet o señales inalámbricas (WiFi). En esta capa se definen las características funcionales de los emisores.
2. Capa de enlace de datos: Esta capa se encarga de la transmisión integra de los datos entre nodos u *endpoints* adyacentes en una red. Detecta y corrige errores en los datos y maneja el acceso al medio físico.
3. Capa de red: Esta capa se ocupa del enrutamiento de paquetes a través de la red. Determina la mejor ruta para enviar los datos desde el punto de origen al destinatario, teniendo en cuenta factores como la congestión y la calidad del servicio.
4. Capa de transporte: Esta capa proporciona servicios de transporte de extremo a extremo, asegurando la entrega confiable y ordenada de los datos. Puede dividir y reensamblar grandes mensajes en segmentos más pequeños.
5. Capa de sesión: Esta capa establece, administra y finaliza las conexiones entre las aplicaciones en diferentes dispositivos. Permite la sincronización y el control de diálogo entre los procesos de las aplicaciones.

6. Capa de presentación: Esta capa se ocupa de la representación y de formatear los datos entrantes, traduciendo, cifrando y comprimiendo los datos según sea necesario. También se encarga de la compresión y descompresión de archivos.
7. Capa de aplicación: Esta capa ofrece servicios de red a las aplicaciones de usuario, dentro de este nivel se toman en cuenta los protocolos para servicios como correo electrónico, transferencia de archivos, navegación web, entre otros.

Cada capa se comunica con las capas adyacentes a través de interfaces bien definidas, y la comunicación de datos se realiza de manera descendente (desde la capa de aplicación hasta la capa física) y ascendente (desde la capa física hasta la capa de aplicación). El modelo OSI proporciona una estructura jerárquica que facilita el desarrollo, la implementación y la solución de problemas en las redes de comunicación, como se aprecia en la siguiente figura.

Figura 2.

Modelo OSI



Obtenido de https://www.cloudflare.com

Donde según Cloudflare (s.f.), “El modelo OSI se puede ver como un lenguaje universal para la conexión de las redes de equipos. Se basa en el concepto de dividir un sistema de comunicación en siete capas abstractas, cada una apilada sobre la anterior.”, este tema no se definirá en profundidad debido a que es altamente técnico y no agrega valor más que conocer su existencia.

Para las Pymes es importante conocer este modelo debido a que con base en esto se puede comprender cómo funciona de manera más apropiada el proceso de comunicación entre los *endpoints* y el internet como tal, inclusive al adquirir sistemas de defensa perimetrales como

*firewalls (*capa 2 y 4 del modelo OSI) o antivirus (capas 3, 5, 6 y 7 del modelo OSI) usualmente se toma en cuenta que algunos de estos operan en capas distintas a las usuales, realizando acciones más elaboradas, elevando su costo o reduciéndolo según su función.

Como se aprecia en la figura 2, se busca que todo el tráfico enviado a través de los protocolos se encuentre debidamente protegido, aquí se introduce un concepto de gran importancia en la ciberseguridad conocido como cifrado, este permite que toda la información trasladada en la red se mantenga completamente confidencial e íntegra, proporcionando una capa de seguridad adicional para los datos, sin embargo, siempre existe la posibilidad de que puedan aprovecharse de que esta forma de proteger los datos sea débil o no sea configurada apropiadamente.

Las redes pueden ser internas y externas según su forma de implementación, la red interna corresponde a todos aquellos activos conectados en una red local, esta es inaccesible para cualquier persona o *endpoint* que no esté directamente conectado a ella, este proceso de conexión puede darse mediante una *VPN* o bien conexiones *Wireless y ethernet,* a diferencia de la interna, la externa son todos aquellos activos que se pueden encontrar de forma pública en el internet, estos usualmente cuentan con un enlace que les permite mantenerse conectados a la red interna y otro que lo hace accesible mediante internet.

- VPN (*Virtual Private Network*): Permite establecer una conexión directa con la red interna, a través de un servidor ubicado en la red externa, desde cualquier punto del mundo, siempre y cuando el equipo que intenta realizar la conexión tenga acceso a internet y al dicho servidor.
- *Ethernet*: Conexión del equipo mediante un cable de red, estos permiten conexiones seguras y rápidas en la red.
- *Wireless*: Conexión del equipo mediante redes inalámbricas o WiFi, esta conexión puede resultar insegura, si no se cuenta con protocolos de cifrado de información, sin embargo, tiene la ventaja de la versatilidad físicamente mientras se esté en el alcance del *router*.

Las redes internas tienen una funcionalidad importante y es que permiten la segmentación y separación de redes mediante VLANs. Segun Weiss, (2020) “*A VLAN provides a way to limit broadcast traffic in a switched network, creating a boundary and, in essence, creating multiple, isolated LANs on one switch. A VLAN provides a logical separation of a physical network.”* (pág. 492).

Haciendo énfasis en lo anterior, una VLAN puede generar redes dentro de otras redes, donde por ejemplo los servidores internos, solo puedan ser accedidos por el personal de tecnologías de información, pero no por los del área de ventas.

Es importante mencionar que al diseñar una arquitectura de redes se debe inventariar todo equipo o *software* adquirido, como una buena práctica, crear un inventario de activos es un proceso realmente simple y que puede simplificar futuros procesos.

Las redes externas usualmente son las más sensibles y protegidas, debido a que cualquier persona podría acceder a la misma si no se cuenta con un debido control de acceso o soluciones de seguridad perimetrales, como un *firewall*, sin embargo, no por esto se debe descuidar la seguridad en las redes locales e incluso en las oficinas físicas, debido a esto existen las políticas.

Las políticas son las directrices de más alto nivel empresarial que dictan el "qué" se debe de hacer ante cierta situación y cuáles son los comportamientos que los colaboradores deben de acatar mientras formen parte de la organización, estas son establecidas por un departamento organizacional y realmente son fundamentales para establecer un marco de actuación consistente y coherente en las diferentes áreas y niveles de una empresa.

Adicionalmente, estas corresponden a uno de los principales temas por abarcar en la propuesta por desarrollar, debido a que la ciberseguridad gira en torno a las políticas, esto se ira apreciando conforme al desarrollo del presente capítulo, según Clavijo (2006):

> Una política de seguridad son un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico. (pág. 89).

Tomando en consideración lo expuesto por Weiss (2020) cada política planteada en la organización existe a su vez un procedimiento**,** si la política dicta "qué" se debe hacer, un procedimiento plantea "cómo" se debe de realizar o cumplir, por ejemplo, si internamente la empresa tiene una política de respaldo de la información que dicta que el respaldo de este debe realizarse cada semana, el procedimiento guía al o los responsables de realizar dicha acción en cómo llevar a cabo el proceso adecuado y avalado por la empresa, ambos son utilizados comúnmente como un punto de referencia en los estándares.

Un estándar es un conjunto de criterios, especificaciones o directrices establecidas para garantizar la uniformidad, calidad, compatibilidad y seguridad en diversos procesos, productos o servicios. Los estándares son desarrollados y publicados por organismos de normalización reconocidos a nivel nacional o internacional.

Estos desempeñan un papel crucial en diferentes áreas, como la tecnología, la industria, la salud, el medio ambiente, la seguridad y muchos otros campos. Establecen requisitos técnicos, metodologías, prácticas recomendadas y protocolos de comunicación que las organizaciones y los profesionales deben seguir para asegurar la eficiencia, la interoperabilidad y el cumplimiento de los estándares de calidad.

De acuerdo con Weiss (2020) un estandar es un conjunto de controles mandatorios, basados en politicas, entre los estandares de ciberseguridad más importantes se destacan las normas ISO (*International Organization for Standardization*) y NIST (*National Institute of Standards and Technology*), este ultimo esta especialmente relacionado con la ciberseguridad y sera el utilizado como marco de referencia a lo largo de la propuesta, Weiss (2020) define estos controles como:

> Control is a simply a defense or countermeasure put in place to manage risk. If a risk cannot be completely avoided or transferred, but the organization is not willing to completely accept the risk, the most appropriate action is to mitigate the risk. [Un control es simplemente una medida de defensa o contramedida implementada para gestionar el riesgo. Si un riesgo no puede ser completamente evitado o transferido, pero la organización no está dispuesta a aceptar completamente el riesgo, la acción más apropiada es mitigar el riesgo.] (pág. 778).

Analizando lo mencionado anteriormente los controles corresponden a todas aquellas medidas que se pueden tomar para compensar un riesgo, al que pueda estar expuesta la organización, la empresa NIST propone el *CyberSecurity Framework*, donde se detallan las acciones y controles consideradas por NIST como relevantes y que toda empresa debería cumplir, basándose en la ISO 27001, 27002, la NIST SP 800-53 y CIS (*Center for Internet Security*) *Critical CyberSecurity Controls*, a su vez estos pueden ser de distintos tipos según Weiss (2020):

- Técnicos: Se refieren a todos aquellos controles que son accionados por sistemas avanzados, entre estos se pueden encontrar los sistemas de monitoreo, recolección de

datos o listas de control de acceso, este último es de vital importancia en toda organización ya que se basa en el concepto de *least privilege*, este indica que a los colaboradores únicamente se les debe dar acceso a la información que sea necesaria para cumplir con su rol.

- Administrativos: Esta clase de controles se refieren a las políticas, procedimientos y procesos, usualmente se refieren o van orientados hacia las personas y a su forma de actuar según la situación o la actividad que se presente.
- Operativos: También conocidos como controles físicos, estos forman parte de la primera línea de defensa contra el acceso a los datos, entre estos se encuentran: proteger los medios de respaldo, asegurar los dispositivos de almacenamiento de archivos móviles y de salida, y prestar atención a los detalles del diseño de las instalaciones, incluyendo el diseño de puertas, cerraduras y sistemas de vigilancia.

Tras definir aspectos técnicos del área de tecnología, administración y ciberseguridad es importante conceptualizar los roles de las personas en la ciberseguridad, en cualquier clase de empresa se deben designar responsabilidades en función del puesto que se desempeña, por ejemplo, si una pyme tiene una persona encargada de realizar inventarios y otra de llevar la contabilidad se deben de asignar las responsabilidades de cada uno de forma independiente. al haber múltiples funciones y responsabilidades internas, las empresas optan por crear áreas especializadas, esto con el fin de mejorar su organización interna y cumplir con un principio de separación de funciones.

Una vez separadas las áreas se debe realizar un organigrama, el mismo le permite a la empresa diseñar una cadena de mando, para que así se cumplan principios básicos como el mencionado anteriormente de *least privilege*, dentro de las Pymes comúnmente se encuentran:

- Área financiera (Finanzas o contabilidad, compras): Son las encargadas de manejar o velar por los aspectos económicos de la empresa, así como adquisición de las materias primas o activos que se comercialice según el foco de negocio,
- Área administrativa (Directivas, Gerentes): Principalmente están encargados de la toma de decisiones, la mayoría de las políticas y procedimientos se definen por la junta directiva de la empresa.

- Área de ventas: Como su nombre lo indica, buscan comercializar los productos o servicios que ofrezca la empresa, así mismo están encargados de buscar posibles negocios o clientes que puedan ser favorables para la empresa.
- Área de TI (Tecnologías de la información, soporte técnico, mantenimiento de servidores…): dentro, se encuentran las personas que dan mantenimiento constante a los equipos utilizados en la empresa, velar por la correcta operación de todo *software y hardware* empresarial, en las Pymes usualmente es tercerizado y utilizado por demanda.

Cabe mencionar que no todas las Pymes tienen esta segregación de áreas ya que no todas cuentan con los recursos para tercerizar o contratar el personal necesario, sin embargo, es importante que se conozca que una buena práctica, proyectando un crecimiento es ir designando áreas y dividiendo los roles y funciones de todo colaborador de la empresa, teniendo como objetivo que cada área tenga una especie de "gerente" que se encargue de gestionar y mostrar los resultados del personal designado, acorde a Weiss (2020):

> *Too much power can lead to corruption, whether in politics or network administration. Most governments and other organizations implement some type of balance of power through separation of duties. It is important to include a separation of duties when planning for security policy compliance. Without this separation, all areas of control and compliance could end up in the hands of a single individual. The idea of separation of duties hinges on the concept that a scenario in which multiple people conspire to corrupt a system is less likely than a scenario in which a single person seeks to corrupt it.-(pág. 794).*

Según lo analizado en el texto anterior un exceso de permisos o privilegios puede llevar a las personas o colaboradores a realizar acciones poco éticas, y esto aplica en toda clase de áreas, para evitar este "abuso de poder" los gobiernos y demás instituciones buscan el equilibrio mediante una separación apropiada de roles y funciones y esta clase de separaciones debe ajustarse y planificarse previamente en las políticas institucionales ya sean sobre ciberseguridad o algún otra área relacionada a la gobernanza, delimitando un posible escenario donde se materialice un caso de abuso de poder.

La segmentación de roles y responsabilidades en los proyectos usualmente se realiza mediante el desarrollo de una matriz RASCI (*Responsible, Accountable, Support, Consulted,*

Informed), la cual le indica a los involucrados en el proceso cuál es la correcta distribución de tareas y cómo se debe de proceder al realizar o concluir una tarea.

Dentro de las áreas se encuentran las distintas posiciones organizacionales, especialmente para esta propuesta se destacan los más técnicos, correspondientes a ingenieros en tecnología o en general, administradores y personal más operativo.

Los ingenieros en tecnología es el personal especializado, encargado de mantener, desarrollar o mejorar sistemas, específicamente en el área de sistemas tecnológicos, Gonzàlez (2022) indica que este sector "es una rama de la ingeniería que se encarga del diseño, desarrollo, aplicación y mantenimiento de sistemas informáticos." (párr.1.). Los orientados al área de tecnología, donde laboran principalmente:

- Ingenieros de soporte: Estos podrían definirse como todos aquellos con la misión de implementar, instalar y mantener los servicios, son comúnmente encontrados en las áreas relacionadas con las tecnologías de información y ciberseguridad como servicios tercerizados en pymes, acorde con lo mencionado por González (2022) "Tiene capacidad de dar soporte y resolver problemas operativos y técnicos a los usuarios de los sistemas de información." (párr. 11).
- Consultores: **"**Experto capaz de asesorar a otras personas u organizaciones en la identificación de oportunidades informáticas para la solución de problemas de su campo de especialidad" (González, 2022, párr. 11), en el área de ciberseguridad específicamente, estos se pueden considerar como los encargados de ayudar a un cliente en la instalación de un *software* adquirido, la ejecución de una prueba, o bien brindar asesoramiento y soporte en caso de ser requerido, a su vez dentro de esta "rama" se encuentran los ingenieros de implementación, *pentesters* y analistas de SOC (*Security Operations Center*), estos últimos tienen la función de monitorear el tráfico entrante y saliente de la red para detectar una posible intrusión de los sistemas del cliente.
- Desarrolladores de *software:* Los desarrolladores suelen ser expertos en la construcción o como su nombre lo indica desarrollo de sistemas informáticos, páginas web o servicios, usualmente los *softwares* cuentan con ciclos de vida y procesos de desarrollo, sin embargo, estos no se contemplarán para efectos de esta propuesta.

Dentro de los puestos operativos usualmente se encuentran en posiciones encargadas las actividades centrales y cotidianas relacionadas con la producción, entrega de productos o

servicios, y satisfacción de las necesidades de los clientes, garantizando la eficiencia, calidad y rentabilidad de los procesos de producción y entrega, por ejemplo, vendedores, repartidores, recepcionistas, supervisores, ingenieros de inspección.

Los administradores se encargan de gestionar y coordinar todas actividades necesarias para el funcionamiento eficiente y eficaz de la organización. Su principal objetivo es planificar, organizar, dirigir y controlar los recursos disponibles para el mantenimiento y el crecimiento de las operaciones de la empresa, dentro de estas se encuentran principalmente los gerentes de área y el gerente general o la junta directiva (en el caso de una empresa más grande).

Dando principal énfasis en lo atendido por los consultores en el caso de las empresas grandes y uno de los temas claves de esta propuesta está la ciberseguridad, una vez identificados los factores humanos, administrativos y tecnológicos (*software y hardware*) se puede comenzar a desarrollar este concepto.

Según Kaspersky (s.f. a) una de las empresas lideres en soluciones de ciberseguridad se puede definir como “la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica” (párr.1.).

Tomando en cuenta lo anterior, la ciberseguridad es un tema crucial en el día a día, en aspectos desde lo cotidiano hasta lo laboral, la forma en la que se resguarda la información y los procesos internos para manejarla, pueden llegar a ser críticos desde el momento en que una empresa se encuentra en vías de desarrollo hasta su consolidación, para una pyme es crítico definir desde etapas tempranas estas buenas prácticas que pueden marcar la diferencia.

Los sistemas informáticos como se mencionó previamente es un aspecto fundamental, establecer políticas, procedimientos, estándares de calidad y crear la conciencia del valor de la información en los colaboradores debería de ser una prioridad para las pymes, ya que aunque muchos de los servicios y aplicaciones son tercerizadas es importante conocer que la información debe de clasificarse, Kaspersky, (s.f. a) declara que “La protección del usuario final o la seguridad de endpoints es un aspecto fundamental de la ciberseguridad. Después de todo, a menudo es un individuo (el usuario final) el que accidentalmente carga *malware* u otra forma de ciberamenaza” (párr. 39.)

En la ciberseguridad el usuario final, es un punto esencial, en toda empresa, una gran cantidad de ataques informáticos son realizados mediante ataques dirigidos al eslabón más vulnerable de la empresa el usuario, aunque se cuenten con sistemas seguros y buenas prácticas, basta con que uno solo caiga en un ataque de este tipo o bien un simple "*bug"* en una aplicación para que toda la red sea comprometida.

Ahora bien, la ciberseguridad son esas metodologías, procesos y soluciones que se encargan de defender a los usuarios finales, *endpoints* e información de la empresa de algo especifico, los atacantes, un atacante o *hacker* es considerado como el adversario principal de todo sistema informático y como un ciberdelincuente, actualmente las personas que desempeñen estas labores en Costa Rica pueden exponer a largas penas de prisión, estos usualmente desempeñan actividades ilícitas, robando información confidencial, datos con distintos fines, según Weiss (2020) los hackers se pueden dividir en:

- *Script kiddies*: Usualmente no poseen un gran talento para "hackear" ya que en el mundo de la cibernética para detonar fallos o ejecutar un fragmento de código no se requiere de experiencia como tal, lo que los vuelve peligrosos como tal, es que al no tener esta capacidad de análisis o madurez no suelen tener noción del peso de sus acciones y lo que puede desencadenar.
- *Insiders* o actores internos: Los *insiders* pueden ser atacantes internos en la empresa y pueden ir desde un empleado hasta un tercero subcontratado molesto, estos pueden vender, filtrar o infectar deliberadamente a la empresa debido a diversas situaciones, sin embargo, hay un escenario particular y es que un empleado puede ser un *insider* sin saberlo o inclusive sin que haya malas intenciones de por medio que es el escenario más común. Un ejemplo de esto es un usuario que se mande por correo archivos confidenciales de la empresa para trabajar desde su hogar, lo que pasa externamente en la empresa puede ser muy crítico ya que estos archivos se pueden contaminar con *malware* y posteriormente infectar a la red de la empresa.
- Hacktivista: Los grupos hacktivistas no tienen fines de lucro como tal, no buscan una "ganancia" por sus acciones si no que actúan como "vigilantes" en el mundo digital, en distintas situaciones en lugar de ser considerados como criminales, se toman como actores buenos, ya que han llegado a "bajar" sitios web relacionados con pornografía

infantil, venta de animales maliciosos o inclusive drogas, como lo ha hecho el grupo de *Anonymous* anteriormente.

- Sindicatos criminales: Son grupos dedicados completamente al crimen organizado, desarrollando *malware* o buscando fallas en la seguridad de empresas "grandes" con el único fin de obtener dinero, particularmente se destacan por dos técnicas especificas la ingeniería social y el *ransomware* una especie de *malware* que puede resultar crítico, esto se definirá más adelante cuando se describan este tipo de técnicas.
- Competidores: Usualmente son agentes tercerizados especializados en la búsqueda de información de la competencia directa de la empresa, esto se ve más como una especie de guerra de espionaje, con el fin de ver precios, productos o ideas en desarrollo que puedan ser aprovechadas por otra empresa.

Habiendo mencionado a los atacantes como los principales "adversarios" de la información, se debe destacar que estos buscan principalmente vulnerabilidades y vectores de ataque que les puedan permitir acceder a la información o a un equipo, este es un tema sumamente amplio, sin embargo, de forma resumida, Chavez (2023) lo define como "Una vulnerabilidad informática **es cualquier fallo o error en el *software* o en el *hardware***. Esto hace posible a un atacante o *hacker* comprometer la integridad y confidencialidad de los datos que procesa un sistema." (párr. 4.).

Las vulnerabilidades a nivel de *software* más comunes en el día a día incluyen versiones desactualizadas de instalación, las empresas usualmente adquieren aplicaciones y no se encargan de darles un mantenimiento apropiado a estas, conforme avanza el tiempo los atacantes encuentran "*bugs*" en la programación de las aplicaciones que les pueden permitir comprometer el *endpoint* y su información, esta clase de vulnerabilidad es comúnmente explotada, sin embargo estas son clasificadas ya que no todos estos errores de programación significan una exposición tan alta, para esto una corporación estadounidense conocida como FIRST (*Forum of Incident Response and Security Teams*) desarrollo una métrica o estándar denominada como CVSS *(Common Vulnerability Score System)* la cual de acorde con IBM (2023 a) "se utiliza para evaluar la gravedad y el riesgo de la seguridad del sistema informático." (párr.1).

Tabla 3.

Clasificación de severidad según el CVSS

Severidad	Valor
Baja	0.1 – 3.9
Media	4.0 – 6.9
Alta	7 – 8.9
Critica	9 -10

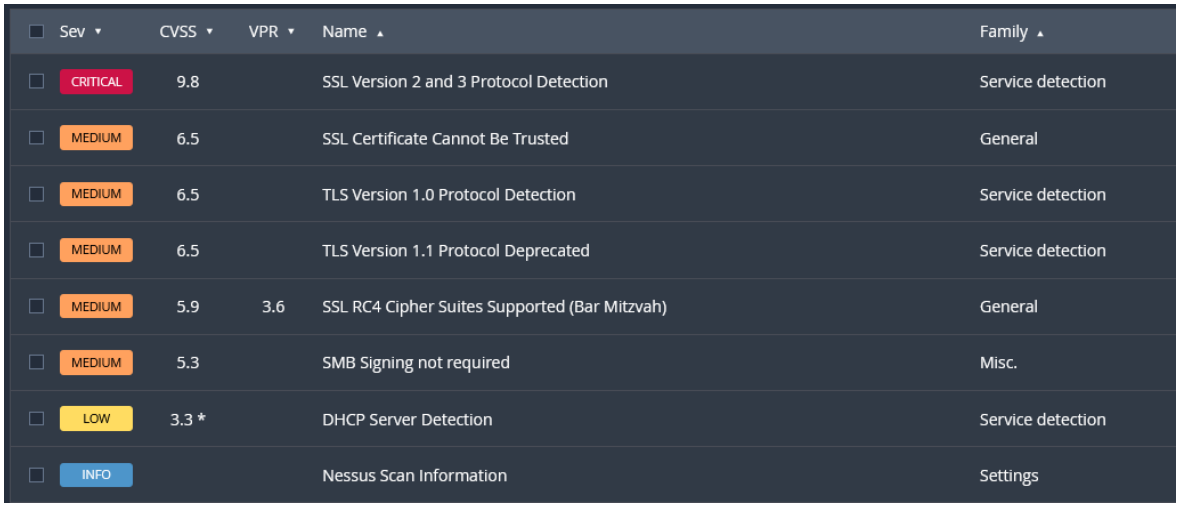
Fuente: Elaboración propia.

Para calcular el valor que estas vulnerabilidades representan, *FIRST* se basa en la triada de la información también conocida como CID, (donde se dice que la información y los datos deben permanecer confidenciales, íntegros y disponibles para la organización) y el impacto que las vulnerabilidades tienen en la misma.

A su vez existen escáneres de vulnerabilidades, estos tienen el fin de detectar configuraciones débiles, parches o actualizaciones faltantes, por ejemplo, *Nessus*, el escáner de vulnerabilidades de una de las empresas lideres en esta clase de soluciones, Tenable, este se encarga de escanear puertos, servicios en los equipos de la red y clasificar los hallazgos o vulnerabilidades según el estándar de *FIRST (*el CVSS), adquirir esta clase de soluciones puede significar un costo muy grande para una empresa, por lo que usualmente optan por tercerizar este servicio de análisis de vulnerabilidades con empresas como IBM, SISAP o Deloitte que a su vez las interpretan y emiten recomendaciones según su severidad.

Figura 3.

Resultados de un análisis de vulnerabilidades efectuado por Nessus.



Fuente: *Nessus Professional*, instalado en el equipo del autor.

Un concepto que usualmente es confundido con vulnerabilidad es el riesgo, el riesgo corresponde a todas aquellas acciones o situaciones que puedan poner en una situación de peligro a un *endpoint*, a un colaborador o inclusive a la empresa, y se puede calcular con la siguiente formula: Riesgo = Amenaza x Vulnerabilidad x Impacto.

De acuerdo con Chavez (2023) “el riesgo o amenaza informática es cualquier acción que desenlaza una vulnerabilidad informática. Es decir, es toda aquella acción que a raíz de estas toma provecho para atacar o invadir un sistema informático” (párr.8), el factor humano, también juega un papel fundamental para las pymes, un riesgo que fácilmente puede desencadenar una vulnerabilidad critica es la adquisición de *software* de forma ilícita o ilegal, estas aplicaciones perfectamente pueden esta alteradas por el distribuidor no autorizado e incluir *malware*, o *software malicioso*, lo que le permite perfectamente comprometer el equipo y hasta la red en el peor de los casos.

Un riesgo es un factor a lo que indudablemente cualquier activo de la pyme está expuesto, sea un *endpoint*, información de la empresa o inclusive personal de la pyme, definiéndose como algo que puede suceder y que puede o no tener un impacto en el activo que está expuesto al mismo, lo importante es saber cómo manejarlo y cómo clasificarlo, para manejarlo apropiadamente se deben de considerar las formas de responder ante estos, según Weiss (2020) hay 4 formas de responder ante él.

- Transferirlo
- Aceptarlo
- Mitigarlo
- Evitarlo

A su vez antes de tomar una decisión sobre cómo responder ante este, se debe realizar una categorización del riesgo, para esto una gran cantidad de empresas desarrolla una matriz de riesgo, la cual según Team Asana (2022) “La matriz de riesgos analiza los riesgos del proyecto en función de su probabilidad y gravedad. Una vez que identifiques los riesgos, podrás calcular el impacto general y otorgarle a cada riesgo la prioridad que le corresponda.” (párr.1). tomando en consideración lo anterior se tiene que todo riesgo identificado debe priorizarse adecuadamente evaluando el impacto que este pueda tener en los activos, para calcular este impacto Tema Asana (2022) propone tomar la gravedad o severidad del riesgo y multiplicarla por la probabilidad de que se dé, donde la severidad corresponde al nivel de afectación que pueden tener estos activos,

Siguiendo una cronología, una vez identificadas las vulnerabilidades, riesgos o un vector inicial de compromiso, se realiza un ataque, también conocido como evento o brecha, esta acción maliciosa efectuada por los "*hackers*" tiene como principal objetivo afectar al activo de alguna forma, específicamente en ciberseguridad afectan a la triada de la información, en la mayoría de los casos para obtener una ganancia financiera de la empresa que fue vulnerada o atacada, un ejemplo claro de esta clase de eventos son los sucesos dados en Costa Rica, relacionados con el grupo de "cibercrimen" conocido como Conti en el 2022 donde de acuerdo con Siles (2023), "El ataque a los sistemas informáticos del Ministerio de Hacienda por parte del grupo Conti en abril del año pasado, destaca entre los seis ciberataques más agresivos durante el 2022,". (párr.1), donde el objetivo principal de CONTI es completamente económico, perteneciendo a un grupo criminal.

Un concepto primordial en el área del "hacking" es una superficie de ataque, la cual se refiere a múltiples vectores de compromiso mediante los cuales un atacante podría realizar una explotación inicial y acceder directamente a la red interna de la empresa, de acuerdo con IBM (s.f. b) un concepto más técnico es " la suma de vulnerabilidades, vías o métodos —a veces llamados vectores de ataque— que los *hackers* pueden utilizar para obtener acceso no autorizado a la red o a datos confidenciales, o bien para perpetuar un ciberataque." (párr.1).

En un ataque informático una vez identificada la superficie de ataque y detectado una vulnerabilidad explotable, el atacante se da la tarea de explotar dicha vulnerabilidad, conocida comúnmente como un vector inicial de ataque la cual es el punto principal por el cual el *hacker* accedió a su objetivo, este vector puede ser una vulnerabilidad de *software* o inclusive una persona, posteriormente este realiza labores de post-explotación, esta es una serie de acciones ejecutadas con el fin de recabar más información que pueda servir para comprometer completamente la red.

Los ataques a su vez pueden ser de distintos tipos, dentro de los más comunes y los más presentados en el mundo se encuentran, la ingeniera social, *ransomware*, *malware* y ataques web, la ingeniería social es uno de los ataques y vectores iniciales más comunes y principales, ya que, pese a que una empresa pueda tener seguridad avanzada y aun así el eslabón más débil de toda compañía, son los usuarios, tal y como lo menciona Kaspersky (s.f. b):

Los *hackers* pueden tratar de aprovecharse de la falta de conocimiento de un usuario; debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no

son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de proteger esta información. (párr.1).

Esta técnica es tan utilizada debido a que aunque la empresa tenga sistemas de defensa perimetrales robustos y otra clase de soluciones, por un error de un usuario estas se pueden ver sobrepasadas mediante un simple correo, ese correo contiene un link o liga que redirige a un sitio controlado por el *hacker* del cual este puede obtener información del mismo o acceso mediante un *malware* u otra clase de *software*, en el mundo laboral, es común encontrarse con esta clase de estafas comúnmente conocidas como *phishing*.

El *phishing* se vuelve un vector sumamente utilizado por los atacantes, y de esta estafa salen algunas ramas, como el *spear phishing* y el *whale phishing*, estos se refieren a una metodología del atacante que mediante una investigación en internet encontrar puestos operativos que cumplan ciertos requisitos para hacer una campaña más especializada o dirigida, donde *spear* se refiere a que el atacante selecciona meticulosamente sus víctimas y en el de *whale* o *whaling* busca específicamente gente con cargos altos o administrativos en la empresa, ya que usualmente estos tienen cierto nivel de privilegios para realizar ciertas acciones.

Otro ataque común en Costa Rica perteneciente a esta rama de ataques es el *vishing*, que consiste en hacer que la víctima comunique datos confidenciales a través de canales de voz. La empresa estrategiaynegocios.net (2021) declara que “El *Vishing* es una práctica criminal fraudulenta realizada por teléfono, donde se tima a la víctima y la dirigen a realizar acciones o bien divulgar información sensible” (párr.12), esta clase de ataque se volvio favorable debido a la situación mundial con el Covid-19, donde la mayoria de los tramites se volvieron remotos.

Finalmente dentro de estas “estafas” se encuentra el *smishing*, como su nombre sugiere, este va orientado a mensajes de texto, por lo que afecta principalmente a dispositivos moviles, todas estas tecnicas tienen un punto común cuando buscan recopilar información y es que utilizan un concepto de ataque llamado “pozo de agua” o *wattering hole*, que consiste en copiar sitios o formularios de *páginas* frecuentemente utilizadas por las personas de forma regional o empresarial, estas “copias” son fieles al original y muy pocas veces contienen errores de redacción, por lo que es importante aprender a identificar esta clase de estafas, incluso antes de abrir el correo, mensaje o dar datos por llamada.

El *malware* es mundialmente conocido y uno de los más comunes también, este consiste en archivos o aplicaciones maliciosas alteradas con el objetivo de *tener* acceso a información

potencialmente sensible o inclusive llegar a comprometer toda una red, dentro de esta clase de ataques se encuentran:

- Virus: Un virus es uno de los tipos de *malwares* más comunes y usualmente son bloqueados por soluciones de antivirus como Kaspersky o Sophos, estos son fragmentos de código de programación maliciosa que se adhieren a archivos con el fin de ejecutarse en un *endpoint* y hacer que realice acciones que no debería como enviar información a través de internet, estando en un equipo, estos buscan la forma de replicarse en los archivos de este para infectar demás *endpoints.*
- *Bots*: Los *bots* consisten en múltiples maquinas controladas por una persona con el fin de realizar distintas funciones, en el mundo de la ciberseguridad son comúnmente utilizados por los ciberatacantes para realizar ataques de denegación de servicios, estos tienen como principal objetivo de saturar o "botar" servicios y dejarlos completamente inaccesibles por usuarios válidos.
- Gusanos: Un gusano es una especie de virus que busca moverse y adentrarse en la red o en el equipo, buscando intensamente información que le pueda ser útil y conservar su posición en el equipo o en la red, propagándose a través de todos los dispositivos conectados.
- Troyanos: son un tipo de malware o software malicioso que se camufla como un programa legítimo para engañar a los usuarios y acceder a sus dispositivos sin su conocimiento ni consentimiento. A diferencia de otros tipos de *malware*, como los virus o los gusanos, estos no se propagan por cuenta propia. En cambio, dependen de que la víctima realice una acción como ejecutar un programa para infectar un sistema y suelen distribuirse a través de archivos adjuntos de correo electrónico, descargas de software o enlaces maliciosos.
- *Spyware*: Como su nombre lo indica, estos corresponden a *softwares* espías, estos les permiten a los atacantes tener acceso a la máquina de una forma menos directa, ya que lo único que pueden hacer es observar las acciones del usuario, para detectar patrones de comportamiento, sustraer credenciales de sitios web o visualizar datos privados.
- *Adware:* Es una especie de *malware* que se instala en el equipo de una víctima con el objetivo de mostrar de forma persistente anuncios sobre sitios web, productos o paginas

maliciosas, desencadenando acciones indebidas por parte del usuario, saturación en la velocidad de procesamiento del equipo e instalaciones de otros tipos de *malware*.

Finalmente, los *ransomwares*, es una especie de *malware* considerado como uno de los riesgos más críticos a los cuales se pueden enfrentar las empresas hoy en día. El *ransomware* es un *software* malicioso criptográfico que se encarga de encriptar toda la información de los equipos afectados con el objetivo de pedir un rescate para recuperar la información, en caso contrario los atacantes usualmente amenazan con filtrar todos los datos en la *dark web* y eliminar cualquier rastro de ellos en la red de la empresa, dejando completamente expuesta toda la información de clientes o de colaboradores que haya registrada , la criticidad de esta clase de malware puede variar según la cantidad de equipos en los cuales se propago.

Dentro de los ataques más comunes se encuentran también todos los relacionados con vulnerabilidades en páginas o sitios web, estos usualmente suceden al haber fallos o "*bugs*" en la programación de la aplicación, ya sea por una programación deficiente o bien problemas en librerías utilizadas para el desarrollo, para comprender esto de una forma más clara es importante definir los siguientes conceptos:

- Código: Son los fragmentos básicos de programación que componen servicios, dentro de los que se encuentran todos aquellos procedimientos, variables y lógica utilizadas para el funcionamiento adecuado de las aplicaciones, el código puede variar según su lenguaje de programación, cada uno de estos se comporta de distintas maneras, por ejemplo, *python* es usualmente utilizado para el análisis de datos o javascript, utilizado frecuentemente como un *middleware* (enlace) entre el *front-end* y el *back-end*.
- *Scripts:* Son utilidades de código que realizan diversas funciones, en el "*hacking*" el concepto *de script* de refiere a una utilidad que permite escanear, explotar e inclusive remediar vulnerabilidades, comúnmente ejecutados en lenguajes de programación como *bash, python, php y rubí* sobre consolas comandos u interpretadores de código.
- Librerías: Las librerías son funciones previamente programadas accesibles que les permite ahorran tiempo y recursos a los desarrolladores, incluyendo en ellos fragmentos de código completamente desde 0, un ejemplo de una librería es *jQuery o Log4j*.
- Base de datos: se podría definir como un repositorio de datos centralizado, donde se carga toda la información de una aplicación o sistema, dentro de las bases de datos se pueden encontrar información, archivos y credenciales, dentro de las bases de datos se

utilizan consultas, estas suelen ser sentencias o fragmentos de código conocidos como SQL (*Structured Query Language*) que permiten la manipulación y gestión de la base de datos en general.

- *Front-End*: Se refiere a toda la capa de información que se le presenta por pantalla a los usuarios finales, también conocida como GUI (*Graphic User Interface*).
- *Back-End*: Esta es toda la capa lógica de la aplicación, todos los procesos, métodos y mecánicas de la aplicación se realizan en esta parte de la aplicación, en el *back-end* se procesa toda la información y se realizan las consultas respectivas.

Toda aplicación debería contar con ciertos parámetros defensivos antes de ser publicada, ya que es importante probar las aplicaciones antes de probarlas e incluso analizarlas de ser posible, antes de "cargar a producción" un servicio web este debe de pasar por un proceso de calidad, durante esta fase de pruebas de debe de analizar la aplicación en su totalidad (*front-end y back-end*) de forma estática y dinámica.

Las evaluaciones dinámicas usualmente se basan en probar todos aquellos ataques relacionados con vulnerabilidades web contra la aplicación en ejecución de forma manual por un experto o *pentester*, con el fin de medir los niveles de seguridad de la aplicación y si esta fue desarrollado entorno a buenas prácticas, de acuerdo con lo expuesto por OWASP (s.f. a) "*The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications*." (párr.1).

Dentro del top 10 de OWASP se encuentran ataques como la inyección SQL, fallos criptográficos, procesos de autenticación deficiente, utilización de librerías, servidores o demás componentes que sean vulnerables o tengan vulnerabilidades reportados.

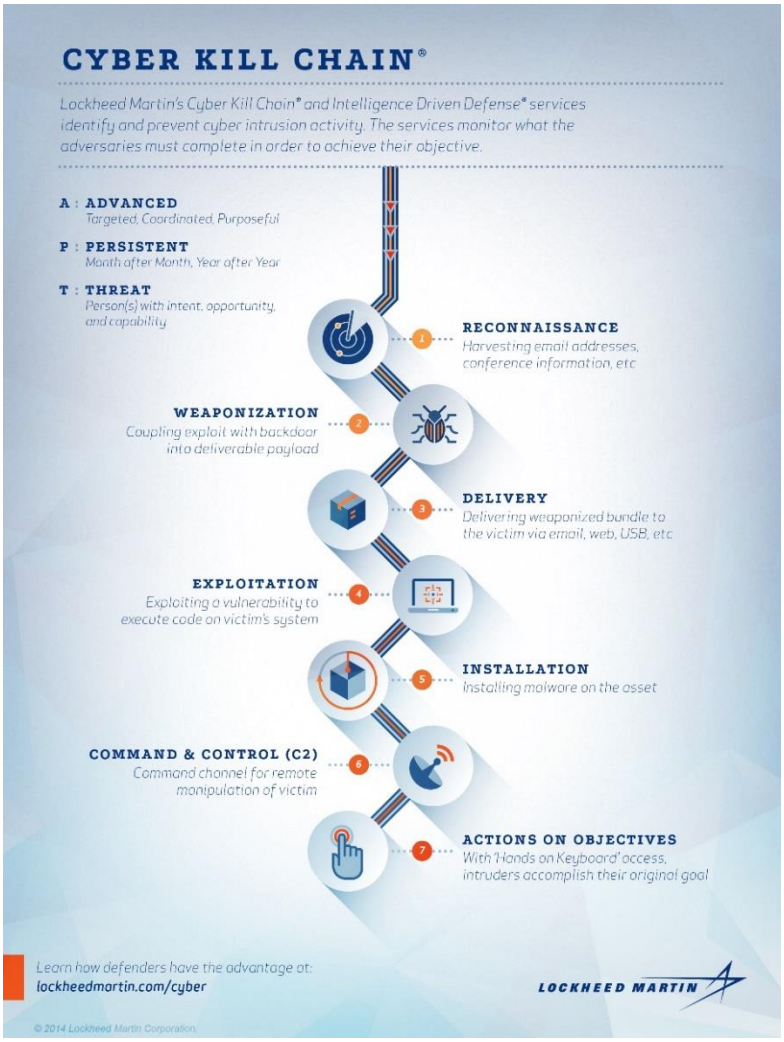
Las evaluaciones estáticas corresponden a analizar el código fuente de la aplicación en busca de posibles vulnerabilidades, este análisis a diferencia del anterior se hace con el código y no requiere que la aplicación este en ejecución, este se carga en un *software* que analice todas las líneas (*strings*) y sentencias de esta para detectar en el caso de haberlas, vulnerabilidades o potenciales riesgos, como credenciales en texto plano o *strings* de conexiones a bases de datos, un ejemplo de esta clase de *software* son *Veracode*, *SonarQube y Fortify de Microfocus*.

Parte importante para defenderse de un posible ataque es comprender la forma de pensar de un hacker real, pensar como un atacante e incluso conocer herramientas básicas como

metasploit, nmap o Covenant puede ser determinante, una mentalidad ofensiva puede permitirle a la persona técnica usar sus conocimientos para reforzar puntos que usualmente un atacante podría evaluar como parte de su superficie de ataque, para facilitar este proceso de comprensión la empresa MITTRE desarrollo una metodología mundialmente reconocida en el mundo de la ciberseguridad y el "*hacking*" llamada la "*Cyber Kill Chain*", la cual representa las fases de un ataque desde el reconocimiento de la superficie de ataque hasta la "limpieza". Estas fases se pueden apreciar la figura No. 4.

Figura 4.

Cyber Kill Chain.



Fuente: (Spitzner, 2016) Obtenido de https://www.sans.org

Tomando en cuenta estas ocho fases, las empresas pueden prepararse adecuadamente realizando simulacros de esta clase de pruebas, para esto suelen contratar o buscar un servicio de

terceros, que pueda poner a prueba su seguridad, sus sistemas y ver qué clase de información se puede encontrar de forma pública, esta clase de consultores responden al nombre de "*pentesters*", quienes realizan esta clase de pruebas con el fin de evaluar y analizar las vulnerabilidades que puedan o no tener los sistemas de una empresa, realizando metodologías similares a las que tendría un atacante real, estas evaluaciones se denominan pruebas de penetración, donde lo que separa a estos analistas de un atacante real, es la forma en la que se maneja la información.

Para esta clase de pruebas los consultores deben comprometerse a firmar un acuerdo conocido como NDA (*Non-Disclosure-Agreement*) el cual establece que toda la información recopilada u obtenida debe permanecer absolutamente confidencial. Donde hay tres tipos de escenarios para las pruebas.

- Caja blanca: En esta clase de prueba el cliente le provee, información más detallada sobre la red o el aplicativo por evaluar usuarios con y sin privilegios y permisos de conexión.
- Caja gris: Se le proveen permisos de conexión, en ocasiones y dependiendo de la actividad usuarios sin privilegios, la información es limitada, indicando únicamente el "alcance" de las pruebas.
- Caja negra: Este escenario intenta ser lo más cercano posible al punto de vista de un atacante real, sin información, sin clientes y sin un alcance concreto.

En un escenario donde un ataque se haya materializado, las empresas entran en un estado de recuperación, La recuperación de un ataque informático se refiere al proceso de restaurar y asegurar los sistemas y datos afectados después de un incidente de seguridad. Cuando una organización sufre un ataque informático, es fundamental actuar rápidamente para minimizar el impacto y recuperarse de manera efectiva, para esto se elabora un plan de respuesta a incidentes y uno que pueda servir para mantener las operaciones de la empresa durante el proceso.

Según IBM Services (2020) "un plan de continuidad del negocio (BCP) es un documento que describe cómo una empresa seguirá funcionando durante una interrupción no planificada del servicio". (párr.1).

Inicialmente para comenzar un plan de respuesta a incidentes o a un ataque informático es identificar y contener el impacto. Esto implica determinar cómo ocurrió el ataque, qué sistemas o datos se vieron comprometidos y qué medidas deben tomarse para evitar una mayor

propagación. Se puede requerir que los sistemas afectados sean completamente aislados, el cierre de cuentas comprometidas o realizar los bloqueos de los accesos no autorizados.

Una vez que se ha contenido la brecha de seguridad, se procede a evaluar el alcance del daño y restaurar los sistemas afectados. Esto puede implicar la reinstalación o actualización del *software,* la restauración de copias de seguridad previas o la recuperación de datos dañados o perdidos. Es esencial contar con planes de respaldo y recuperación de datos adecuados para facilitar esta fase y minimizar la pérdida de información crítica.

Finalmente, el alcance de esta propuesta son las pymes, y como pueden empezar a implementar ciberseguridad desde etapas tempranas de desarrollo, sin embargo, es importante definir el concepto de pyme como tal, según la Caja Costarricense del Seguro Social ([CCSS], 2018) “están constituidas por los micros, la pequeña y mediana empresa” (pág. 13). Dando a entender que son empresas consideradas como pequeñas o en etapas de desarrollo, basándose en la informacion provista por la CCSS (2018), se muestra la tabla No. 4.

Tabla 4.

Clasificación de las Pymes según su número de empleados.

Clasificacion del negocio	Rango de empleados
Pequeñas empresas	Mayor que 10 pero menor o igual a 35
Medianas empresas	Mayor a 35 pero menor o igual a 100

Fuente: Elaboración propia.

En Costa Rica las Pymes son de vital importancia en temas economicos debido a que de acuerdo con la Cámara de comercio de Costa Rica (2022) “el 47% de nuestro empleo es generado por este sector, que a su vez representa el 35.7% del Producto Interno Bruto en Costa Rica.” (párr.10), convirtiéndose en un pilar para le economía del país.

CAPITULO III: MARCO METODOLÓGICO

En este capítulo del estudio se describe y explica la metodología utilizada para el desarrollo de este, las herramientas utilizadas para el análisis del problema, así como los indicadores de éxito para cada uno de los objetivos estipulados en el capítulo I.

Enfoques de investigación

Los enfoques de investigación detallan la forma en la que se dan los procesos de la investigación incluyendo el análisis del problema, su concepto puntual es descrito por Sampieri, et al (2014) como "un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema" (pág. 4), y sus enfoques principales son: cualitativo, cuantitativo y mixto.

Cada uno de estos tipos cumple con distintas formas de obtener y analizar la información, donde los enfoques cuantitativos miden mediante datos más complejos mediante el establecimiento de preguntas antes y durante la investigación convirtiéndolo en un proceso más dinámico, por otro lado los cuantitativos se basa en datos cerrados, secuenciales y que puedan ser medidos, finalmente un enfoque mixto corresponde a una combinación de ambos enfoques, obteniendo la mayor cantidad de información y buscando una forma de analizar resultados que puedan ser obtenidos por medio de métodos más estrictamente cerrados como una encuesta o dinámicos como lo es una entrevista.

Enfoque cuantitativo

El enfoque cuantitativo se basa en la recolección y análisis de los datos estructurados que puedan servir como una medida básica de información, mediante el uso de estadística, dicho enfoque es completamente secuencial, debe completarse rigurosamente siguiendo un procedimiento especifico y a su vez requiere de un diseño de instrumentos que puedan servir para obtener la información acorde con el problema identificado mediante la identificación de variables o datos que puedan ser completamente cuantificables en términos numéricos y estadísticos.

Enfoque cualitativo

El enfoque cualitativo está basado en la recopilación y análisis de los datos no numéricos, estos son utilizados para la comprensión y exploración de múltiples situaciones o temas que puedan ser comprendidas mediante un punto de vista y una perspectiva más subjetiva, para esto se desarrollan o diseñan instrumentos que sirven de guía para el analista, dentro de esto se

encuentran, entrevistas y observaciones, las cuales permiten obtener datos que puedan ser más complejos e interpretados.

Enfoque mixto

Este enfoque de investigación busca realizar una integración de elementos extraídos del enfoque cuantitativo y del enfoque cualitativo para consolidarse como un solo estudio. En lugar de abordar una investigación desde una sola perspectiva metodológica, el enfoque mixto busca aprovechar las fortalezas de ambos enfoques para obtener una comprensión más completa y profunda del estudio, para esto se recopilan y analizan tanto datos cuantitativos como cualitativos en una misma investigación, con el fin de buscar conexiones y contrastes entre ellos. Esto permite obtener una visión más rica y contextualizada del tema en cuestión, así como también la oportunidad de validar o enriquecer los hallazgos de una perspectiva con la otra.

Enfoque de Investigación Seleccionado

Para este trabajo final de graduación se utilizará un enfoque mixto, ya que, para poder solventar el problema planteado, se analizarán los datos obtenidos mediante la aplicación de instrumentos (Cualitativo) a distintos profesionales con basto conocimiento en el sector para conocer su punto de vista y recomendaciones, así mismo también serán aplicados a las Pymes (Cuantitativos), con el fin de desarrollar una guía enfocada principalmente a los problemas más comunes presentados por esta clase de empresas, dichos problemas o fallos serán identificados mediante los instrumentos aplicados, las variables de evaluación seleccionadas para ser incluidas en la investigación y la información cuantificable relacionada y actualizada extraídas de fuentes confiables durante el estudio y el desarrollo de la propuesta.

Tipos de Investigación

Los tipos de investigación indican la forma que tomara el estudio, de acuerdo con ciertos aspectos que lo definen, al definir el tipo de investigación que se realizara se deben tomar en cuenta que resuelve cada tipo y cómo cada uno se puede ajustar a los distintos objetivos y problemas detectados mediante el análisis del problema principal de la propuesta o investigación, dentro de los tipos se destacan cuatro principales: exploratorio, descriptivo, correlacional y el explicativo.

El exploratorio busca indagar sobre problemas o situaciones que sean poco conocidos, siendo base fundamental de investigaciones que sean poco comunes o que busquen información sobre campos poco explorados y dar recomendaciones o identificar problemas con base en el

mismo. El explicativo determina las causas de los problemas y busca definir cuáles son las causas de los fenómenos y cómo estos pueden ser solventados, los descriptivos por otro lado investigan ese problema e identifican los componentes de forma detallada. Finalmente, la investigación correlacional busca determinar una relación entre las variables de un tema de investigación y cómo estas pueden interactuar en la ausencia o en la convergencia de una conexión.

Investigación Correlacional

La investigación correlacional busca establecer relaciones o asociaciones entre dos o más variables. El objetivo principal de esta es determinar si existe una relación medible entre los elementos de la investigación y en qué medida pueden estar relacionadas. Sin embargo, la investigación correlacional no implica establecer una relación de causa y efecto entre las variables, por otro lado, mediante el uso de estadísticas se puede recopilar información sobre estas y así comprender los efectos de la ausencia o la existencia de dicha relación.

Tipo de Investigación Seleccionado

Tomando en cuenta que el enfoque principal de la propuesta es identificar y medir la relación existente entre la ciberseguridad y las Pymes y cómo esta se puede fortalecer, se utilizará un método correlacional, debido a que esta busca principalmente definir y medir estas relaciones entre distintas variables, para esto se hace un análisis de las principales vertientes de estos temas para extraer las posibles variables que conformaran el estudio de esta relación durante el estudio, dentro de las cuales se pueden encontrar:

- Grado de cumplimiento de las políticas en general de las pymes.
- Nivel de efectividad de sistemas de defensas perimetrales contra amenazas o ataques cibernéticos.
- Capacitaciones o conocimientos básicos de seguridad de la información en el personal como, identificar una posible estafa, conocer el orden jerárquico de la información dentro de la organización y cómo podría afectar a la empresa una brecha de información.
- Cantidad de brechas de información pueden existir en el año, en Costa Rica.

Fuentes de información

Para el desarrollo de esta propuesta se utilizarán diversas fuentes de información con el fin de recopilar y analizar datos que puedan ser de utilidad para el desarrollo del estudio y de los conceptos específicos que este busca detallar, a modo conceptual las fuentes de información son

los recursos utilizados para obtener datos, hechos, opiniones y conocimientos sobre un tema específico, según Sampieri. et al (2014) “Siempre y cuando el tiempo y los recursos lo permitan, es conveniente tener varias fuentes de información y métodos para recolectar los datos” (pág. 417), debido a esto existen diferentes tipos de fuentes de información que pueden variar según la naturaleza y el propósito de la investigación. Estas se dividen en tres principales, primarias, secundarias y terciarias.

Fuentes de información primarias

Las fuentes de información son basadas y tienen información completamente original y publicada por primera vez propiamente el resultado del estudio realizado por el autor, estas investigaciones incluyen datos recopilados, investigados y son registros completamente directos de las fuentes consultadas, dentro de las fuentes más comunes se pueden encontrar entrevistas, grabaciones, fotografías, documentos oficiales, diarios y entrevistas.

Fuentes de información secundarias

Las fuentes de información secundaria son aquellas que recopilan, analizan e interpretan datos e información que ha sido previamente recopilada por otras fuentes. Estas fuentes proporcionan una visión y análisis de los datos existentes, sin implicar una recolección directa de información de primera mano. Algunas fuentes comunes de información secundaria incluyen: Libros y enciclopedias, artículos académicos y revistas, informes de investigación de organizaciones internacionales entre otros, para efectos de esta propuesta esta será principal fuente de información utilizada.

Fuentes de Información Terciarias

Las fuentes de información terciarias son aquellas que recopilan y resumen información proveniente de fuentes primarias y secundarias. Estas fuentes ofrecen una visión general y sintetizada de un tema, proporcionando una referencia rápida y accesible para obtener una comprensión básica o una visión panorámica de un campo de conocimiento. Algunas fuentes comunes de información terciaria incluyen: manuales, diccionarios, resúmenes y bibliografías.

Variables o Unidad de Medida

En este apartado se definirán y determinaran las variables por considerar para esta investigación, una variable es una forma en la que se pueden medir acciones, eventos u opiniones, estas unidades de medida se utilizan en diversos campos, como la ciencia, la investigación, la estadística, la física, la economía, entre otros, y Sampieri, et al (2017) lo define

como: “Una *variable* es una propiedad o característica de fenómenos, entidades físicas, hechos, personas u otros seres vivos que puede fluctuar y cuya variación es susceptible de medirse u observarse.” (pág.82).

Las variables en las investigaciones se desarrollan con base en los objetivos planteados en el Capítulo I, ya que su principal función es verificar que exista la forma de medir todas estas características mencionadas con base en los que busca solventar la propuesta en cuestión.

Variable Conceptual

Como su nombre lo indica, esta tiene como objetivo la definición de un concepto y representan conceptos abstractos que requieren de una definición concisa y para su estudio, simplificadamente se puede decir que es el concepto preciso de la o las variables identificadas por medio del planteamiento de los objetivos,

Variable Operacional

Indica la forma en la que se elaborará el proceso y todos aquellos mecanismos utilizados para la recopilación de información, es una medida concreta y observable que se utiliza para representar o medir una variable conceptual, son medidas específicas que se utilizan para capturar o representar esas variables conceptuales en el contexto de un estudio o investigación.

Variable Instrumental

Indica y refiere el instrumento como tal que se utilizar para obtener la información de la variable identificada, ya sean guías de entrevistas, análisis de datos, encuestas o demás formas de recolección de información.

Tabla 5.

Variables de la investigación.

Objetivos	Variables	V. Conceptual	V. Operacional	V. Instrumental
Definir una campaña de concientización para ataques orientados a ingeniería social	Campaña ingeniería social	Arimetrics (s.f.): "Una ***campaña*** es un esfuerzo de promoción durante un intervalo especificado de tiempo basado en la misma estrategia e idea creativa" (párr.1). Kaspersky (s.f. b): "conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados" (párr. 1.)	Encuestas Entrevistas Observación	Guía de encuestas. Guía de entrevistas Guía de observación
Analizar distintos marcos de referencia y las buenas prácticas, políticas y procedimientos organizacionales de seguridad informática incluidos en ellos.	Marco de referencia Ciberseguridad	Chen (2020) "identifica y expone los antecedentes, las teorías, las regulaciones y/o los lineamientos de un proyecto de investigación" (párr.1). Kaspersky (s.f. a) "práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos." (párr.1).	Encuestas Entrevistas Datos recopilados	Guía de encuestas. Guía de entrevistas Información documental sobre ataques informáticos en Costa Rica. Guía de observación.
Definir una metodología para la eficiencia de los controles internos de la organización.	Eficiencia Organización	(Martins, 2022) "La eficiencia es hacer las cosas "correctamente". Puede ser avanzar más rápido, finalizar trabajos con menos recursos, cumplir con proyectos grandes, pero con poco presupuesto o, de algún modo, hacer "más" con "menos"." (párr.3). (Editorial Etecé, 2021) "Una organización es un sistema social formado por un grupo de personas enfocadas en un objetivo en común a lograr dentro	Encuestas Entrevistas	Guía de encuestas Guía de entrevistas

		de un tiempo, espacio y cultura determinada.” (párr. 2).		
Diseñar un plan de recuperación para las Pymes en caso de un ataque informático.	Ataque informático Plan de recuperación de desastres	Caser (s.f.) “Es un intento de acceder a tus equipos informáticos o servidores, mediante la introducción de virus o archivos malware, para alterar su funcionamiento, producir daños o sustraer información sensible” (párr.1). IBM (s.f. c) es un documento formal creado por una empresa que contiene instrucciones detalladas acerca de cómo responder a incidentes no planificados como desastres naturales, cortes de electricidad, ataques cibernéticos y cualquier otro evento disruptivo. (párr.1)	Datos recopilados Análisis de documentación Encuestas Entrevistas Observación	Información documental sobre ataques informáticos en Costa Rica. Análisis de documentos. publicados en internet. Guía de encuestas. Guía de entrevistas Guía de observación.
Actualizar los conocimientos de los desarrolladores de las aplicaciones de las microempresas con los parámetros que deben de ser evaluados y priorizados a la hora de crear una aplicación	Parámetros Aplicación	(Microsoft, 2023) “Un *parámetro* representa un valor que el procedimiento espera que se pase al llamarlo.” (párr.3). (Calvo, 2022) “Una aplicación es un software que ha sido diseñado para cubrir una necesidad o realizar una tarea concreta dentro de un dispositivo electrónico como una *tablet*, un smartphone o un ordenador.” (párr.8).	Encuestas Observación Análisis de documentos	Guía de encuestas. Guía de observación. Análisis de documentos. publicados en internet

Fuente: Elaboración Propia.

Población

Para tener una visibilidad más clara de la población por estudiar se consultó la base de datos publicadas por el MEIC (*Ministerio de Economía Industria y Comercio de Costa Rica*) donde analizando el documento "Pymes activas al 31 de mayo del 2023" publicado por la entidad, se obtiene como resultado un total de 20280 Pymes activas en Costa Rica, sin embargo; se usará una población especifica, está ubicada dentro de la provincia de San José, en los cantones de Vásquez de Coronado, Goicoechea, Montes de Oca y Moravia con el requisito de que estén clasificadas como pequeña y mediana empresa, dando un total de 219 pymes.

Estos requisitos fueron establecidos debido a que principalmente se busca que las Pymes elegidas tengan cierto nivel o grado de conocimiento y experiencia en el mercado para evaluar sus conocimientos, eventos y acciones ante ciertas situaciones.

Muestra

Debido a que la población corresponde a un número elevado se realizara un proceso conocido como muestreo, la cual según Ortega (s.f.) se puede definir como: "El muestreo es una técnica de selección de miembros individuales o de un subconjunto de la población para hacer inferencias estadísticas a partir de ellos y estimar las características de toda la población." (párr.3), también la misma indica que puede tener múltiples tipos, para efectos de esta propuesta debido al grado de dificultad que puede significar contactar a un número determinado de Pymes se utilizará un muestreo no probabilístico, específicamente el método "por conveniencia".

Este método fue elegido ya que toma en cuenta factores como tiempo, recursos y la dificultad de contactar o rastrear a los sujetos de pruebas que cumplan ciertos requisitos para ser entrevistados, así mismo, se buscará realizar un acercamiento lo más cercano posible a una muestra representativa, la cual se puede calcular de acuerdo con la fórmula propuesta por INA [Instituto Nacional de Aprendizaje] (s.f. pág.1.):

$$n = \frac{Z\ 2\ pqN}{E2\ x(N\ -\ 1)\ +\ Z\ 2\ xPxq}$$

Donde:

- n es el tamaño de la muestra;
- Z es el nivel de confianza;
- p es la variabilidad positiva o probabilidad de éxito;
- q es la variabilidad negativa o probabilidad de fracaso;

- N es el tamaño de la población;
- E es la precisión o error.

Dando como resultado con un nivel de confianza de éxito de un 90 y una población de 219 se obtiene un resultado 53 Pymes por entrevistar, lo cual corresponde a un número factible, pese a que el enfoque no es probabilístico, se buscará alcanzar a la mayor cantidad posible de sujetos dentro de los parámetros definidos anteriormente.

Instrumentos de Recolección de Datos

Para evaluar la validez y el grado de conocimiento en temas de ciberseguridad y el nivel de capacitación que tienen los costarricenses colaboradores en las Pymes, así como apoyarse en el conocimiento de expertos en el tema, se utilizará un enfoque mixto, con el fin de obtener y recopilar la mayor cantidad de información, para esto los métodos de recolección de datos por utilizar son encuestas, datos obtenidos, entrevistas y observaciones sobre la comodidad, el área de trabajo de los empleados y si tienen espacios designados para el uso de equipos de cómputo, estas realizadas durante el proceso del acercamiento a las Pymes consultadas.

Proceso para la Recolección y Análisis de Datos

Una vez definidos los instrumentos por aplicar durante la investigación para obtener información sobre las Pymes y profesionales en el área, se procede a desarrollar el “cómo” serán obtenidos estos datos, para esto a continuación se desarrollarán los procedimientos del análisis y la recolección de información establecidos para esta investigación tomando en cuenta que esta plantea un enfoque mixto.

Para obtener los datos cuantitativos, se utilizarán encuestas, estas serán desarrolladas y aplicadas con la plataforma de Microsoft Forms, con el fin de facilitar la extracción de esta información, el analista, estará encargado de distribuir el vínculo respectivo a las distintas personas que laboren en las empresas que cumplan con los requisitos planteados durante el muestreo, para esto se plantea crear un código QR e imprimirlo para asistir presencialmente a algunas de estas Pymes, para el resto se buscará tener un acercamiento vía electrónico (redes sociales, o bien mediante la mensajería), el análisis de estos datos determinará si efectivamente existe una noción baja, intermedia o alta en temas de ciberseguridad, así como si la empresa estaría interesada en ajustarse en función de mejorar su postura de ciberseguridad.

Para las observaciones se planea evaluar los lugares de trabajo y controles físicos visibles en el momento del acercamiento físico a las Pymes dentro del alcance del muestreo, durante el

tiempo en el que el analista permanezca en el sitio deberá estar atento a sus alrededores y consultar si es posible realizar un recorrido por el local, con el fin de medir si tiene o no alguna especie de control específico. Para analizar estos datos se plantea que deben tener algunas cosas básicas como sistemas de pago electrónico, al menos una computadora, cámaras, *routers* y contraseñas robustas.

Las entrevistas serán realizadas de forma semi estructurada y completamente virtuales a distintos profesionales en el área de ciberseguridad, estos deben ser figuras referentes a este tema en su trabajo actual, además de tener conocimiento de la postura a nivel nacional con respecto a los ataques informáticos y ciberseguridad en general, estas se prestan más a respuestas subjetivas, por lo que parte de las respuestas esperadas son recomendaciones para la investigación, puntos de vista u opiniones sobre la "ciberseguridad en pymes".

La recopilación de datos a partir de documentos u otras fuentes de información debe cumplir el requisito de no tener más de tres años de publicado, con el fin de intentar extraer la información más actualizada posible, para esto se consultarán artículos liberados o publicados por el gobierno de Costa Rica, entidades de renombre a nivel de ciberseguridad, así como noticieros reconocidos.

El análisis de las respuestas de los profesionales y los datos recopilados de las Pymes documentos publicados provenientes de fuentes confiables, pueden ayudar a darle una orientación a la investigación hacia aquellos puntos considerados como "por mejorar" en las empresas y de esta forma ajustar los controles y demás apartados de la guía.

CAPITULO IV: ANÁLISIS DE RESULTADOS

En este capítulo se abarcarán y se analizarán los resultados obtenidos de los instrumentos aplicados, para efectos de esta investigación, se aplicaron tres instrumentos específicos, las entrevistas, observaciones y encuestas, la primera, la entrevista fue aplicada a profesionales en el campo de ciberseguridad y las dos últimas fueron aplicados a las empresas Pymes de Costa Rica contempladas dentro del alcance (muestra).

Resultados Obtenidos en las Entrevistas

Como se indicó previamente estas fueron aplicadas de forma semiestructurada por lo que se abrieron vertientes de las 12 preguntas planteada con el objetivo de obtener la mayor cantidad de información pertinente y para tener una mejor visibilidad de cuáles son los temas más relevantes o que necesitan una mayor profundidad durante el desarrollo de esta propuesta, para esto se analizaron las respuestas provistas por distintos profesionales en ciberseguridad que en el momento de la elaboración de esta investigación, laboran en empresas como el BCT, Ernst and Young (EY) y SISAP.

Estos no tienen una relación estrecha de trabajo con Pymes en Costa Rica, específicamente, si no con corporaciones más grandes de *retail*, finanzas y gobierno. Pese a esto, las perspectivas que los mismos tienen de las Pymes es correcta, ya que todos tienen una idea clara de su definición y de que hay distintas clasificaciones dentro de estas.

Principalmente consideran que los puntos de mejora en ciberseguridad son temas sobre políticas, al no existir realmente un marco sobre el cual se puedan basar para establecer esta clase de normativas relacionadas a ciberseguridad, las Pymes quedan a la deriva y muchas veces delegan estos servicios a terceros, estos usualmente implican un gasto adicional que puede ser bastante elevado, algunas de las políticas que consideran como necesarias es la limitación de accesos, identificación de roles, segregación de tareas, políticas de uso aceptable y de seguridad de la información en general.

Como otro punto importante destacan los procesos, establecidos mediante las políticas, la mayoría de estos muestran deficiencias, por lo que se deben establecer correctamente, específicamente en algunos puntos:

- Procesos de contratación de personal.
- Procesos de despido o retiro de personal.

- Procesos de adquisición de equipos y licencias.
- Procesos de respaldo de la información.

Dichos puntos serán tomados en cuenta durante el proceso de creación de la propuesta, adicionalmente estos procesos son vinculados a los de recuperación de desastres informáticos, donde se abarca el respaldo de la información, así como tener identificados los riesgos a los cuales la Pyme está expuesta para prevenir y planear acciones para tratar los eventos, por lo que también los controles entran como un factor relevante, estos son tan importantes como cualquier política según los profesionales del grupo BCT, debido a que esto demuestra que realmente no tiene una idea clara de sus riesgos.

La concientización fue mencionada por todos los profesionales entrevistados y consideran que es un problema principal, esto debido a que consideran que la mayoría del personal que labora en las Pymes tiene un conocimiento sumamente limitado, lo que los convierte en una especie de “blanco fácil” para los ataques informáticos, especialmente los orientados a ingeniería social y estafas (Phishing, Vishing, entre otras), debido a que este es el vector de ataque más común no solo para Pymes, si no para la sociedad en general.

Habiendo dicho la anterior consideran que capacitar a la población costarricense ante esta clase de ataques y métodos es de esencial importancia, al menos una vez al año, para evitar una exposición e ir desarrollando cada vez más una cultura de práctica de la ciberseguridad no solo laboralmente si no en la vida cotidiana.

Resultados Obtenidos de las Observaciones

Durante el proceso de la recolección de información con las encuestas, se realizaron ciertas observaciones relacionadas con la forma en la que se maneja la información, controles y reacciones de las personas que colaboraron con la encuesta, esto con el fin de identificar qué tanto se conoce o desconoce sobre el tema institucionalmente y qué medidas son adoptadas para mantener la seguridad de los activos pertenecientes a las Pymes.

En algunas de las empresas (aproximadamente un 60 %) fue posible identificar puntos de acceso visibles y expuestos al público, un *Access Point* colocado sin las medidas apropiadas de seguridad le puede permitir a los atacantes o un actor malicioso acceder a la red mediante WiFi o un cable que se conecte en el dispositivo, esta clase de elementos deben de colocarse en sitios elevados fuera del alcance de personas que no estén autorizadas a manejarlos o bien utilizar

“jaulas de seguridad” para mantener estos equipos seguros y evitar sean manipulados por terceros.

Las cámaras predominan en las medidas aplicadas como controles físicos, por lo general se encontraron en posiciones estratégicas, como en entradas, mostradores y almacenes, determinando que existe un nivel apropiado de conciencia, en uno de los sitios visitados se identificó que uno de los equipos de vigilancia ubicado en una sala de espera, estaba apagado y únicamente una de las empresas visitadas contaba con una bitácora de ingreso al sector administrativo.

El manejo de la información se volvió un punto más complejo de evaluar, debido a que no había una gran visibilidad de los archivos o de cómo se manejaba la información, sin embargo, en una de las empresas mediante la aplicación de una técnica de ingeniería social conocida como “*shoulder surfing*”, fue posible observar credenciales y documentos físicos con información bancaria, sobre la Pyme visitada.

Mediante el desarrollo de las encuestas fue posible observar comportamientos dudosos, sobre el conocimiento, algunas de estas personas indicaron que las aplicaciones utilizadas fueron sometidas a pruebas de penetración, sin tener conocimiento de qué es, esto se comprobó realizando la pregunta adicional de “si pudiese definir qué es una prueba de penetración” a la cual no hubo respuesta alguna, adicionalmente algunos conceptos básicos sobre ciberseguridad de los cuales se “tenía conocimiento” generaron reacciones de confusión entre los entrevistados.

Resultados Obtenidos de las Encuestas

Debido a que la ciberseguridad puede volverse un tema muy complejo y delicado, la gran mayoría de las encuestas realizadas fueron presenciales, durante este proceso muchas de las Pymes se sintieron amenazadas y prefirieron no responder ante las preguntas. Debido a estos inconvenientes se recopilaron 20 respuestas de distintas Pymes dentro del alcance o muestra mencionado previamente, es importante recalcar que dichas encuestas fueron realizadas por colaboradores de las Pymes (únicamente se aplicó a uno de ellos por cada Pyme visitada), que no necesariamente tienen tiempo trabajando en la empresa o conocimiento en profundidad sobre la misma, en el siguiente apartado se detallarán los resultados obtenidos de dichas preguntas.

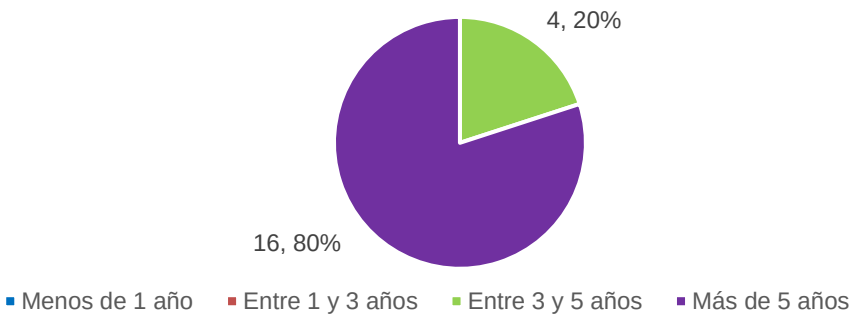
Pregunta #1

El objetivo de esta pregunta es servir de introducción al tema y sirve para conocer un poco más sobre las empresas encuestadas, conocer si son lo suficientemente longevas para

desarrollar políticas internas, aplicaciones *web* e incluso implementar controles, a sabiendas de lo vulnerable que es el país en temas de ciberseguridad.

Figura 5.

Tiempo activo del negocio.



Fuente: Elaboración propia.

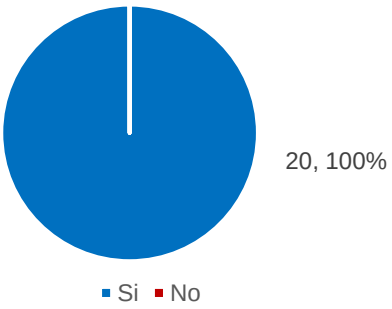
Tras un análisis de las respuestas se puede determinar que aproximadamente 16 (80 %) tienen más de 5 años de su creación y 4 (15 %) tienen entre 3 y 5 años, tomando en cuenta que una empresa o Pyme de 5 o más años "sobrevivió" el gran impacto de la pandemia del Covid-19 del 2020, se puede asumir que dichas empresas pueden llegar a tener una buena infraestructura, procesos apropiados y políticas rigurosas.

Pregunta #2

La presente pregunta fue aplicada con el objetivo de realizar un reconocimiento general sobre los distintos métodos empleados por la empresa en su día a día.

Figura 6.

Existencia de correo electrónico exclusivo del negocio.



Fuente: Elaboración propia.

Todas las pymes encuestadas (100 % de la muestra) respondió que, sí utilizan correos electrónicos dedicados únicamente a asuntos laborales, lo cual permite asumir que esta cuenta de

correos se utiliza para la tramitación de pedidos, inventarios y demás plataformas o servicios, tener cuentas de servicio asociadas a un correo especifico puede convertirse en un vector adicional de ataque.

Pregunta #3

La presente pregunta fue aplicada con el objetivo de realizar un reconocimiento general sobre los distintos métodos empleados por la empresa en su día a día.

Figura 7.

Existencia de dispositivos exclusivos del negocio.

Fuente: Elaboración propia.

Todas las pymes encuestadas (100 % de la muestra) respondieron que, sí tienen equipos dedicados exclusivamente a asuntos internos o laborales, demostrando que existe un nivel apropiado de conocimiento en temas de “controles de uso apropiado” en las distintas empresas, ya que no se utilizan dispositivos personales para manejar información confidencial o privada de la Pyme.

Pregunta #4

La presente pregunta fue aplicada con el objetivo de realizar un reconocimiento general sobre los distintos métodos empleados por la empresa en su día a día para la atracción de nuevos y potenciales clientes.

Figura 8.

Uso de redes sociales para la promoción de servicios.

Fuente: Elaboración propia.

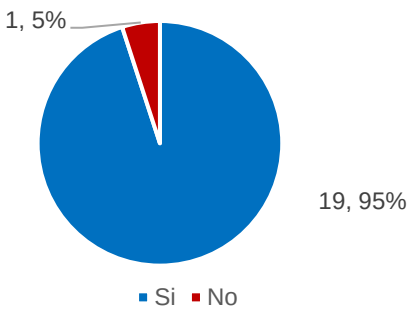
Todas las pymes encuestadas (100 % de la muestra) respondieron que, sí utilizan sus redes sociales para promocionar sus servicios, las redes son un punto de influencia bastante importante en la actualidad ya que plataformas como *Instagram o Facebook* son altamente navegadas por las personas y mostrar sus servicios, ofrecer descuentos e interactuar con el público, lo que le permite a la empresa alcanzar un mayor nicho de mercado y así tener más exposición a nivel nacional.

Pregunta #5 y #6

El objetivo principal de saber si aceptan o no pagos de SINPE móvil es que estos se prestan para realizar cierto tipo de estafas, haciéndole creer a la víctima que en efecto se le realizó un depósito bancario, esto mediante el uso de imágenes falsificadas, creadas a través de edición fotográfica.

Figura 9.

SINPE móvil como método de pago aceptado.

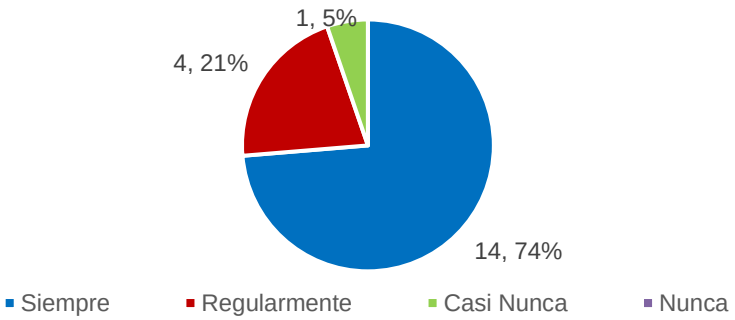


Fuente: Elaboración propia.

De las respuestas recopiladas se puede observar que aproximadamente un 95 % de las Pymes encuestas aceptan SINPE Móvil como un método de pago válido, de estas según los resultados de la pregunta #6, un *74 %* (14) de las Pymes revisan siempre que dichos pagos hayan sido debidamente acreditados, un 21 % (5) lo hacen regular y únicamente un 5 % (1) casi nunca verifica la acreditación de dicho método de pago.

Figura 10.

Validación de la acreditación de los pagos de SINPE móvil.



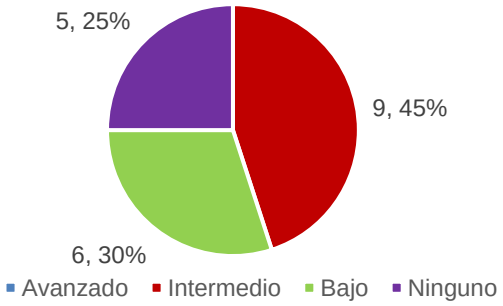
Fuente: Elaboración propia.

Pregunta #7

Entrando en materia de ciberseguridad, se busca conocer cuál es el nivel de conocimiento en general sobre el tema de forma generalizada (conceptos, métodos, procesos políticos, entre otras) que tienen las Pymes de Costa Rica.

Figura 11.

Nivel de conocimiento general de ciberseguridad.



Fuente: Elaboración propia.

Mediante la aplicación de este instrumento se puede determinar que un 45 % de los empleados de las Pymes tienen un conocimiento “intermedio” o básico sobre ciberseguridad, el 55 % restante se distribuye en un 30 % con un nivel bajo y el 25 % restante no poseen

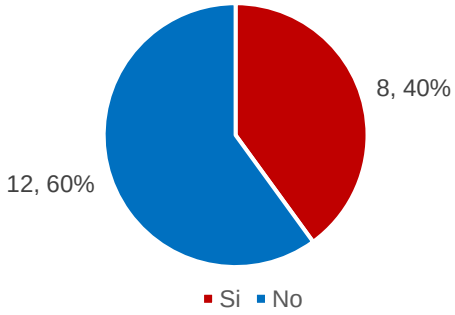
conocimiento alguno sobre el tema, dando a evidenciar que hay una clara falta de información en la población costarricense.

Pregunta #8 y #9

Estas preguntas se hacen para saber si internamente la Pyme o alguna otra entidad le ha realizado algún tipo de capacitación formal sobre ciberseguridad con las normativas básicas, identificación de estafas y demás buenas prácticas que pueden ser utilizadas para reducir una superficie de ataque.

Figura 12.

Recibimiento de capacitaciones o cursos de ciberseguridad.

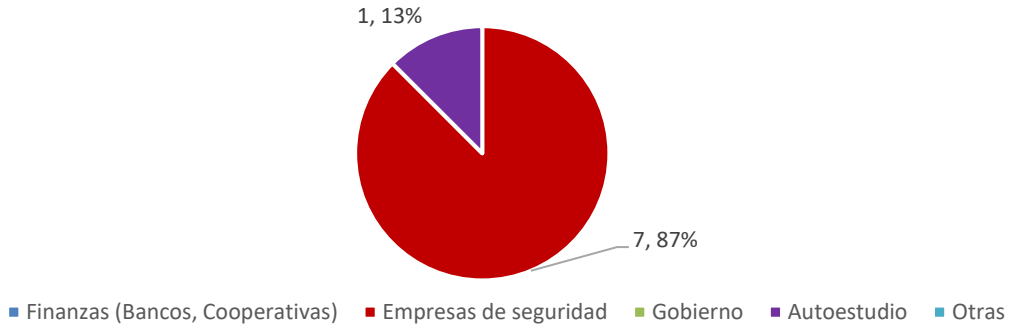


Fuente: Elaboración propia.

Tomando en cuenta los resultados recopilados anteriormente se puede apreciar que un 60 % de los colaboradores de las Pymes no han recibido capacitación alguna sobre ciberseguridad, donde según la Pregunta #9 el 40 % restante lo han recibido de empresas de seguridad informática (87 %) y mediante el autoestudio (13 % restante).

Figura 13.

Sector de la empresa que dio la capacitación.



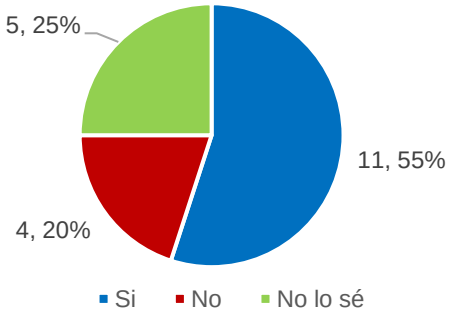
Fuente: Elaboración propia.

Pregunta #10

Sabiendo que uno de los principales problemas de las Pymes es la falta de concientización e información es de gran importancia saber si los colaboradores encuestados han sido víctimas de ataques específicos que pueden ser prevenidos mediante la capacitación.

Figura 14.

Víctima de estafas u otros ataques informáticos.



Fuente: Elaboración propia.

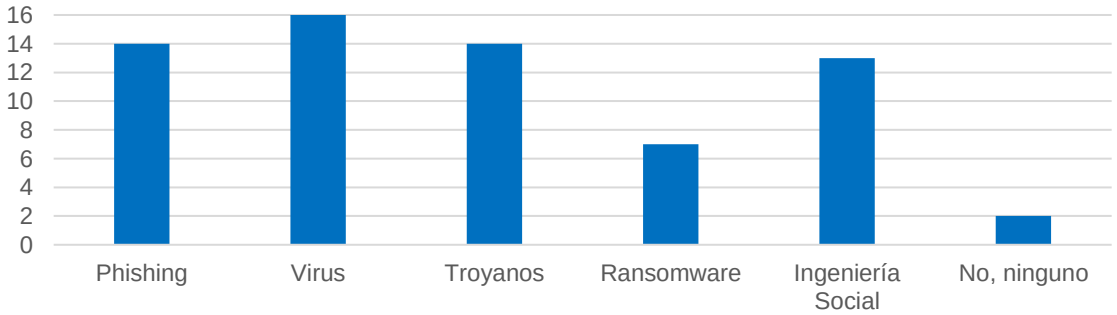
Según los datos recopilados, se determina que aproximadamente 11 (55 %) Pymes han sido afectadas por esta clase de eventos o ataques relacionados a ingeniería social, 4 (20 %) de ellas, no han sido víctimas, y 5 (25 %) de ellas no tienen conocimiento si han sido o no afectados.

Pregunta #11

El objetivo de esta pregunta es saber cuán familiarizados están los encuestados con ataques y técnicas que son considerados como básicos en el mundo de la ciberseguridad, entre los que entran los principales vectores a los que estos están completamente expuestos.

Figura 15.

Nivel de familiarización con ataques básicos informáticos.



Fuente: Elaboración propia.

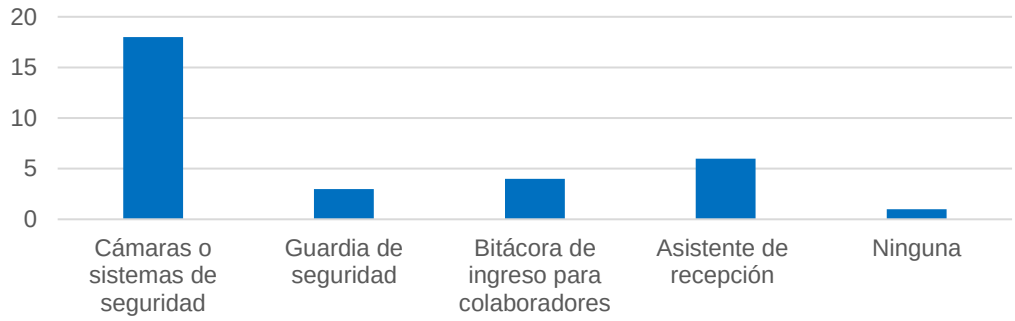
De los resultados representados anteriormente, se puede apreciar que el concepto con el que los colaboradores se encuentran más familiarizados es el de "*virus" con* 16 colaboradores anuentes del término, seguidamente "*phishing"* y "troyanos" con 14, ingeniería social con 13 y únicamente 7 colaboradores conocen el concepto de "*ransomware"*, finalmente 2 de estos, no están familiarizados con ninguno de los mencionados.

Pregunta #12

Esta pregunta se realizó con el fin de conocer si las Pymes tienen alguna especie de control físico implementado en sus instalaciones, estos son algunos de los más básicos y que usualmente son aplicados en esta clase de empresas.

Figura 16.

Implementación de controle de seguridad físicos.



Fuente: Elaboración Propia

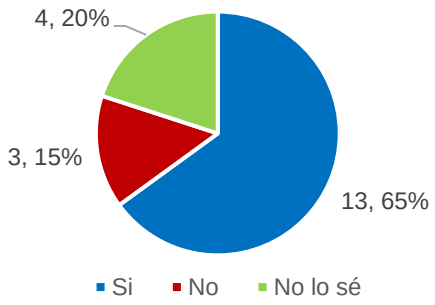
Mediante el análisis de estos resultados se determina que prácticamente el 95 % (18) de las Pymes encuestadas tienen al menos un control perimetral físico, en este caso este corresponde a las Cámaras o sistemas de seguridad, seguidamente seis de estas cuentan con un asistente de recepción, cuatro cuentan con bitácoras de ingreso para colaboradores, tres de ellas con un guardia de seguridad y una de estas no tiene ninguno de estos controles, esta última mencionó durante la encuesta que están en proceso de adquisición de un sistema de vigilancia.

Pregunta #13

El antivirus es una de las soluciones más esenciales en todo activo computarizado, este previene ataques con firmas conocidas o incluso los más complejos detectan comportamientos indebidos, algunos de estos son completamente gratuitos como *Windows Defender*, por lo que es de gran relevancia conocer si los encuestados saben o no de la existencia de este control lógico en sus computadoras.

Figura 17.

Existencia de antivirus u otros *softwares* similares en la empresa.



Fuente: Elaboración propia.

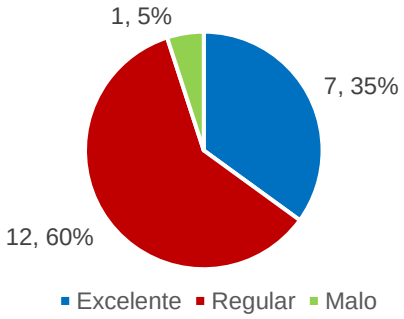
De las respuestas recopiladas se puede determinar que 13 colaboradores (65 %) saben que su equipo está seguro con un antivirus, cuatro (20 %), no conocen si tienen dicha solución aplicada en sus equipos y finalmente tres de estos (15 %) no tienen un *software* de defensa, infiriendo que desconocen de la existencia del antivirus básico incluido con las licencias de sus equipos de operación.

Pregunta #14

Parte importante de la seguridad es tener equipos operativos en un estado aceptable, debido a que si estos llegaran a presentar algún fallo físico dependiendo del estado o la capacidad del activo la recuperación de datos de este puede dificultarse, asumiendo que no haya copias de respaldo de la información del equipo.

Figura 18.

Estado general de los equipos informáticos.



Fuente: Elaboración propia.

Según sus colaboradores, la mayoría de las Pymes tienen equipos en estados aceptables, habiendo siete (35 %) que consideran que sus equipos están en excelentes condiciones y 12 (60

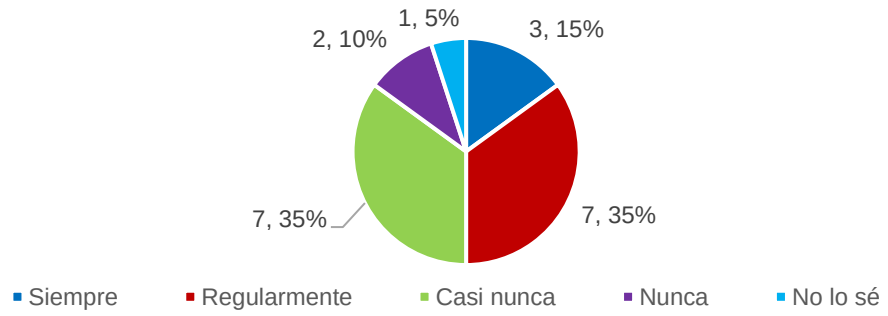
%) en un estado regular de operación, únicamente un trabajador considera que los equipos de la empresa se encuentran en un estado deplorable o malo.

Pregunta #15

Siguiendo con el posible evento de qué pasaría si, ocurriese un evento de seguridad, fallo, robo o extravío del equipo, es importante conocer cada cuanto realizan las Pymes los respaldos de su información, siendo esta una de las principales contramedidas de contingencia ante esta clase de siniestros.

Figura 19.

Frecuencia de los respaldos de información.



Fuente: Elaboración propia.

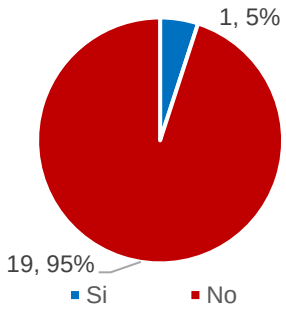
La distribución presentada en las respuestas es bastante variada, ya que abarcan todas las opciones posibles, teniendo en cuenta que es un aspecto relevante realizar un respaldo de información siempre que se pueda, únicamente tres (15 %) de estas lo hacen “Siempre” o diariamente, siete (35 %) de estas lo realizan regularmente, de igual forma la misma cantidad de Pymes casi nunca lo realizan, dos (10 %) no realizan los respectivos respaldos, y únicamente un colaborador desconoce si su empresa realiza o no esta actividad.

Pregunta #16

Los marcos de referencia son una especie de guía para realizar o implementar ciertas actividades, políticas o procesos en las empresas, tomando en cuenta que la ciberseguridad es un tema que se aplica en general, cada día se ponen al alcance de las empresas más grandes esta clase de documentos que sirven de apoyo, sin embargo, hay pocas conocidas que estén completamente orientadas a Pymes como tal.

Figura 20.

Conocimiento sobre marcos de referencia específicos para Pymes.



Fuente: Elaboración propia.

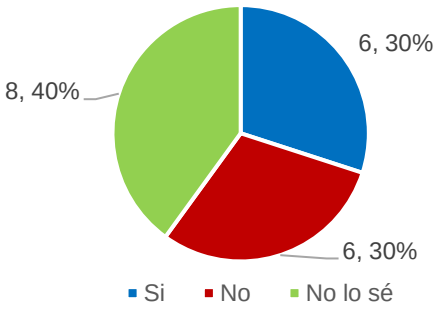
El análisis de esta pregunta infiere que la mayoría (19, un 95 % de la muestra) de las Pymes o colaboradores de esta no conocen de alguna guía para orientar el negocio en temas de ciberseguridad, una de las personas encuestadas confirma que tiene conocimiento de la existencia de una guía, sin embargo, esta no proveyó más detalles adicionales.

Pregunta #17

Como se ha venido mencionando, las políticas son uno de los pilares fundamentales que deberían de existir en toda organización, las mismas indican las formas apropiadas de realizar ciertos procesos o acciones, siendo así las instrucciones de los comportamientos esperados en la organización, habiendo dicho esto, el objetivo de esta pregunta es conocer si las Pymes aplican al menos una de las políticas más comunes en seguridad informática.

Figura 21.

Aplicación de políticas básicas de ciberseguridad.



Fuente: Elaboración propia.

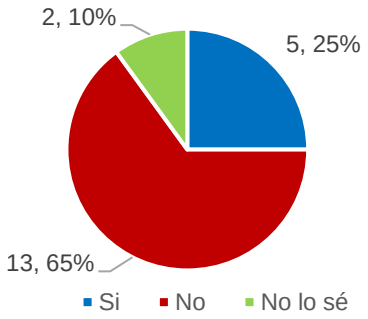
De las respuestas obtenidas se infiere que hay una falta considerable de información con respecto a las políticas básicas institucionales, debido a que un 30 % de los colaboradores encuestados desconocen, si existen o no esta clase de políticas, otro 30 % confirman que las mismas no existen en la empresa finalmente, el 40 % restante han llegado a afirmar que tienen conocimiento de su existencia y que en su empresa se aplican estas políticas.

Pregunta #18

Un gestor de contraseñas válido y licenciado debería de ser esencial para toda empresa que empiece a contar con distintos portales de acceso y cuentas, contar con esta clase de soluciones permite el almacenado seguro de las credenciales, evitando filtraciones de información confidencial, estos pueden ir desde los embebidos en dispositivos móviles hasta soluciones de navegadores, como *Kaspersky*, considerando que muchas Pymes pueden tener contraseñas relativamente sencillas porque son fáciles de recordar, al aplicar políticas más rigurosas para las credenciales una solución de esta índole se vuelve esencial, el objetivo de esta pregunta es conocer si las Pymes tienen esta clase de *softwares* dentro de sus herramientas.

Figura 22.

Uso de gestores de contraseñas.



Fuente: Elaboración propia.

Analizando las respuestas de los colaboradores se puede observar que tienen conocimiento de dicha solución sin embargo únicamente cinco de las 20 encuestadas cuentan con esta solución, 13 Pymes no tienen esta clase de *software* implementado y únicamente dos desconocen si existe un gestor dentro de su organización.

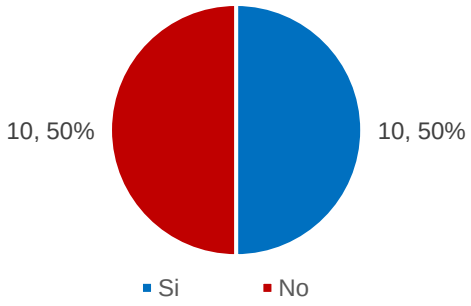
Pregunta #19, 20, 21 y 22

Algunas de las Pymes buscan crear páginas *web* o sitios electrónicos en los cuales los usuarios y clientes puedan apreciar su menú de servicios, historia entre otras, dichas aplicaciones

son esenciales mantener el servidor en el cual se ejecuta la lógica de la aplicación, esto debido a que los *hackers* o atacantes pueden encontrar este servidor en la *web* e intentar vulnerarlo, habiendo dicho esto, se detallan las preguntas relacionadas a servicios y aplicaciones propias de la empresa.

Figura 23.

Existencia de aplicaciones de la empresa.

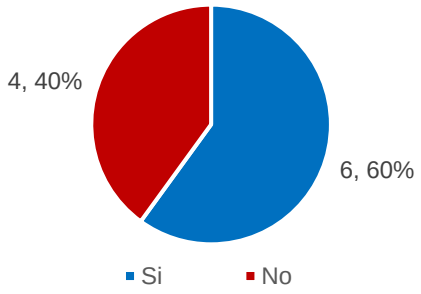


Fuente: Elaboración propia.

Del análisis de los resultados obtenidos mediante la aplicación de las encuestas en las Pymes se puede determinar que un 50 % de las encuestadas tienen al menos una aplicación móvil o una aplicación *web.*

Figura 24.

Recibimiento de soporte por los desarrolladores de la aplicación.

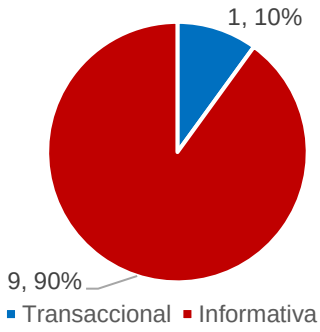


Fuente: Elaboración propia.

Del 50 % (diez) de las Pymes que cuentan con una aplicación, seis de ellas reciben un soporte activo del fabricante de la aplicación y cuatro de ellas no cuentan con esta clase de soporte o apoyo por parte de la persona o la empresa que desarrollo la aplicación.

Figura 25.

Tipo de aplicación desarrollada.

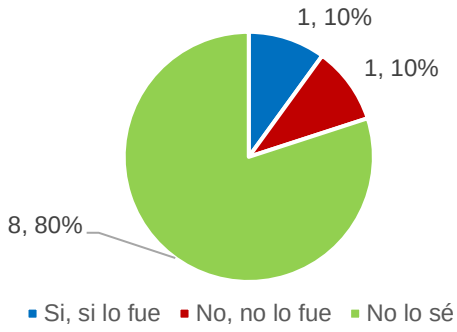


Fuente: Elaboración propia.

De esas Pymes con aplicaciones, un 90 % declaran que dichas aplicaciones son únicamente con un fin completamente informativo, en esta clase de páginas se detallan los servicios que estas proveen, y únicamente un 10 % (1) de las Pymes tiene una aplicación transaccional, por lo que en esta se pueden realizar pagos electrónicos de los servicios y productos.

Figura 26.

Realización de pruebas de penetración a la aplicación.



Fuente: Elaboración propia.

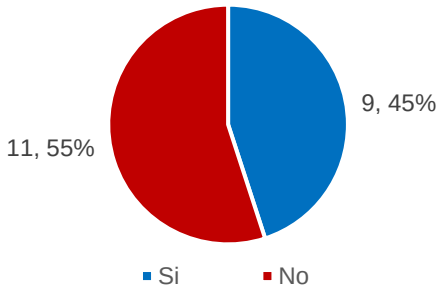
Finalmente, las aplicaciones deben ser sometidas ante pruebas de penetración ya sean dinámicas o estáticas, de esta forma se garantiza que dicha aplicación no pueda ser utilizada por un atacante para orquestar siniestros para obtener información, analizando los resultados obtenidos un 80 % (ocho) de las Pymes que cuentan con aplicaciones desconocen si su aplicación fue sometida a pruebas, y el 20 % restante se distribuye en una Pyme que realizo las pruebas y en otra que no.

Pregunta #23

Un área de TI o personal técnico encargado de realizar ciertas labores en relación con la parte más informática de la organización, estos se encargan de dar mantenimiento a los equipos, velar por el cumplimiento de algunas políticas relacionadas con contraseñas y realizar respaldos constantes de la información en los equipos de la organización.

Figura 27.

Existencia de personal de tecnologías de información.



Fuente: Elaboración propia.

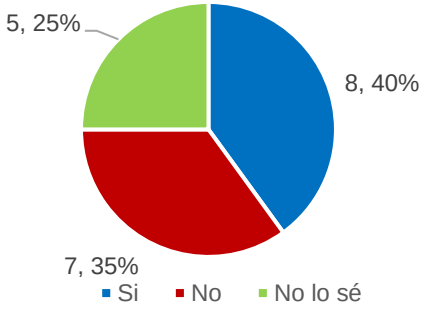
De los resultados recopilados durante la aplicación de este instrumento, se puede inferir que una gran parte de las Pymes no cuentan con esta clase de servicios ya que 11 (55 %) de ellas no cuentan con personal o un área que se encargue de realizar ciertas funciones informáticas, las nueve (45 %) restantes son Pymes de un tamaño más considerable que incluso optan por tercerizar esta clase de servicio, reconociendo la importancia de tener mantenimiento constante en sus equipos de red.

Pregunta #24

Parte importante de la ciberseguridad es el licenciamiento de todas las distintas soluciones utilizadas por la empresa, tener una licencia de *software* válida previene la necesidad de instalar algún tipo de *software* catalogado como “pirata”, en este se puede incluir programa maligno u otros archivos maliciosos inyectados por atacantes.

Figura 28.

Licenciamiento válido de software.



Fuente: Elaboración propia.

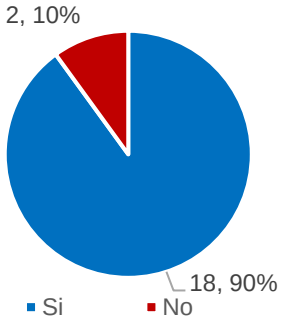
De los resultados obtenidos, ocho (40 %) de las Pymes encuestadas claman tener *software* completamente licenciado por parte del proveedor, siete (35 %) de ellas claman que no cuentan con aplicaciones legales y finalmente cinco (25 %) de ellas desconocen si tienen o no licencias válidas. Lo que permite determinar que existe una mala praxis con respecto a la forma en la que se instalan esta clase de aplicaciones, ya que no hay una conciencia apropiada de los riesgos que puede conllevar instalarlas.

Pregunta #25

La mayoría de las empresas cuentan con al menos una red interna ya sea mediante *WiFi* o conexiones cableadas, esta red es la utilizada para realizar ciertas acciones de forma segura, como lo son transferencias bancarias y demás actividades que deben permanecer completamente confidenciales.

Figura 29.

Existencia de una red interna.

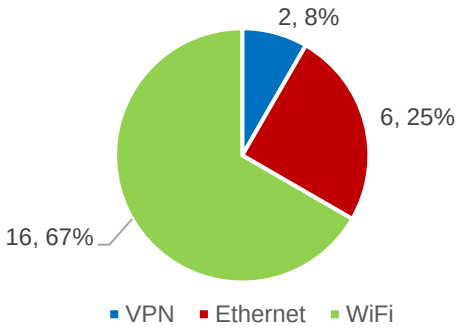


Fuente: Elaboración propia.

De esta pregunta se puede determinar que una gran mayoría de las Pymes cuentan con una red interna dentro de sus establecimientos, habiendo 18 (90 %) que cuentan con esta clase de implementaciones, dos de ellas, no lo hacen, sin embargo durante la realización de la encuesta una de ellas definió que la razón de esto es que se en el momento en el que se realizó esta encuesta están en un proceso de migración a la un sistema *cloud* para reducir costos de operación y han bajado los servicios momentáneamente.

Figura 30.

Formas de acceso a la red interna.



Fuente: Elaboración propia.

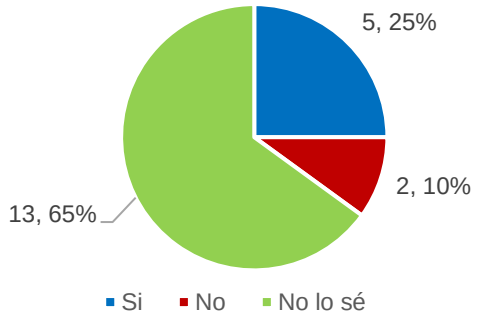
La pregunta #26 de selección múltiple, hace referencia a la forma en la que las empresas que cuentan con una red interna acceden principalmente a su red, donde 16 declaran que utilizan las *redes Wireless*, de esas mismas dos acceden mediante un servicio de VPN (conexión remota) y finalmente únicamente seis declaran que utilizan el *ethernet* como una alternativa.

Pregunta #27

Las políticas de "*hardening*" son principalmente orientadas a todas aquellas configuraciones que se aplican a los equipos con el fin de asegurarlos, esto incluye la aplicación constante de actualizaciones, contraseñas rotativas y seguras, entre otras cosas que se realizan para agregar una capa de seguridad adicional a los usuarios, datos y equipos.

Figura 31.

Políticas de "hardening" en activos informáticos.



Fuente: Elaboración propia.

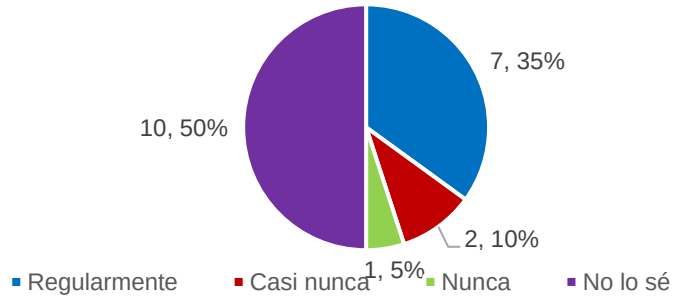
De las 20 Pymes encuestadas, según sus colaboradores, en cinco (25 %) se aplican esta clase de políticas de endurecimiento de servidores y demás equipos, dos (10 %) de ellas no aplican configuraciones seguras en sus equipos y finalmente los 13 (65 %) desconocen si su empleador se preocupa o bien aplica configuraciones recomendadas.

Pregunta #28

Los parches y actualizaciones en los equipos es una parte fundamental de la seguridad, esta es una práctica y cultura que se debe aplicar en profundidad desde que la empresa está en etapas de desarrollo e implementación, esto debido a que las migraciones "bruscas" de una versión a otra puede resultar en serios problemas de integridad de los datos e incluso de funcionalidades.

Figura 32.

Revisión y aplicación de parches y actualizaciones en equipos de software.



Fuente: Elaboración propia.

Analizando los resultados obtenidos se puede determinar que existe una clara falta de conocimiento del tema debido a que la mayoría de los encuestados (10, 53 %) declara que no

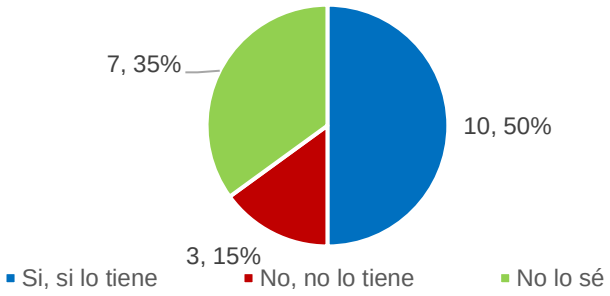
tienen conocimiento en sí, su empresa aplica dichas políticas de actualizaciones, sin embargo, siete (35 %) de estos saben que se aplican parches regularmente, dos (10 %) casi nunca aplican actualizaciones y finalmente una de ellas (5 %) declara que nunca se realiza este proceso de parcheado y actualización.

Pregunta #29

Un inventario es uno de los elementos principales en toda empresa, no solo de sus productos o servicios si no de sus activos tecnológicos, esto les permite a las empresas tener una trazabilidad de los equipos internos, quien tiene acceso a los datos y cuando corresponde revisar, cambiar o actualizar el elemento según corresponda.

Figura 33.

Existencia de inventario de activos informáticos.



Fuente: Elaboración propia.

Una gran mayoría de las Pymes conoce de la existencia de este inventario dentro de su organización, habiendo diez (50 %) de los encuestados que conocen del tema, únicamente tres (15 %) Pymes no cuentan con un inventario de los activos informáticos dentro de su organización y siete (35 %) de las personas consultadas no saben realmente si este tipo de documento existe en su organización.

Análisis de los resultados

La aplicación de las entrevistas fue sencilla debido a que los participantes tenían un verdadero y genuino interés en aportar valor a la guía, durante el desarrollo de estas todos los entrevistados hicieron énfasis en lo importante de que exista una clase de documento que sirve de apoyo para estos emprendimientos y distintas empresas en vías de desarrollo, así mismo dentro de su contenido lo principal rescatado de estas reuniones fue “la aplicación de políticas” y

la “concientización”, debido a que consideran que realmente el centro del problema radica en la falta de información.

Lo que fue posible observar durante la visita durante el desarrollo de las encuestas, deja mucho que pensar en aspectos de seguridad, debido a que existe una clara falta de cultura de ciberseguridad a nivel general, en una sociedad cada vez más digitalizada es importante tener la conciencia de que la forma en la que se protegen los activos de información puede tener repercusiones importantes a nivel de reputación, el uso de un gestor de contraseñas, la correcta localización de dispositivos de red o incluso un licenciamiento válido, que hablando de empresas relativamente pequeñas, no debería ser un costo tan alto como para no poder asumirlo.

De las encuestas se evidencia lo mencionado por los distintos profesionales entrevistados, una clara falta de información, capacitación y concientización por parte de las Pymes y sus colaboradores, adicionalmente, durante el proceso de desarrollo de estos instrumentos algunas de las respuestas brindadas por los colaboradores pueden sonar poco “honestas” debido a lo observado dentro este proceso, lo que confirma que, pese a que muchos conocen de ciberseguridad, pocos lo practican.

Finalmente se puede determinar con estos instrumentos, la importancia de crear una guía básica de ciberseguridad que sirva de base fundamental y de fuente de conocimiento para las empresas en vías de desarrollo, así como también la importancia de crear una cultura más profunda en las personas en general del valor que tiene la información en la “era digital”.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La ciberseguridad se ha convertido en un aspecto crucial en el mundo empresarial y su importancia se extiende en una sociedad más tecnológica, las pequeñas y medianas empresas o Pymes de Costa Rica no son ajenas a las amenazas y desafíos que esta sociedad trae, por lo que este proyecto se propuso cumplir con un objetivo general: desarrollar una guía de ciberseguridad básica que estableciera políticas y procedimientos destinados a proteger los activos de estas Pymes.

A lo largo de esta propuesta, se establecieron cuatro objetivos específicos con el fin de abordar aspectos clave en la ciberseguridad de las Pymes. Estos objetivos se centraron en la concientización y capacitación, la adopción de buenas prácticas y políticas, la planificación de la respuesta ante incidentes cibernéticos, y la promoción de la seguridad durante el proceso de desarrollo de *software.*

Con la finalización de esta propuesta, se han alcanzado con éxito todos los objetivos planteados inicialmente, construyendo una guía que permita mediante la aplicación de los controles desarrollados un avance significativo en el campo de la ciberseguridad para las pequeñas y medianas empresas (Pymes) en Costa Rica.

Se ha definido un proceso y una metodología apropiada para crear una campaña de concientización y capacitación para identificar ataques de ingeniería social como lo es el *phishing*. Este apartado le permitirá a las Pymes poder fortalecer la educación y concienciación de todos sus colaboradores, reduciendo así la probabilidad de que se materialicen los riesgos asociados a estos tipos de ataques, lo que cumple satisfactoriamente el objetivo detallado.

Se ha realizado un análisis en detalle de distintos marcos de referencia y buenas prácticas en seguridad informática como lo son *NIST y CIS*, incorporando los puntos más relevantes en la guía y adaptándolos a las necesidades y carencias reales de las Pymes, lo que garantiza que estas empresas tengan acceso a controles prácticos que puedan ser aplicables a su operación diaria, cumpliendo el objetivo planteado.

Se ha diseñado y creado una metodología para establecer un plan de recuperación y respuesta ante ataques informáticos específicamente orientado a este tipo de empresas, definiendo todas aquellas prácticas y métodos usados comúnmente, este plan proporciona un enfoque flexible para que la Pyme pueda identificar sus riesgos y establezca la forma apropiada

de enfrentarlos poniendo en práctica simulacros que las preparen en la respuesta a situaciones de crisis, minimizando el impacto del evento y mejorando la capacidad de respuesta y recuperación ante desastres informáticos, lo que cumple el objetivo específico.

Se han establecido exitosamente los conocimientos y las buenas prácticas que los desarrolladores de *software* de las Pymes deben considerar y adoptar durante el proceso de creación de las aplicaciones. Esto garantiza que se establezcan métricas y pruebas que son necesarias para un desarrollo seguro, como la aplicación de pruebas de penetración y guías de seguridad mundialmente reconocidas, cumpliendo el objetivo de la propuesta.

El Objetivo General de desarrollar una guía de ciberseguridad básica que establezca políticas y procedimientos orientados a la protección de activos dirigidos a las Pymes se ha logrado de manera efectiva. La guía desarrollada proporciona un marco sólido de referencia que puede ser utilizado para mejorar la postura y "cultura" de ciberseguridad en este sector empresarial.

Finalmente, esta propuesta ha logrado con éxito la creación de una guía de ciberseguridad básica, proporcionando a las Pymes de Costa Rica una herramienta integral para fortalecer su base y postura en ciberseguridad. Los Objetivos Específicos se han cumplido en su totalidad, de tal forma que para las empresas que lo pongan en práctica le contribuirá a la protección de los activos y a minimizar la probabilidad de que los riesgos se lleguen a materializar. En caso de que una Pyme opte por implementar esta guía dará un paso importante en la dirección de un entorno empresarial más seguro, capacitado y resiliente en el contexto de la ciberseguridad

Recomendaciones

Entendiendo que implementar marcos de referencia y madurez de ciberseguridad es un reto para cualquier empresa independientemente de sus ingresos o tamaño, contar con un compromiso al más alto nivel es requerido para impulsar la implementación de guías de esta clase, este debe ser un proceso escalonado y se debe de aplicar siguiendo un orden, estableciendo un programa o *roadmap* de implementación, estas actividades deben ser desarrolladas por el personal técnico y administrativo de la Pyme.

- En un supuesto escenario donde se comience con el programa de implementación en enero, 2024, con un compromiso adecuado y personal técnico se puede decir que podría proyectar de 8 a 16 meses de duración.

- Inicialmente se debe empezar por el punto “Responsables y Roles” el cuál puede tomar aproximadamente de 1 a 3 meses.
- Seguidamente por “Políticas y Buenas Prácticas” este puede tener una duración de dos a cuatro meses.
- Después por el punto “ILR – 1. Inventariado de Activos” del apartado “Inventario, Legitimización y Respaldo de Activos” para posteriormente considerar los puntos de “Análisis e Identificación del riesgo” específicamente los uno y dos, considerando que una Pyme puede que no tenga tantos activos de información este proceso puede tomar de dos a cuatro meses.
- Continuar con la implementación de los puntos faltantes de “Inventario, Legitimización y Respaldo de Activos”, este proceso puede demorar dos meses.
- Analizar los puntos de “AR – 2. Identificación de los Riesgos”, con una duración de uno a tres meses.
- Implementar los puntos de “Plan de Capacitaciones”, crear este material e impartirlo puede tener una duración de uno a dos meses.
- Concluidos los puntos de identificación de riesgos se deben de establecer las bases de “Recuperación a Ataques y Desastres informáticos”, lo que puede durar aproximadamente de seis a siete meses, con recursos dedicados a este análisis.
- Los puntos abarcados en “Vulnerabilidades y Parámetros en Aplicaciones Móviles y Web” pueden irse implementando en paralelo a otras actividades, debido a que los desarrolladores pertenecen a otro nivel técnico que el personal de TI.
- Finalmente, los puntos restantes de “Análisis e Identificación del riesgo”, que miden la eficacia y eficiencia de los controles implementados, este proceso puede demorar de unos a cuatro a cinco meses debido a la complejidad de estas evaluaciones y no son necesariamente una prioridad para las Pymes con menor nivel de ingresos, adicionalmente estos puntos pueden aplicar más a un tercero.
- Como consideraciones, muchos de estos puntos pueden realizarse de forma paralela, lo que podría agilizar el programa. Los tiempos establecidos son una estimación promedio, que varía de acuerdo con el tamaño, esfuerzo y recursos de cada organización.

Si bien algunos de los controles en la guía implican un costo económico, afrontarlos es completamente opcional, hay muchas alternativas gratuitas que pueden ser evaluadas antes de adquirir licencias o servicios, estos procesos de adquisición de *software* y *hardware* pueden demorar aproximadamente uno a dos meses, debido a que esto involucra a un tercero a la organización, y este proceso debe de ser realizado por personas con cargos administrativos que gestionen las relaciones con los proveedores.

Es recomendable aplicar medidas de protección adicionales como *firewalls* y *hardening* en todos los equipos de red, principalmente los que están públicos al internet, estas acciones deben de ser supervisadas por personal técnico y aplicar estas medidas pueden demorar de uno a dos meses, algunos de los puntos requieren de cierto nivel técnico de conocimientos, especialmente los orientados a respuesta a incidentes y configuración de políticas de equipos, si la Pyme no cuenta con este personal o infraestructura interna estos puntos pueden ser omitidos momentáneamente hasta que se puedan abordar.

Cada punto y familia de controles tienen un distinto enfoque, por lo que es importante alinear las necesidades del negocio al programa de implementación y ajustarlo según corresponda, considerando siempre que la implementación de algunos de estos puntos puede tener una duración variable de unos tres meses, según el esfuerzo aplicado y personal técnico y administrativo asignado, este enfoque, debe de ser principalmente analizado por el director general de la empresa y los gerentes o jefes de área de tecnología de información y ciberseguridad.

CAPÍTULO VI: PROPUESTA

Durante la completitud de este capítulo, se detallarán y desarrollarán todos aquellos puntos importantes definidos anteriormente en la propuesta, dando lugar a la guía preventiva básica de ciberseguridad aplicable dentro de las Pymes de Costa Rica.

UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS
ESCUELA DE INGENIERÍA INFORMATICA

Proyecto de graduación

Para optar por el grado de Bachillerato en Ingeniería en Sistemas de Información

Propuesta de una Guía de Ciberseguridad Preventiva básica en empresas Pymes de Costa Rica

Isaac José Villalobos Torres

AUTOR

Carlos Humberto Aguilar Mora

TUTOR

Daniel Álvarez Garro

LECTOR

San José, Costa Rica

Noviembre, 2023

CONTENIDO

Introducción

En una era digitalizada y con avances muy constantes beneficiosos en la tecnología, se empiezan a crear y generar nuevas superficies de ataques y vectores de ataque, por lo que es importante adoptar una nueva postura más defensiva con los datos personales y empresariales, pese a que todos los días distintos proveedores de servicios están en una investigación y desarrollo constante por mejorar y detectar fallas en aplicaciones y servicios, de nada sirve si no existe una debida "cultura" de cuidado de la información, tomando en cuenta que los vectores principales de un atacante es mediante la aplicación de técnicas de ingeniería social, esto les permite acceder a las redes a través de un descuido de un usuario y estos usualmente se deben a la falta de capacitación y conciencia.

Esto da como resultado que cada día se desarrollen nuevas metodologías y guías que las empresas pueden ir adoptando, para resguardar su información de forma segura y apropiada, sin embargo, su aplicación requiere de un nivel de infraestructura e incluso de personal técnico que son validadas continuamente por equipos de ciberseguridad por medio de evaluaciones o auditorías de seguridad. Estas pruebas y procesos de acompañamiento pueden llegar a tener costos muy elevados, lo que las hace realmente inaccesibles para muchas empresas, dejando a las empresas clasificadas como Pymes sin un asesoramiento en temas de ciberseguridad.

Propósito

Lo esperado de esta propuesta o investigación es que sea utilizada como un marco de referencia inicial en ciberseguridad completamente gratuito dirigido a las Pymes en Costa Rica, con el objetivo principal de que personas sin un conocimiento precisamente técnico puedan usarla como una guía de implementación de buenas prácticas de ciberseguridad, desde etapas tempranas de la empresa, hasta que esta pueda costear o cumplir con los requerimientos de una asesoría o evaluación de normas más avanzadas como la ISO 27001 o el *CyberSecurity Framework de NIST.*

Beneficios

Uno de los principales objetivos de esta propuesta es servir como una guía de conocimiento sobre la cual las Pymes puedan basarse para construir sus políticas y procedimientos en torno a una cultura de seguridad desde tempranas etapas de desarrollo, de forma que estas implementaciones se den de forma escalonada, empezando con aspectos

considerados básicos, a continuación, se mencionan algunos de los beneficios esperados de esta propuesta:

- Agilidad y sencillez: Implementar muchos de los puntos de esta guía no requiere de un nivel de conocimiento avanzado en tecnologías de la información, debido a que uno de sus principales focos es que pueda ser aplicado y utilizado por cualquier persona con un nivel bajo o intermedio en informática.
- Costos: El gasto por aplicar algunos de estos puntos claves es considerado bajo, ya que los costos en los que se vaya a incurrir para el cumplimento de la guía en su mayoría son opcionales e incluso algunas de las soluciones mencionadas pueden llegar a ser gratuitas, la adquisición de licencias pagas, queda completamente a criterio de la Pyme.
- Conocimiento: La información recopilada en la guía puede darle al lector una forma clara de comprensión de todos aquellos puntos que son esenciales conocer para inculcar esta cultura de ciberseguridad en la vida personal o en un entorno laboral.
- Practicidad: La presente guía busca crear un repositorio centralizado para la búsqueda de información, así como guiar en la aplicación de buenas prácticas y configuraciones seguras, centralizar todos aquellos puntos primordiales que deben ser tomados en cuenta, puede facilitar la "digestión" de la información.
- Buenas prácticas: Utilizando algunas de las guías más importantes de seguridad como las normativas ISO, NIST y CIS se pretende que la información, controles y puntos claves detallados en esta propuesta sean similares y alineados con dichas guías, pero aplicados a una menor escala, siendo así más accesible.
- Otro punto de vista y enfoque: Esta propuesta es creada principalmente desde el punto de vista del autor y su experiencia como auditor de sistemas, ejecutor de pruebas técnicas, consultor de ciberseguridad y cazador de vulnerabilidades informáticas (Programas de "*Bug's Bounty*"), lo que da una perspectiva de cómo piensa un atacante real y cuáles son los puntos sobre los cuales este dirige su atención durante una evaluación.

Objetivos

Objetivo General

- Desarrollar una guía de ciberseguridad básica que establezca las políticas y procedimientos de ciberseguridad orientados a la protección de los activos dirigido a las pequeñas y medianas empresas de Costa Rica.

Objetivos Específicos

- Definir el proceso adecuado para crear una campaña de concientización y capacitación para ataques orientados a ingeniería social.
- Analizar distintos marcos de referencia y las buenas prácticas, políticas y procedimientos organizacionales de seguridad informática incluidos en ellos.
- Diseñar un plan de recuperación y respuesta para las Pymes en caso de un ataque informático.
- Establecer los conocimientos y buenas prácticas que los desarrolladores de software de las Pymes deben de tener en cuenta durante el proceso de desarrollo de una aplicación web o móvil.

Proyecciones

Se espera que esta propuesta pueda convertirse en un marco de referencia de ciberseguridad para las Pymes de Costa Rica en general, ya que muchos de los temas abarcados en esta guía se verán de forma general para alcanzar y contemplar a la mayor cantidad de Pymes posibles, entre sus beneficios el principal sería servir de apoyo para agregar una capa de seguridad adicional a esta clase de empresas y servir de fuente de conocimiento para el entendimiento de algunos conceptos utilizados en el área de la ciberseguridad optimizando y reforzando su forma de pensar y de actuar.

Adicionalmente se busca que las Pymes creen una cultura de seguridad informática y de riesgos cibernéticos desde etapas tempranas de desarrollo, aprendiendo a valorar la información utilizada internamente y el daño que puede realizar una simple acción desinteresada o descuidada, así como incentivar la aplicación de capacitaciones obligatorias y de interpretación de las políticas, entre otras.

Alcance Funcional

Dentro de los entregables finales de esta propuesta se encontrará la guía, la cual contendrá información relevante sobre las políticas y procedimientos que pueden ser de utilidad en una pyme de Costa Rica, algunos de los apartados que se incluirán son:

- Manejo apropiado del riesgo de una amenaza informática: Se creará una matriz de riesgos que las Pymes puedan utilizar con el fin de clasificar riesgos a los que están expuestas, definiendo así un top diez riesgos más comunes presentes en las Pymes y cómo responder apropiadamente siguiendo las cuatro formas detalladas en *CompTIA*.

- Inventario de Tecnología y priorización de activos: Desarrollar una metodología para crear un inventario de *software y hardware* basado en el foco de negocio de la empresa que les permita determinar y priorizar los activos y datos críticos para el negocio que deben ser protegidos.
- Responsables de gestionar la información: En este apartado se desarrollará una guía para crear una matriz RASCI, con el fin de definir los roles internos de las empresas para cada proceso que se realice.
- Plan de capacitaciones de ataques de ingeniería social: Definir un proceso de capacitación dirigido al personal de las Pymes a fin de que mediante la aplicación de las mejores prácticas estén en capacidad de identificar ataques de ingeniería social como *vishing*, *phishing* y otros que pongan en riesgo su operación.
- Respaldos de la información: Desarrollar la metodología de un proceso adecuado para el respaldo de la información, identificando:
    - ¿Quién debe de hacerlo?
    - ¿Cuándo debe hacerse?
    - ¿Cómo debe hacerse?
    - ¿Qué debe de respaldarse?
- Legitimización de activos: Crear un procedimiento de adquisición y mantenimiento de *software y hardware* utilizado por las Pymes (Paquetes de Office 365 y máquinas como computadoras o servidores).
- El uso apropiado de cuentas de la Pyme: Crear un procedimiento para manejar información confidencial de la empresa (contraseñas, PII, cuentas…) según NIST y definir políticas seguras de contraseñas y accesos implementando los principios de *least privilege* y *need-to-know de CompTIA.*
- Buenas prácticas informáticas: En este apartado se desarrollarán todas aquellas prácticas seguras utilizadas comúnmente en las áreas de TI, con el fin de mejorar la postura de ciberseguridad de las pymes.
- Evaluación de vulnerabilidades: Crear un proceso de evaluación de vulnerabilidades interno para las pymes, para evaluar la efectividad de los controles, políticas y procedimientos internos mediante cuatro fases:
    - Identificación de vulnerabilidades.

    - Análisis de las vulnerabilidades.
    - Priorización de activos (tomando en cuenta el inventario organizacional)
    - Remediación de vulnerabilidades.
- Plan de recuperación de ataques informáticos: Desarrollar un plan que permita a una pyme recuperarse de un incidente informático según el tipo de negocio al que este orientado.
- Vulnerabilidades en aplicaciones web y móviles según OWASP: Crear parámetros defensivos para que el desarrollador los aplique en el desarrollo seguro de aplicaciones.
- Análisis de código estático y dinámico y su importancia: Desarrollar una metodología para desarrollar pruebas sencillas para evaluar la seguridad del código dinámico y estático basándose en la *WSTG v4.2 de OWASP,* (donde se evalúan ataques como *Cross Site Scripting*, *SQL Injection*, *Clickjackin*g …).

Todos estos apartados o módulos son tomados en consideración debido a que son los principales fallos detectados en empresas más grandes y maduras, inclusive que una pyme, por lo que durante el desarrollo de la guía se procederá a detallar estos apartados con los pasos para que los mismos se puedan desarrollar con éxito durante el proceso de implementación por parte del ingeniero o el personal asignado para la tarea, además de mantenerse lo más simple posible para evitar posibles problemas de comprensión.

Alcance Metodológico

Los insumos utilizados para desarrollar la propuesta son marcos de referencia o estándares como CIS, NIST y para los conceptos a modo más general se utilizará un *e-book de CompTIA*, el cual incluye información relevante y actualizada, esto con el fin de obtener la mayor cantidad de información posible, adicionalmente se incluirán referencias a la ISO 27001 y 27002, estas con el fin de evaluar los controles indicados en el marco de trabajo de NIST *Cybersecurity Framework* y utilizarlos como referencia para evaluar su ajuste a una empresa Pyme.

Alcance Tecnológico

Para la implementación de esta propuesta, no se requiere alguna especie de requerimiento técnico, ya que la misma buscará trabajar con los recursos tecnológicos con los que cuenten estas

empresas, sin embargo, dentro de los sistemas y elementos utilizados más comúnmente en Pymes se encuentran:

- Sistemas POS (*Point of sale*), usualmente estas vienen acompañadas de un sistema de inventariado como lo es *Alegra*.
- Servidores EC2 de AWS.
- Computadoras de escritorio.
- *Laptops y* equipos de red.
- Licencias de Microsoft y Office 365.
- Licencias de antivirus como Kaspersky, Avast, Sophos.
- Una solución de *firewall*, como *PfSense* o algún otro sistema de WAF (*Web Application Firewall*) como los provistos por cloudflare.

Nomenclatura y Contenido

Con el fin de identificar fácilmente los puntos abarcados dentro de la guía, se procederá con su desarrollo según su función o categoría, de acuerdo con lo presente en la tabla No. 6.

Tabla 6.

Definición de las categorías de los tipos de controles y puntos claves (PC)

Identificador	Definición	PC/ Controles
AR - #.	Análisis e identificación del riesgo	**6**
ILR - #.	Inventario, legitimización y respaldo de activos	**6**
RAC - #.	Responsables y roles	**3**
CAP - #.	Plan de capacitaciones	**2**
POL - #.	Políticas y buenas prácticas	**11**
RES - #.	Recuperación a ataques y desastres informáticos	**3**
WEB – #.	Vulnerabilidades y parámetros en aplicaciones móviles y web	**4**
TOTAL, Puntos clave		**33**

Fuente: Elaboración propia.

Análisis e Identificación del riesgo

Antes de definir una estrategia de seguridad es recomendable establecer un mecanismo para el manejo y medición del riesgo, definiendo el riesgo como un posible evento al cual está expuesto un individuo o entidad y que puede llevar a consecuencias como perdida de información o reputación. Por lo que identificar los posibles riesgos a los cuales están expuestas las organizaciones es un paso primordial en el negocio.

AR – 1. Matriz de Riesgos

Objetivo.

a) Utilizar una matriz de riesgo para la clasificación de este determinando el valor del siniestro mediante la probabilidad y el impacto si este llega a materializarse.

Procedimiento.

a) Tener claro el funcionamiento de una matriz de riesgos es esencial para su identificación. En relación con las Pymes se utilizará una matriz de 5 x 5, donde se define el valor riesgo, que se calcula mediante su probabilidad y el impacto.
    a. Una matriz de riesgos es un mapa de calor utilizado para identificar la criticidad o el valor del riesgo mediante la fórmula de "Riesgo = Probabilidad x Impacto" y es comúnmente utilizada como un apoyo para determinar la forma en la que se abordara el riesgo analizado (Obsérvese tabla No. 7.).

Tabla 7.

Matriz de riesgo (5x5)

Probabilidad \ Impacto	Bajo (1)	Menor (2)	Medio (3)	Alto (4)	Crítico (5)
Muy alta (5)	Menor (5)	Medio (10)	Alto (15)	Crítico (20)	Crítico (25)
Alta (4)	Bajo (4)	Menor (8)	Medio (12)	Alto (16)	Crítico (20)
Media (3)	Bajo (3)	Menor (6)	Medio (9)	Medio (12)	Alto (15)
Menor (2)	Bajo (2)	Bajo (4)	Menor (6)	Menor (8)	Medio (10)
Baja (1)	Bajo (1)	Bajo (2)	Bajo (3)	Bajo (4)	Menor (5)

Fuente: Elaboración propia.

a) Habiendo detallado la matriz de riesgo, es importante definir sus componentes.
    a. Probabilidad: Definir si es posible que se materialice el riesgo.
    b. Impacto: Magnitud y consecuencias de la materialización del riesgo.
    c. Riesgo: Evento o siniestro al cual se considera que hay una exposición.
    d. Valor del riesgo o criticidad: Como su nombre lo indica es el valor que adquiere el riesgo al haber sido analizado en la matriz, teniendo cuatro posibles valores, bajo (1 - 4), menor (5 - 8), medio (9 - 14), alto (15 - 19) y crítico (20 - 25).
b) Asignar el valor de la probabilidad y el impacto son temas subjetivos, por lo que se debe tomar en cuenta el análisis realizado durante la discusión del punto "AR – 2. Identificación de los Riesgos" para asignar una calificación o un valor al riesgo.

AR – 2. Identificación de los Riesgos

Objetivo.

a) Identificar los riesgos a los cuales está expuesto la Pyme, reflejando la situación actual de la empresa
b) Listar dichos riesgos para su posterior clasificación y gestión, algunos de estos riesgos pueden tener impactos económicos, esto también debe ser incluido.

Procedimiento.

a) Identificar el riesgo:
    - Este punto se debe realizar en conjunto con las personas con roles de administrador y directivos de la empresa.
    - Se deben discutir cuáles son los riesgos a los cuales están expuestos como empresa y deliberadamente determinar qué tan probable es que este evento se materializa y cuál es el efecto que tendría sobre la empresa, estos eventos pueden incluir Desastres naturales, robos de información, ataques informáticos y estafas telefónicas y electrónicas
b) Determinar la forma en que se abordará dicho riesgo, detallado en el punto: "AR – 3. Manejo del Riesgo".
c) Definir cuál es la probabilidad o la ocurrencia en la cual se puede materializar el riesgo.
d) Definir cuál es la magnitud del posible impacto si se llega a materializar el riesgo.

e) Asignar una calificación o valor al riesgo

f) Construir un documento de identificación y manejo de riesgo.

Tabla 8.

Estructura propuesta para un documento de identificación de riesgo

Riesgo	Probabilidad	Impacto	Criticidad	Respuesta	Acciones	Estado

Fuente: Elaboración propia.

Donde:

- Riesgo: Evento o siniestro al cual se considera que hay una exposición.
- Probabilidad: Valor de la ocurrencia del riesgo, se puede extraer del análisis realizado en la matriz de riesgo.
- Impacto: Valor de la magnitud o consecuencias relacionadas con el riesgo, se puede extraer del análisis realizado en la matriz de riesgo.
- Criticidad: Valor del riesgo se puede extraer del análisis realizado en la matriz de riesgo (Probabilidad x Impacto = Criticidad/Valor del riesgo).
- Respuesta: Determinar cómo se manejará el riesgo.
- Acciones: Definir cuáles serán las medidas que se deben tomar.
- Estado: Determinar el estado del riesgo (1. Sin empezar 2. En proceso 3. Tratado).

AR – 3. Manejo del Riesgo

Objetivo.

a) Realizar un manejo apropiado de los riesgos, e identificar cuáles son las distintas formas de tratarlo.

Procedimiento.

a) Identificar las formas para manejar apropiadamente el riesgo: según Weiss (2020) hay cuatro formas de manejar el riesgo al cual está expuesta la organización.

- Evitarlo: Probablemente es una de las opciones más factibles, al identificar un riesgo se puede tomar la decisión de simplemente evitarlo como se pueda, sin embargo, mantener la evasión de riesgos puede ser un trabajo arduo el cual se debe complementar con capacitación constante, configuraciones seguras y políticas robustas según donde se identifique el riesgo.

i. Ejemplo de una acción evasiva: riesgo: Exposición de los equipos al público, medida tomada: Evitar dejar equipos importantes sin protección o vigilancia alguna.

- Transferirlo: al transferir esta clase de sucesos, la Pyme ya no se hace responsable por mantenerse segura contra el riesgo si no que delega esta responsabilidad a un tercero, otra entidad que se hará cargo de evitar que se del evento, sin embargo, esto no quiere decir que no vaya a poder tener un impacto en la empresa, debido a esto las empresas deben tener claro a quién designan esto, y previamente realizar un estudio del mercado para escoger una opción financieramente aceptable.
    i. Un ejemplo de transferencia es: riesgo: La posibilidad de un incendio en el edificio de la empresa, medida tomada: Asegurar el edificio si es propio o bien asegurar los equipos de mayor valor alojados en él.
- Aceptarlo: Cuando el riesgo no tiene un impacto tan severo (limitado únicamente a aquellos identificados con una criticidad baja (1 y 4) según los niveles definidos en el punto "**Error! Reference source not found.**") o no hay una verdadera forma de mitigarlo, transferirlo o evitarlo en la organización es posible asumir este riesgo y las responsabilidades que este conlleva, por lo que se deben tomar todas aquellas acciones posibles para evitar que este se materialice.
    i. Ejemplo de una acción de aceptación: riesgo aceptado: Colaboradores con acceso a su cuenta corporativa de correo electrónico.
- Mitigarlo: Como su nombre lo indica, esto implica solucionar completamente el riesgo, dependiendo del riesgo se deben aplicar distintas formas o controles compensatorios como soluciones *software,* respaldos, entre otros.
    i. Ejemplo de una acción de mitigación: riesgo: Equipos de *Windows* desactualizados, medida tomada: Actualizar dichos equipos.

b) Discutir qué acciones serán tomadas para manejar dicho riesgo y definirlo en el documento.

Una vez comprendidas las formas de manejar el riesgo, en el "documento de riesgo" se deberá detallar cuál será la forma de abordar los riesgos identificados previamente, así como

indicar cuáles serán las medidas y acciones que se tomarán para que el manejo del riesgo sea completo y válido, un ejemplo de esto sería el siguiente: Si se decide que se transferirá un riesgo, indicar, quién o qué entidad se hará cargo, los acuerdos tomados al abordar el tema y el alcance de lo que gestionarán los terceros.

AR – 4. Evaluación de Vulnerabilidades

Objetivo.

a) Guiar a la persona encargada de realizar la evaluación sobre una forma de hacer una evaluación de vulnerabilidades.
    - Establecer una medida de controles establecidos a nivel técnico, procesos y políticas.

Procedimiento 1: Evaluación y Auditoria de Equipos y *Software.*

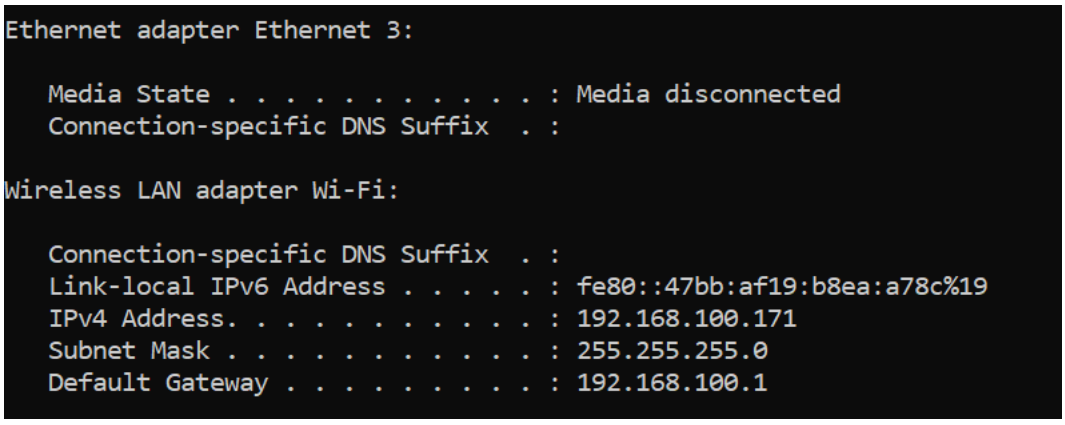
a) En alguna máquina, configurada seguramente (preferiblemente con un sistema operativo de *Windows 10* en adelante) instalar un s*oftware* que permita identificar vulnerabilidades.
b) Seguir los pasos de instalación según el *software* elegido, donde para la referencia:
    - *Nessus Professional*: Es uno de los analizadores de equipos más reconocidos y utilizados mundialmente, posee una de las bases de datos de vulnerabilidades más grandes que hay, sin embargo, es una herramienta que requiere de un licenciamiento pagado, debido a esto existe la versión "*Trial"* que permite analizar hasta 14 equipos de red.
    - *OpenVas GreenBone*: Es un analizador de vulnerabilidades gratuito, conocido en el mundo del "*Ethical hacking",* debido a que no implica un costo adicional para las empresas, sin embargo, su instalación y uso es más complejo y menos intuitivo, además de contar con una base de datos más limitada.
    - *Nmap:* Realmente es un analizador de puertos, por lo que indica puertos abiertos en los equipos y los servicios que estos corren, este cuenta con una función de analizador de vulnerabilidades, es completamente gratuito, rápido y versátil, con la única consideración de que su uso puede ser un poco más complicado ya que es más técnico, que los demás analizadores.

c) Una vez instalado el analizador, se debe estudiar cómo se utiliza, para esto se puede referir a sus guías de uso, sin embargo, el principal insumo que necesitan estos *softwares* es el identificador de la red, para simplificar este proceso, se recomienda conectar el equipo de la instalación en la red de internet donde se encuentren los equipos por evaluar, de forma que:

- Si se sabe que todos los equipos están conectados a una red *WiFi* o red cableada específica, se conecte el equipo a esta.
- Una vez conectada, a la red, ocupamos el identificador de la red, para esto es necesario abrir una consola de comandos en el equipo y digitar el siguiente comando *Windows:* `ipconfig` o bien en sistemas operativos *LINUX/UNIX* `ifconfig` o su equivalente en el equipo utilizado.

Figura 34.

Ejecución de ipconfig en un equipo de red



Fuente: Elaboración propia.

- De la imagen anterior, es importante identificar los datos del "*Subnet Mask*", "IPV4 Address" y "Default Gateway" donde el primero corresponde al tamaño de la red, el segundo al identificador único del equipo en la red y el ultimo al identificador único del *router.*
- En muchos casos, si no existe una segmentación de red es posible cambiar el último número (N) del identificador por 0, de forma que (X.X.X.0).
- El valor de "*Subnet Mask*" es lo que le indica al analizador cuán grande es la red y cuántos equipos debe evaluar, este valor en los equipos viene por lo general en esta estructura: 255.255.255.N. donde el último octeto (N) indica la cantidad de equipos que pueden estar conectados en la red (si el valor es 0, quiere decir que puede haber 255 equipos conectados simultáneamente), esto tiene otra forma de identificarse, "/NN" donde las N, corresponden a un numero de *máscara de subred,* para esto se puede referir a la tabla No. 9.

Tabla 9.

Tabla de subredes comunes en Pymes.

Mascara de red	Identificador	Cantidad
255.255.255.128	/23	128
255.255.255.0	/24	255
255.255.254.0	/25	512

Fuente: Elaboración propia.

d) Una vez identificado la subred, en el analizador se debe colocar la red que se quiere evaluar de la siguiente forma "X.X.X.0/NN".

e) Se puede leer la documentación del fabricante para configurar el analizador con distintos parámetros.

- Ejecutar la evaluación de vulnerabilidades, cada uno de los registros de resultados irán agrupados según la IP o identificador de red correspondiente del equipo, por lo que es importante mantener un inventariado correcto de equipos (véase "ILR – 1. Inventariado de Activos").

Estos procedimientos pueden variar, por lo que es aconsejado realizar estas autoevaluaciones técnicas, con el acompañamiento de una persona con cierto conocimiento básico en sistemas o bien buscar asesoría en fuentes de internet, si estos conceptos se vuelven muy complejos.

Procedimiento 2: Evaluación de Políticas, Controles y Procedimientos (Evaluación de madurez).

a) Esta clase de evaluaciones, conocidas también como evaluaciones de madurez se hacen para evaluar la seguridad, congruencia y el cumplimiento de las políticas y procedimientos internos establecidos por la empresa.
b) Se deben identificar y mapear todas las políticas y procedimientos asociados creados por la empresa.
    - Políticas de manejo de datos e información.
    - Políticas de *hardening* o endurecimiento de equipos.
    - Procedimientos de contratación y liberación de personal.
    - Procedimientos para la adquisición de licencias.
    - Contraseñas por defecto en equipos de red, o portales de gestión de cámaras de seguridad.
    - Políticas de uso aceptable.
c) Los controles por evaluar (Políticas en su gran mayoría) deben de ser analizados para corroborar que en efecto se alineen con lo indicado en la guía, si la empresa cumple con un aproximado de un 75% de los rubros establecidos en las políticas se considera que tiene un buen nivel de madurez en temas de ciberseguridad organizacional, sin embargo, es recomendable estar arriba del 90%. Donde el nivel de madurez se puede medir en cuartos porcentuales, de forma que para las Pymes se pueden definir los siguientes niveles:
    - 25% - Madurez Baja / Recién empezado.
    - 50% - Madurez Intermedia / Carencia y deficiencia de controles.
    - 75% - Madurez Aceptable / Proceso de mejora
    - 90% - Madurez Ideal
d) Aplicar cuestionarios u otros instrumentos a los colaboradores técnicos sobre los activos que crean que es prioritario analizar.
e) Analizar internamente, con un equipo de administradores el cumplimiento de las políticas.

f) Revisar el funcionamiento y estado de controles lógicos (Subredes, *Firewall, Antivirus*, etc.) y físicos (Cámaras, muros, bitácoras, alarmas o sensores) establecidos por la empresa.

Consideraciones.

a) Las evaluaciones de madurez aplican a Pymes con cierta posición en el mercado, ya que deben de contar con experiencia en su área, contar con personal técnico calificado, infraestructura a nivel interno y externo y la soltura económica para establecer un presupuesto definido para evaluaciones de seguridad, las Pymes consideradas “no aptas” o que no puedan aplicar esta clase de pruebas, pueden utilizar los apartados definidos en la propuesta para irse perfilando con un buen nivel de ciberseguridad, dentro de lo posible.

b) Esta clase de evaluaciones “autorrealizadas” son buenas prácticas organizacionales que pueden permitir incrementar y aplicar capas de seguridad en donde se necesite, siendo un medidor para revisar los controles aplicados , sin embargo, conforme la empresa o Pyme realice alianzas estratégicas, negocios de alto nivel e incluso opte por certificaciones organizacionales (como la norma ISO de calidad o de ciberseguridad) puede que se soliciten evaluaciones de una empresa de seguridad tercerizada, garantizando que los resultados sean válidos y legítimos.

c) Estas revisiones del procedimiento #1 también son provistas por muchas empresas bajo el nombre de “pruebas de penetración”, sin embargo, el elevado precio de estas puede resultar en una limitante, hasta que la Pyme empiece a generar más ingresos y logre cierta estabilidad en el mercado.

AR – 5. Análisis, Priorización y Remediación de Vulnerabilidades

Objetivo.

a) Analizar y categorizar las distintas vulnerabilidades resultantes del “AR – 4. Evaluación de Vulnerabilidades” para su posterior mitigación.

- En conjunto con la identificación y manejo de riesgos.

Procedimiento.

b) Una vez concluidas las evaluaciones de vulnerabilidades, estás deben ser categorizadas según corresponda en el documento de identificación de riesgos, sin embargo, las vulnerabilidades a nivel de *software* pese a que representan un riesgo,

son tratadas de una forma distinta a la hora de obtener su “valor de riesgo” o criticidad para esta clase de riesgos se utiliza el CVSS, (*Common Vulnerability Score System*) postulado por FIRST.

- Hay cuatro posibles clasificaciones para cada vulnerabilidad, Bajo, Medio, Alto y Crítico, su valor numérico se representa en una escala del 1 al 10, según el CVSS en su versión 3.1, estos valores son: bajas 0.1 - 3.9, medias 4.0 - 6.9, altas 7.0 - 8.9 y las criticas 9.0 - 10.0.

c) Su probabilidad es un dato más complicado de obtener sin un conocimiento técnico en el área de “pentesting”, por lo que se pueden indicar, que no corresponde, para el CVSS el impacto y el valor del riesgo pueden llegar a significar lo mismo.
d) En el documento de identificación de riesgos, se debe agregar el dato de los equipos afectados en caso de serlo así para tener una mejor visibilidad de los activos expuestos al riesgo o afectados por la vulnerabilidad.
e) Al concluir la identificación de riesgos se deben realizar procesos de validación de la vulnerabilidad y comenzar con la clasificación de cómo se manejará el riesgo siguiendo lo mencionado en controles anteriores.
f) Al iniciar los esfuerzos de remediación de vulnerabilidades se deben tomar en cuenta dos factores claves, el valor del riesgo, e identificar cuáles activos o cumplimientos son de principal importancia para el negocio.

- Por ejemplo: Se realizo una evaluación de vulnerabilidades y los resultados son un servidor con la página *web* informativa de la empresa (público en internet) presenta una vulnerabilidad catalogada como alta y además hay una computadora exclusivamente de uso interno con una crítica. El análisis apropiado de esta situación es:
    i. La página *web* y el servidor están expuestos al público, lo que quiere decir que cualquier persona con conexión podría acceder al sitio y al servidor.
    ii. Para que una explotación en la computadora sea exitosa, el atacante debe estar ubicado internamente en la red de la Pyme.
    iii. Análisis: Un atacante primero debe vulnerar el servidor para acceder al equipo o bien encontrar otro acceso, sin embargo, la puerta de entrada

más evidente es el servidor, por lo que este tiene cierto nivel de prioridad, sobre la computadora.

g) Priorizar la mitigación de riesgos de aquellas situaciones que pueden llegar a ser un compromiso catastrófico para la organización estableciendo ventanas de tiempo limitadas para su solución.
h) Cambiar el apartado de “Estado” de la vulnerabilidad o riesgo del documento de identificación de riesgos según su estado actual.

AR – 6. Top 10 Riesgos Identificados en Pymes.

Objetivo.

a) Identificar los principales riesgos y amenazas a los cuales están expuestas las Pymes desde el punto de vista de un profesional de la ciberseguridad.

Riesgos identificados.

a) Políticas deficientes: Las políticas y normativas de una empresa son las principales guías de comportamiento que toda empresa o Pyme debe establecer para sus colaboradores, en estas se detallan cuáles son los procesos específicos que se deben seguir para realizar ciertas acciones, según lo analizado mediante las entrevistas y posteriores encuestas se identificó que la falta de políticas es un problema latente en las Pequeñas y Medianas empresas, las distintas brechas informacionales de la sociedad, el déficit de no crear estas se convierte en problemas internos, donde no se tienen procesos debidamente establecidos, lo crea fragmentaciones y procedimientos indebidos o pocos seguros.
    - Para abordar este riesgo se recomienda mitigarlo, establecer políticas más rigurosas en un proceso que puede llegar a demandar tiempo, sin embargo, es una forma de establecer todos aquellos comportamientos esperados y que deben ser seguidos dentro de la empresa, la creación de algunas de estas políticas se puede ver más en detalle en “Políticas y Buenas Prácticas”.
b) Falta de conocimiento: La inexistencia de una “cultura” de ciberseguridad, es un problema latente de la sociedad en general, la expresión de “todos lo conocen pero nadie lo practica” es completamente certera, para efectos de las Pymes, no conocer medidas básicas de prevención o normativas especiales pueden llegar a afectar negativamente a sus empleadores, ya que los ciber-atacantes podrían aprovecharse de

esta falta de conocimiento para orquestar ataques dirigidos que podrían comprometer la confidencialidad de los datos de la empresa.

- Se puede mitigar este riesgo impartiendo capacitaciones constantes de ciberseguridad a los distintos colaboradores, reduciendo así la exposición a un ataque real, se pueden analizar los puntos de “Plan de Capacitaciones”

c) Ingeniería social: Este problema derivado de la falta de información, llega a convertirse en un vector de ataque comúnmente explotado, mediante este método es posible que un atacante llegue a:

- Descargar archivos maliciosos en el equipo.
- Ejecutar comandos directamente en el equipo
- Exfiltrar información del colaborador, como datos bancarios de la empresa o incluso personales.

Es importante siempre contar con la debida noción de que el principal vector de ataque son las personas, por lo que mantener al personal debidamente capacitado, aunque pueda volverse una ardua tarea, es altamente necesario, sin excepción alguna. La ingeniería social puede incluir técnicas como *vishing* (estafas por voz), *phishing* (estafas electrónicas), pozos de agua (sitios comúnmente visitados por una gran cantidad de personas), adicionalmente los atacantes también pueden hacerse pasar por personas que no son físicamente, con el din de obtener información.

- La principal forma de manejarlo es evitándolo, como se mencionó anteriormente mediante capacitaciones constantes o por medios de soluciones de filtrado de correo como un “*anti-spam*”.

d) Colaboradores / Excolaboradores molestos: Las principales filtraciones de datos se dan debido a colaboradores que ya no forman parte de la empresa, dependiendo de cómo se haya realizado este proceso puede que estos salgan con información relevante o confidencial sobre la empresa.

- Mitigar este riesgo incluye la firma de acuerdos de salida y la obligatoriedad de que los colaboradores firmen los acuerdos de confidencialidad (“
- POL – 10. Acuerdos de Confidencialidad (NDA)”) así en el caso de detectar qué información confidencial como bases de datos sean filtradas o utilizadas fuera de la organización,

- Otra manera es evitándolo, de forma que si la persona externaliza su deseo de salir de la organización o la empresa optó por el finiquito de su contrato se deben tomar las medidas de desactivación de accesos en cuanto sea posible, evitando así que la persona tome acciones maliciosas contra la empresa (véase "POL – 5. Políticas de Contrataciones y Finiquitos Laborales" y "POL – 6. Políticas para el Provisionamiento de Permisos").

e) *Software* "Pirata" / No licenciado: El proceso de adquisición de algunas aplicaciones catalogadas como más profesionales implican un gasto para la empresa, debido a esto muchas Pymes y personas optan por no adquirir *software licenciado* y buscar en la internet versiones "piratas" del mismo, estos usualmente descargados por medio de sitios de terceros, al proveedor original que no tienen relación alguna con este. En los binarios (ejecutables o instaladores) de estas aplicaciones es posible que un atacante inyecte virus o archivos maliciosos que podrían afectar a toda la organización, incluyendo los datos confidenciales,
    - Esto se puede abordar evitándolo, siguiendo los puntos detallados en ILR – 4. Proceso de Adquisición de Licencias de Software."
f) Ataques a páginas web: En una sociedad digitalizada, muchas Pymes optan por la creación de *sitios web,* donde postean o muestran sus productos a potenciales clientes, sin embargo, crear una aplicación sin un debido proceso de aseguramiento de calidad o pruebas de seguridad puede permitirle a un ciber-atacante explotar una vulnerabilidad desconocida en la página por una programación deficiente o carente de validaciones y ocasionar filtrados de información masivos de las bases de datos y distintos equipos presentes en la red, es importante mencionar que aunque estos equipos estén aislados en términos de red, mediante una subred se deben tomar medidas, como la adquisición de equipos de seguridad, *firewalls*, antivirus y otros equipos de protección perimetral,
    - Esta clase de riesgos se puede abordar de dos maneras, transfiriéndolo y mitigándolo de forma que se puede involucrar un servicio tercerizado de monitoreo y respuesta (transferir) o adquirir soluciones que puedan mantener estos activos seguros y concientizar a los desarrolladores en todas aquellas buenas prácticas durante el desarrollo, así mismo, establecer procesos de

recuperación ante desastres y ataques informáticos mediante "*playbooks"* (véase "Vulnerabilidades y Parámetros en Aplicaciones Móviles y Web" y "Recuperación a Ataques y Desastres informáticos").

g) Robos o hurtos de equipos: Este riesgo, es poco probable que pueda ser mitigado por la empresa, ya que cualquier colaborador puede ser víctima de una sustracción de sus activos empresariales, en el caso de que esto suceda con computadoras u otros dispositivos que no cuenten con un nivel de protección puede significar que el atacante puede tener acceso a todos los datos de estos elementos, usualmente estos son "formateados" de fábrica y comercializados en mercados negros,
    - Lo mejor es aceptarlo y evitarlo, como se mencionó anteriormente es poco probable mitigarlo por lo que es mejor aceptarlo y establecer medidas de encriptaciones de datos, evitando así que se pueda acceder a sus funciones sin antes desencriptar esta información, así como inculcarle al colaborador la responsabilidad de mantener su equipo seguro.

h) Desastres naturales e instalaciones inadecuadas: Pese a que este riesgo no corresponde a uno informático como tal, un desastre natural puede llegar a inhabilitar equipos, redes y otros insumos utilizados durante las tareas diarias en la empresa, esto puede llevar a pérdidas de información y pérdidas financieras realmente importantes,
    - Este riesgo se puede aceptar y evitar, es importante siempre salvaguardar los equipos cuando no se estén utilizando y realizar respaldos de información constantes de la información, las instalaciones deben de cumplir ciertos requisitos, especialmente si se manejan muchos dispositivos electrónicos a la vez, como tener aire acondicionado y mantenerlo a cierta temperatura y mantener accesos restringidos a estas ubicaciones, en caso de las modalidades remotas los mismos colaboradores deben velar por los activos asignados.

i) Equipos en estados deplorables: La empresa debe velar por el funcionamiento óptimo de los equipos asignados a sus colaboradores, de forma que estos siempre tengan un insumo completamente operativo y que funcione de forma óptima, durante el proceso de desarrollo de una Pyme es válido adquirir máquinas reconstruidas, sin embargo estas pueden llegar a presentar más problemas en un futuro, una máquina que no tenga un debido mantenimiento puede llegar a significar en pérdidas de información

si no hay políticas establecidas de respaldo de información, así como una abrupta interrupción de las operaciones fungidas desde ese equipos, adicionalmente estos equipos pueden entrar en situaciones donde están completamente fuera de soporte de actualizaciones, lo que los deja vulnerables ante ciertos ataques informáticos.

- Lo recomendable es evitar que estos riesgos se materialicen manteniendo un control adecuado de los activos, así como un mantenimiento programado.

j) Actualizaciones faltantes: La falta de actualizaciones en los equipos puede significar que hayan parches dirigidos a mitigar vulnerabilidades críticas descubiertas en los equipos que no serán aplicados, lo que deja a los equipos en estados vulnerable, esto a su vez pasa con los distintos softwares adquiridos, a la hora de adquirir alguno de estos debe existir una consciencia de que estos sistemas deben analizarse, evaluarse y actualizarse de ser posible cada cierta cantidad de tiempo no mayor a un año.

Sin embargo, no todos los sistemas reciben actualizaciones y van cayendo en la obsolescencia, estos sistemas son denominados "*legacy*" y pueden no solo generar problemas a nivel propio del sistema, si no en el equipo en general debido a que este no puede recibir actualizaciones para no alterar el funcionamiento del sistema, por lo que siempre es importante contar con sistemas de defensa perimetral lógicos, que imposibiliten o dificulten una explotación exitosa de una de estas vulnerabilidades.

- En donde sea posible se deben mitigar estos riesgos a través de la aplicación de parches y actualizaciones, en caso de que estas puedan afectar a estos equipos "*legacy*" es recomendable, aceptar este riesgo y tomar las medidas necesarias para que este no pueda ser materializado.

Inventario, Legitimización y Respaldo de Activos

Toda empresa debe aplicar buenas prácticas con sus activos informáticos para evitar posibles inconvenientes y riesgos, principalmente los activos deben ser inventariados, legitimados (mediante el licenciamiento), respaldados y actualizados constantemente.

ILR – 1. Inventariado de Activos

Objetivo.

a) Crear una metodología para realizar un apropiado inventariado de activos en las Pymes, para activos como: Información (cuantificada), *hardware* y *software*, personal, redes.

Procedimiento.

a) Realizar un reconocimiento general de los distintos tipos de activos de la empresa.

b) Definir y desarrollar en conjunto con los administradores de la empresa, un documento de "inventario", orientado al foco de negocio de la Pyme.

c) Es recomendable que sea construido en *softwares* como Excel para facilitar su edición.

- Este documento centralizado debe mantenerse meticulosamente actualizado ya que cada vez que uno de estos activos entre a formar parte de la empresa, sea o no temporal.

d) En la tabla No. 10, se define una estructura para un documento de inventariado a nivel general.

Tabla 10.

Estructura propuesta para un documento de inventario de activos (Datos generales)

Producto	Marca	Fecha de ingreso	Cantidad	Precio	Contacto/ Proveedor

Fuente: Elaboración propia.

e) Para el inventariado de los activos se define la estructura de la tabla No. 11.

Tabla 11.

Estructura propuesta para un documento de inventario de activos (Equipos)

Clientes	Marca	Modelo	Sistema Operativo	Tipo	Actualizado	Encargado

Fuente: Elaboración propia.

- Equipos: Dirección IP o nombre / "*hostname*" del equipo.
- Marca: Marca del equipo.
- Modelo: Modelo del equipo
- Sistema operativo: Versión del sistema operativo del equipo.
- Tipo: Para que es utilizado en la organización (producción, contabilidad…).
- Actualizado: Fecha de la última comprobación de actualizaciones pendientes.
- Encargado: Persona a la cual se le fue asignada la maquina o equipo.

Tabla 12.

Estructura propuesta para un documento de inventario de activos (Redes)

VLAN	Tipo	Rango de IPs (X.X.X.X/NN)	Equipos aproximados

Fuente: Elaboración propia.

- VLAN: Nombre de la segmentación de red.
- Tipo: ¿Cuál es el uso dentro de la red? (producción, contabilidad…).
- Rango de IPs: Indicar el segmento de red que abarca la subred/VLAN.
- Equipos aproximados: cuantos equipos aproximadamente hay activos en dicha VLAN.

Tabla 13.

Estructura propuesta para un documento de inventario de activos (Personas)

Nombre	Apellido	Fecha de entrada	Posición	Usuario/Cuenta	Reporta

Fuente: Elaboración propia

f) Una vez establecida la estructura del documento se debe realizar un reconocimiento general en la empresa para identificar todos los activos según su tipo e irlos actualizando en sus tablas correspondientes.

g) Para los datos, es importante cuantificar la información obtenida, agregar información de contactos, proveedores o alianzas estratégicas, pese a que es un dato difícil de expresar en un documento general, se debe pensar en ellos como lo principal de toda organización.

h) Los nuevos equipos y aplicaciones se deben ir agregando según vayan siendo adquiridas por la organización, conforme la Pyme vaya avanzando pueden utilizarse también equipos virtualizados en la nube (*cloud*) o localmente, estos también deben ser agregados, para que haya una noción y percepción de su existencia (incluso permite una claridad en caso de que este recurso se esté desaprovechando o incurriendo en gastos innecesarios).

i) Las redes son uno de los puntos centrales de las organizaciones, conforme la Pyme vaya desarrollándose, se tendrán que implementar segmentaciones para evitar

"cuellos de botella" en la red, creando VLANs o segmentos lógicos de red para cada área, por ejemplo, las áreas operativas, ventas, contabilidad y tecnologías de información es importante separarlas debido a que todas manejan información distinta y delicada, conforme se den estas segmentaciones es importante mapearlas.

j) Llevar un "inventario" o registro de personas es vital y esencial para toda empresa en general, para esto usualmente las empresas optan por utilizar un directorio activo o "*Active Directory*", un servidor centralizado en donde se gestiona la creación de usuarios de dominio (así como datos relacionados a este como su fecha de inicio, área y permisos), en Pymes es importante comenzar este gestión desde tempranas etapas de desarrollo e implementar sistemas asociados, que sirvan para que los administradores o áreas de recursos humanos puedan gestionar vacaciones y demás trámites necesarios para sus colaboradores.

Beneficios. Tener un inventario actualizado y debidamente desarrollado puede evitar posibles confusiones en un futuro y una mejor gestión y organización de todos los activos que maneja la Pyme, de esta forma, procesos de automatización, adquisición o renovación pueden ser llevados de manera más consciente y evitar gastos adicionales que pueden llegar a ser completamente innecesarios.

ILR – 2. Priorización de Activos

Objetivo.

a) Crear un proceso de identificación y resguardo de los activos más importantes de la organización.

Procedimiento.

a) Una vez creado el inventario e identificado todos los activos organizacionales, se deben establecer niveles de importancia para aquellos más relevantes.
    - Es importante establecer medidas más rigurosas de seguridad para todos aquellos usuarios que puedan tener accesos a toda la organización o datos confidenciales.

b) Discutir junto con los directores de área, cuáles son aquellos activos que consideran como los más importantes dentro de sus operaciones diarias.

c) Priorizar la protección de los datos confidenciales del negocio y datos personales de colaboradores y clientes, A nivel de personas esta información es conocida como PII, Información identificable personal (*Personal Identificable Information)*.
d) Velar porque existan múltiples baterías y formas de respaldos disponibles (Ver "ILR – 6. Metodología de Respaldo de Información")
e) Proteger equipos o máquinas con riesgos identificados como críticos y altos que no hayan sido tratados, especialmente si estos no pueden ser mitigados.
    - En caso de contar con equipos que estén expuestos al internet, tenerlos debidamente configurados y actualizados es prioritario, por sobre los utilizados internamente.

ILR – 3. Proceso de Adquisición de Hardware

Objetivo.

a) Definir un proceso de adquisición de equipos de *hardware* de forma legítima.

Procedimiento.

a) Adquirir *hardware* es un proceso delicado, debido a que estas máquinas deben ser aptas para funciones diarias dentro de un entorno laboral, conforme la tecnología avanza, los requerimientos de los programas se vuelven más exigentes en temas de recursos de computación.
b) Debe contemplarse tener al menos dos tipos de máquinas, técnicas y operativas, las primeras, serán utilizadas para realizar mantenimientos en servidores o aplicaciones que se usen internamente, por lo que requerirá de mayor potencia a nivel de recursos que las demás computadoras, por otro lado, las operativas, serán las utilizados en la operación diaria de la empresa, como documentación, correos electrónicos, entre otros.
c) Identificar un proveedor confiable de equipos de *hardware* debería ser prioridad para las Pymes, según su crecimiento esta requerirá de rapidez y calidad para la adquisición de equipos.
d) Estos proveedores deben poder garantizar la proveniencia del artículo en cuestión, proveer garantías en caso de algún fallo en el mismo durante cierto tiempo (por lo general 1 año o más), algunos de ellos incluso pueden proveer un soporte técnico y

ayudar con la cotización de distintos elementos de *hardware* que puedan fallar o verse deteriorados, como pantallas o baterías, que son los más desgastados por el uso diario.

e) En caso de ser posible es recomendado hacer un estudio del mercado y sondeo entre otras Pymes u organizaciones para analizar la viabilidad de un nuevo proveedor de equipos.

f) Al adquirir equipos de *hardware,* estos vienen con un identificador conocido en informática como dirección MAC (*Media Access Control*), el cuál es un identificador absolutamente único entre los equipos físicos, es recomendable identificar esta dirección (usualmente viene en la parte central, trasera de algunas computadoras y componentes y está compuesta de 12 números) y verificarla en internet, esto garantiza que el equipo es completamente válido y está autorizado por el fabricante.

    - En caso de adquirir una máquina “refabricada”, este número si puede llegar a cambiar.

ILR – 4. Proceso de Adquisición de Licencias de Software

Objetivo.

a) Definir un proceso de adquisición de licencias de *software* de forma legítima.

Procedimiento.

a) Adquirir un licenciamiento válido puede ser todo un reto, debido a los gastos que conllevan, sin embargo, se vuelve algo completamente necesario, algunas de las maquinas adquiridas pueden venir con licencias preinstaladas, sin embargo, adquirir una propia licencia empresarial puede traer más beneficios (aplicable según la capacidad de la Pyme).

    - En el caso de *Microsoft,* adquirir licencias corporativas y utilizarlas junto con sistemas operativos *Windows* puede resultar en integraciones importantes entre las aplicaciones, lo que facilita el uso de sistemas internos, así como implementar opciones de inicio de sesión como SSO (*Simple Sign On*), lo que permite a los usuarios acceder a sus perfiles con solo estar autenticado en el equipo en general.

b) Identificar todas aquellas aplicaciones que requieren de un licenciamiento para su correcto funcionamiento, así como seleccionar cuáles se utilizarán en la empresa.

c) Una vez identificadas las aplicaciones por utilizar, se debe indagar directamente en la página del proveedor, por ejemplo, si se buscan licencias de Office 365, se debe de visitar el sitio oficial de Microsoft para analizar los planes oferentes o bien contactarlos directamente para verificar la información pertinente a su *software*.
d) No seguir redirecciones de páginas externas al proveedor, lo recomendable es siempre buscar la página del fabricante original, algunas de estas páginas pueden ser sitios maliciosos, suplantando al original.
e) Adquirir aplicaciones pagas puede generar cierto nivel de desconfianza, debido a la forma en la que el proveedor maneja los datos bancarios, en caso de realizar compras por medio de portales electrónicos con una tarjeta bancaria o agentes de ventas es recomendable realizar una investigación previa del proveedor y analizar distintos factores como el soporte y la confiabilidad.
f) Al adquirir licencias o *softwares* gratuitos, una alternativa de seguridad adicional es cargarlos en páginas como "Virus Total" la cual se encarga de analizar "firmas" de virus preexistentes para validar que este sea completamente seguro de instalar.
g) Usualmente los fabricantes, proveen un paso adicional para validar que el archivo que se está descargando sea completamente legítimo, generando un valor computado denominado *"hash"* el cual consiste en un valor único creado a partir de la codificación del binario (descargable) original, la peculiaridad de esta valor, es que cualquier cambio en el archivo generará un *hash* completamente distinto, garantizando la integridad del archivo, este valor se puede generar cargando el archivo en la previamente mencionada "*Virus Total*" o bien descargando otros ejecutables que puedan crear estos valores, para poder comparar su legitimidad e integridad.

ILR – 5. Aseguramiento y Actualización de Activos

Objetivo.

a) Desarrollar un proceso de aseguramiento y actualización constante para los activos informáticos de la Pyme.

Procedimiento.

a) Capacitar a los empleados es una de las acciones principales para evitar futuros problemas que comprometan a la organización, crear esta cultura de ciberseguridad,

debería ser una prioridad para toda empresa, este proceso de capacitación se ve más en detalle en el apartado “CAP – 1. Capacitaciones”.

b) Mantener los datos seguros implica crear políticas robustas para el manejo apropiado de los mismos.

c) Dependiendo de la clasificación de la confidencialidad de los datos que se manejen internamente (véase “POL – 8. Políticas para el Manejo de la Información”) se puede optar por soluciones contra el filtrado de información, conocidas también como “DLP” (*Data Loss Prevention Solutions*), detallada en el punto mencionado previamente.

d) Otras soluciones como cortafuegos, antivirus o SIEM (*Security Information and Event Management*) permiten aplicar una capa de seguridad extra en la red de los usuarios, estos pueden llegar a detectar tráfico de red indeseado o incluso detectar acciones poco comunes por parte de los usuarios, según el presupuesto y los riesgos de la empresa estas licencias y soluciones deben ser analizadas para determinar si su implementación y adquisición será beneficioso en tempranas etapas de desarrollo.

e) Configurar reglas y soluciones de *Anti-Spam*, que puedan detectar y filtrar correos que puedan contener potencialmente peligrosas, como enlaces, imágenes u otra clase de archivos enviados de forma maliciosa.

f) Mantenerse anuente de los boletines de seguridad de los distintos proveedores de servicios de la Pyme, así como mantener un proceso de actualización continuo en todos los equipos y aplicaciones utilizadas, como un punto de apoyo para determinar cuáles equipos y *softwares* se consideran “vulnerables” o desactualizados en que se pueden realizar evaluaciones de seguridad, según lo mencionado en el punto “AR – 4. Evaluación de Vulnerabilidades”, sin embargo, es importante realizar mantenimientos constantes, al menos una vez al mes.

ILR – 6. Metodología de Respaldo de Información

Objetivo.

a) Crear una metodología para realizar respaldos de la información.

- ¿Quién debe de hacerlo?
- ¿Cuándo debe de hacerse?
- ¿Cómo debe hacerse?

- ¿Qué debe de respaldarse?
- Tipos de respaldo.
- Pruebas de respaldo

Procedimiento.

a) Tipos de respaldo: según Weiss (2020), existen tres tipos de respaldos de datos a nivel de *software*, los cuales son:
    - Completo: es una copia completa de todos los datos almacenados por el equipo, requiere de una gran capacidad de procesamiento, pero es una de las más rápidas y efectivas ante la pérdida completa de datos, un respaldo de datos completo debe considerarse hacerse como mínimo una vez a la semana.
    - Diferencial: los de tipo diferencial son incompletos, realizan el respaldo a partir de la información que cambio en un periodo de tiempo según el último completo que se haya realizado, sin tomar en cuenta los demás respaldos diferenciales hechos previamente (no acumulativos).
    - Incremental: a diferencia de los diferenciales estos son acumulativos de forma que hace respaldos desde la última carga completa, tomando en cuenta los otros respaldos incrementales que se vayan haciendo.
b) Pruebas de respaldo.
    - Las cargas de los datos de respaldo muchas veces pueden verse afectados o ser corrompidos por un mal guardado, una falla en la red, entre otras posibilidades, por lo que poner a prueba el funcionamiento de estos mediante restauraciones completas o parciales (según el tipo) es recomendable hacerlo como mínimo una vez cada mes, en el momento que se hayan realizado las cargas (en caso de cargas masivas o muchos datos).
    - Si se guarda un archivo relevante, se puede generar el *hash* de este en un algoritmo de MD5 y guardarlo, para una posterior revisión, este valor calculado lo que comprobara es que los datos se mantengan íntegros, en el caso de que este valor sea distinto quiere decir que hubo un cambio o corrupción de los datos.

- Se debe de designar una persona a esta tarea (preferiblemente los definidos en la sección de “¿Quién lo realiza?”), esta estará encargada de documentar y automatizar estas tareas.
- Estas pruebas también se pueden realizar en el punto de “RES – 3. Ejercicios de Simulación” del punto de Recuperación a Ataques y Desastres informáticos.

c) ¿Quién lo realiza?

- Según el tamaño de la Pyme se debe contar con una persona dedicada al mantenimiento y debido respaldo de la información, siendo este parte del equipo de TI (Tecnologías de información), si bien puede que los recursos de la Pyme no sean los suficientes para una contratación de este tipo, se debe crear un rol que afronte esta función (véase “RAC – 1. Definición de roles”).
- Algunas empresas tercerizan los servicios de TI, para evitar afrontar este gasto directamente, esta es una excelente opción para Pymes que estén iniciando, sin embargo, este debe tener la función de velar por el respaldo de la información como lo haría una propia área de TI.
- Las personas encargadas de respaldar la información catalogada como principal o esencial para el negocio son todas aquellas que cumplan con un papel técnico dentro de la organización.
- Todo colaborador debe velar porque su información pueda ser accedida por el mismo en cuanto este o alguien lo necesite, toda información interna de la empresa debe mantenerse confidencial y disponible.

d) Cuando debe de hacerse.

- Por buenas prácticas, los respaldos de información deberían hacerse diariamente en caso de contar con un *software* que lo permita.
- En caso de que no se cuenten con soluciones tan accesibles como una infraestructura *cloud*, los respaldos deberían hacerse al menos una vez cada semana, esto debido a que la pérdida de datos al hacer respaldos mensuales puede llegar a ser bastante grande, también se debe contar con respaldos de información aislados y protegidos completamente fuera de la red, estos deben realizarse y actualizarse al menos una vez cada dos semanas o cada mes.

e) ¿Qué se debe respaldar?

- La información como uno de los dos principales activos de una empresa debe mantenerse siempre segura y respaldada, todos los datos que impliquen información confidencial, contratos entre otros deben mantenerse siempre disponibles y protegidos.
- Configuraciones claves en equipos de red y *software*, mediante la creación de guías de configuraciones base por equipo o aplicación según su función o bien por medio del respaldo de configuraciones a través de archivos xml (disponible en equipos de red y algunas aplicaciones).
- Imágenes de disco o "ISO" que contengan configuraciones preestablecidas por la Pyme, al momento de adquirirse equipo como computadoras y servidores, estas "imágenes" pueden permitir facilitar y agilizar las configuraciones debido a que ya existen.

f) ¿Cómo debe hacerse?

- Se debe designar a una persona o equipo encargada de velar por el respaldo de la información (áreas o personal de tecnologías de información).
- Priorizar los datos por resguardar, más según lo establecido en "ILR – 2. Priorización de Activos".
- El uso de algunos *softwares* como *Office 365*, incluyen funcionalidades de respaldo automático de documentos y únicamente requiere de activar las funciones de auto guardado, en las directivas de los equipos, esto se hace mediante el uso de políticas personalizadas establecidas en directorios activos, cabe mencionar que dicha solución esta alojada específicamente en la nube (*cloud*) de *Microsoft.*
- Si no se cuentan con estas soluciones en la nube, se deben configurar otra clase de soluciones como lo son los NAS (*Network Attached Storage*) o los servidores SAN (*Storage Area Network*) estas son completamente locales y no están expuestas a una red pública, si no que por lo general se mantienen aisladas en la red.

i. Un NAS o almacenamiento conectado a la red implica dedicar un servidor exclusivamente al almacenamiento de archivos y establecerlo como un repositorio centralizado de información, usualmente estos demandan una alta cantidad de recursos, especialmente de disco duro. Esta clase de servidores usualmente es un sistema licenciado que le permite a los usuarios o a los administradores de red configurar sus reglas o acceder a este y almacenar su información.

ii. Un SAN por otro lado, requiere un nivel de conocimiento mucho más técnico para su mantenimiento e implementación debido a que este consiste en la conexión y uso de múltiples discos de alto rendimiento y velocidad configurados de forma única, permitiendo una mayor escalabilidad y adaptabilidad que la de un NAS, esta solución se vuelve más viable si el tamaño de la Pyme es considerable (mayor a 50 empleados), si existe un flujo de datos muy alto y también se puede ver como una alternativa para Pymes con muchos años en el mercado y con muchos documentos.

- En caso de utilizar máquinas virtuales, existe la opción de crear capturas conocidas como "*snapshots*", las cuales son un tipo de respaldo que les permite a los técnicos restaurar el equipo en un punto en el tiempo donde la máquina tenga cierta información y configuraciones, es decir, si antes de aplicar configuraciones que puedan afectar su funcionamiento o rendimiento se realiza una captura, se puede utilizar para recuperar el estado del equipo antes de que las configuraciones fuesen aplicadas.
- Si se usa una infraestructura en la nube, se deben tener posibles puntos de restauración en equipos físicos completamente aislados de la red principal de la empresa.
- Desarrollar un lineamiento escrito (documentación) del proceso interno utilizado para realizar los respaldos de la información.
- Definir una nomenclatura para los archivos respaldados, por ejemplo "Nombre_Apellido_Fecha Completa_Nombre General" para archivos de

usuarios y para equipos y configuraciones se puede utilizar "Hostname_DireccionIP_Fecha_Configuración/Respaldo_NombreGeneral"

- Crear una cultura de respaldos de la información mediante capacitaciones dirigidas a todo el personal de la empresa, sin excepción alguna.
- Evitar crear respaldos de información en equipos o discos que no estén aprobados por la dirección de la empresa (esto se puede catalogar como un riesgo ya que pese a la existencia de múltiples soluciones como las mencionadas previamente, no puede existir una visión completa a las acciones del colaborador).
- Proveer acceso a la información respaldada únicamente a aquellos colaboradores que verdaderamente lo necesitan, así como mantener una debida segmentación de los archivos, esto según su área, evitando confusiones (tomando en cuenta los responsables y colaboradores de área).
    i. Ejemplo: Si un colaborador operativo requiere acceder a sus archivos respaldados este únicamente debe poder acceder a los suyos, archivos de otras personas, de distintas áreas debe estar completamente limitado, siguiendo un organigrama, de forma que el gerente o administrador de área tenga acceso a los archivos de las personas a su cargo, pero estos no puedan acceder a los del gerente.

Responsables y Roles

Definir todos aquellos roles que cumplen los colaboradores internamente puede ayudar a crear un ambiente más organizado y apto para el trabajo, así mismo establecer formas apropiadas para manejar proyectos y llevar control de todas las actividades relacionadas a estas pueden propiciar un ambiente más profesional.

RAC – 1. Definición de roles y puestos internos

Objetivo.

a) Proporcionar una guía de los roles que deberían existir como mínimo en una Pyme.
b) Propiciar la creación de un organigrama organizacional desde tempranas etapas del desarrollo en la Pyme.

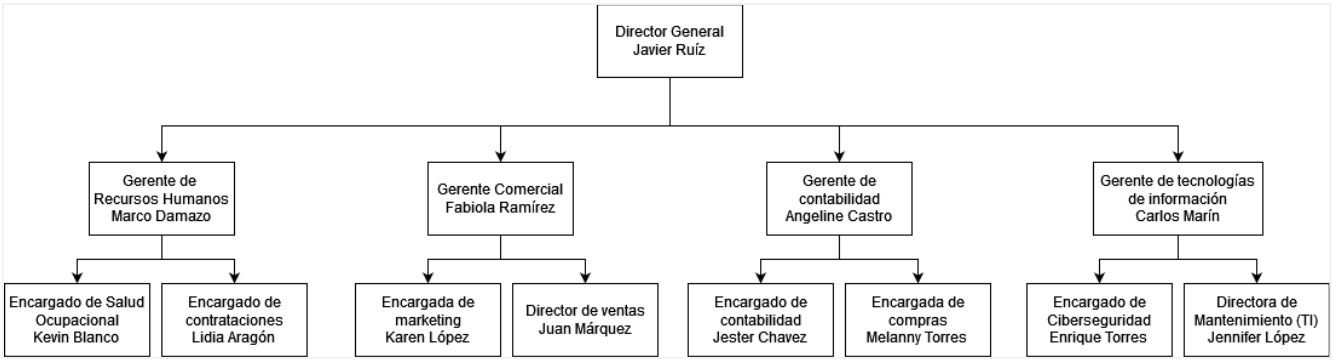
Procedimiento.

a) Junto con las personas encargadas de distintas áreas en la empresa se deben definir todos aquellos roles y posiciones relevantes dentro de la Pyme.

b) Crear en conjunto un organigrama que pueda detallar la forma en la que la empresa está construida y establecida, de forma que las personas sepan a quién deben reportar eventos, dudas o escalar puntos importantes, hay múltiples *softwares* que permiten la creación de esta clase de diagramas, sin embargo, las más populares son *draw.io* y *Microsoft Visio.*

Figura 35.

Ejemplo de organigrama institucional.



Fuente: Elaboración propia.

a) Definir los puestos más relevantes de negocio, jefaturas y jefes de equipo principalmente, este diagrama debe ser difundido en la empresa, para que en caso de requerir acudir ante alguna de las jefaturas saber y conocer a quién buscar.

b) Definir los distintos roles que cumplirán las distintas jefaturas y encargados de área dentro de la empresa, de forma que todos los integrantes y responsables sepan su función, a continuación, se definen algunos de estos roles comúnmente encontrado en su área respectiva.

c) Área administrativa (de menor a mayor grado de relevancia):

- Supervisores o lideres de equipo: son personas con cierto grado de experiencia que se encargan de velar porque se cumplan los proyectos dar apoyo cercano en caso de dudas o consultas, tiene el deber de garantizar que su “equipo” cumpla con las políticas e indicar posibles problemas o

situaciones de riesgo dentro de los colaboradores, dependiendo del tamaño de la empresa pueden existir más de un líder de equipo.

- Jefe o gerente de área: las personas que ocupan estos cargos son los encargados de velar porque las metas establecidas por las directivas de la empresa sean cumplidas, estos usualmente pueden tomar las decisiones de su área respectiva, ya sean contrataciones preaprobadas, despidos justificados, aprobación de nuevos proyectos e iniciativas y buscar presupuestos para mejorar el área.
- Director general: la persona en esta posición cumple como cabecera principal y cara de la empresa ante el público, la responsable de establecer metas, autorizar presupuestos de gastos, este a su vez debe dar cierto nivel de seguimiento a todos los proyectos y llamar a las distintas jefaturas para que se dé una "rendición de cuentas" donde se indica el avance de cumplimiento de las metas, así como analizar y aprobar las distintas propuestas de proyectos.
- Junta directiva/Socios: usualmente presente en empresas grandes y que cuentan con múltiples inversionistas, sin embargo, conforme un emprendimiento va avanzando se van requiriendo más fondos, lo que hace a los propietarios y directivos buscar fondos de inversionistas, estos inversionistas una vez que realizan un aporte importante en la empresa pueden ser tomados en cuenta en las decisiones importantes de la empresa, llegando a formar parte de este grupo de "Junta directiva".

d) Área de recursos humanos:

- Jefe de salud ocupacional: es el encargado de velar por la seguridad, salud y ánimo de los colaboradores en la empresa, actualizando las políticas y directrices relacionadas continuamente, manteniéndolas debidamente actualizadas y validas ante las leyes del país, este a su vez puede escoger planes relacionados a salud y seguros.
- Jefe de contrataciones: es el encargado de establecer los procesos de inducción de nuevos talentos incluidos dentro de las empresas, así como establecer y

velar porque las personas que dejan la empresa realicen ciertas acciones antes de abandonar la empresa.

e) Área comercial:

- Jefe de ventas: Es la persona encargada de velar porque las metas y ventas organizacionales se realicen, también puede estar involucrado en la atención a cuentas de gran importancia de la empresa y en la búsqueda de nuevos mercados y potenciales clientes junto con el resto del departamento o área de ventas.
- Jefe de marketing: Este rol abarca a aquella persona que debe de realizar y buscar formas de atraer potenciales clientes a la empresa, creando publicidad en redes sociales, televisión u otros medios, debe aprobar campañas publicitarias, buscar ideas innovadoras y analizar distintos competidores junto con los supervisores del área de *marketing* organizacional.
- Jefe de servicio al cliente: La persona a cargo debe velar por que la forma en la que sus colaboradores dan soporte a los clientes en caso de que este tenga dudas o consultas que sean respetuosa y de valor, a su vez debe verificar que todas sus personas a cargo sean capacitadas debidamente sobre los procesos internos de la empresa y establecer las normativas que limitaran la cantidad de información que estos puedan brindar.

f) Área de contabilidad:

- Jefe de contabilidad: la cabecera de este departamento tiene la función de velar por las finanzas de la empresa, donde mediante informes de ingresos de las áreas se pueden tomar decisiones relacionadas a la reducción de presupuesto para distintos procesos internos y aprobación de presupuestos para proyectos o nuevas iniciativas que la empresa vaya a ejecutar o poner en desarrollo.
- Jefe de compras: la persona que ocupa este rol debe verificar todas las contrataciones administrativas, compras de equipo y distintos estudios que impliquen un gasto dirigido a terceros a la empresa que se realicen o se necesiten. Adicionalmente debe apoyar con la búsqueda y estudio de posibles

alianzas estratégicas con otras empresas que puedan ser de beneficio para los servicios y productos que desarrolle u ofrezca la empresa.

g) Área de tecnologías de información:
    - Jefe de ciberseguridad: el encargado de esta área tiene la responsabilidad de que la empresa este alineada a ciertos estándares de seguridad informática, de forma que vigile la implementación de nuevos procesos y equipos de red y apruebe las políticas implementadas en los equipos operativos, así mismo debe velar por la seguridad de todos los activos de la empresa ante posibles ataques informáticos que puedan afectar la disponibilidad, integridad y confidencialidad de la información, este así mismo, puede buscar el apoyo de distintas empresas que ofrezcan servicios de acompañamiento durante estos procesos.
    - Jefe de mantenimiento (TI): La jefatura de mantenimiento o de tecnologías de información es la encargada de mantener los equipos utilizados dentro de la empresa completamente funcionales y actualizados, así como realizar ciertas capacitaciones, desarrollar guías de uso y dar soporte para todos las aplicaciones y equipos utilizados internamente por la Pyme, también es el encargado de velar porque las vulnerabilidades detectadas mediante evaluaciones de seguridad sean completamente remediadas y difundir constantemente cambios en las políticas de los equipos en caso de ser completamente necesario.
h) Algunas otras áreas que se pueden ir creando según el crecimiento puede ser el área de gestión proyectos, la cual busca nuevas iniciativas y vela por el cumplimiento de todas las nuevas propuestas y proyectos que se quieran implementar dentro del negocio, según su tipo, informático, industrial o de otra índole.
i) Es importante destacar que dichos roles o puestos dentro de la empresa pueden llegar a variar según el tamaño de la Pyme, y puede ser normal que una persona ocupe más de un cargo a la vez, esto debido a que al momento de definir estos roles se debe pronosticar un crecimiento escalonado, en donde la Pyme únicamente realizará estas contrataciones y bifurcara las áreas cuando su administración se vuelva una “carga

pesada” para una única persona o bien en caso de un declive tomar las acciones necesarias para mantener la empresa en cierto nivel de viabilidad financiera.

Beneficios.

a) Crear una cultura organizada desde tempranas etapas, con acciones simples como definir los roles internos en la empresa y contar con un organigrama debidamente actualizado puede ayudar a la Pyme a contar con bases fuertes según se dé un crecimiento y desarrollo en sus operaciones.
b) Desarrollar documentación para capacitar a los nuevos colaboradores puede ser una buena práctica organizacional si existe una guía de cuáles son las funciones que entrará a desempeñar y el “cómo” realizarlas apropiadamente.

RAC – 2. Proceso de Creación de una Matriz RASCI

Objetivo.

a) Guiar en el proceso de la creación de una matriz RASCI para los proyectos y procesos que puedan ser implementados por la empresa interna o externamente.

Procedimiento.

a) Inicialmente se debe haber creado un proceso o proyecto con sus debidos riesgos, beneficios y requerimientos iniciales para su puesta en desarrollo, una vez que este pase por un proceso de revisión y autorización.
b) Se procede a identificar a todos aquellos involucrados en el proyecto.
c) Identificar todas las tareas asociadas al proyecto.
    - Procesos / Desarrollo de tarea.
    - Reuniones de seguimiento.
    - Entregables.
    - Desarrollar una matriz RASCI para cada tarea del proyecto.
d) Una matriz RASCI es una matriz de asignación de responsabilidades, donde su función principal según RockContent, (2019) “Definir los roles y responsabilidades de cada persona involucrada en los proyectos y procesos de la empresa**.** Incluso porque muchas veces un solo empleado puede realizar varias funciones y es por eso por lo que todo necesita ser documentado.” (párr. 4), esta se basa en definir cinco roles especificos para la realizacion del proceso, Responsable, Aprobador, Soporte, Consultado e Informado.

e) Identificar los roles utilizados por la matriz para cada uno de los involucrados.

- Responsable (*Responsable*): La persona con este rol dentro del proceso es la encargada de llevarlo a cabo o desarrollarlo y se hace completamente responsable de su ejecución y finalizacion, los procesos pueden tener múltiples tareas por lo que pueden existir múltiples responsables para una o distintas tareas, sin embargo siempre debe asigarse un "Responsable lider" de efectuar la actividad.
- Aprobador (*Approver*): Este rol esta encargado exclusivamente de aprobar o rechazar las tareas efectuadas por el responsable, usualmente este cargo es tomado por lideres de equipo o de proyecto, ya que evaluan si los requerimientos establecidos incialmente son cumplidos o no, de igual forma puede que el proceso pase por multiples fases de aprobacion, por lo que puede que existan múltiples personas con un rol de aprobación.
- Soporte o Apoyo (*Support*): Usualmente considerado como un respaldo, son todas aquellas personas que usualmente ocupan un cargo ejecutivo que pueden servir de soporte para la ejecución de todo el proyecto, esta puede hacerse cargo en caso de que el responsable principal sufra de algún problema que le impida continuar su labor o bien puede apoyarlo en distintas tareas que este delege.
- Consultado (*Consulted*): Las personas consultadas son todas aquellas que no estan involucrados directamente en el desarrollo del proyecto pero su consejo y experiencia pueden ser un gran punto de referencia para los responsables de ejecutarla, estos usualmente son personas con basta experiencia en la tarea, esta no necesariamente tiene un cargo administrativo.
- Informado (*Informed*): Dentro de este rol se encuentran todas aquellas personas que no tienen una participacion como tal en su ejecucion por lo que no se tienen papeles de responsabilidad o autorización dentro del proceso, sin embargo deben mantenerse informados en todo momento de los avances del mismo, por lo general son las partes interesadas, que pueden ser tanto internas como externas, según su tipo de implementación.

f) Establecer los plazos de entrega para cada una de las tareas del proyecto.

- Ejemplo: tomando en cuenta la organización ficticia de la
- Figura **35.**, se creó el siguiente ejemplo donde la empresa quiere desarrollar un servicio de consultoría de ciberseguridad para un cliente de la empresa X que dará como resultado un entregable con una evaluación de vulnerabilidades.

Tabla 14.

Estructura propuesta y ejemplo de una matriz RASCI

Tarea N. Creación de reporte de evaluación de vulnerabilidades					
Fecha de entrega:			DD/MM/YYYY		
Recurso	Responsable	Aprobador	Soporte	Consultado	Informado
Aníbal Sánchez	X-1				
Enrique Torres	X-2				
Jennifer López			X		
Melanny Torres				X	
Carlos Marín		X – 1			
Javier Ruíz		X – 2			
Karen López					X
Michael Leeds (Cliente X)					X
Alina Caldentey (Cliente X)		X – 3			

Fuente: Elaboración propia.

- Indicar un número al lado de las “X” significa el orden de prioridad del encargado según su rol, donde para “responsable” el número más bajo corresponde a un mayor nivel de responsabilidad del proyecto y en “aprobador” indican por cuál es el orden en el que se darán las aprobaciones siendo el número más bajo el primero en aprobar o desaprobar los avances y entregables del proyecto.

h) Al ser este un documento maleable e interno de seguimiento su simbología puede cambiar según se requiera para mantener su entendimiento lo más claro posible, sin embargo, los roles y su función deben mantenerse inalterados.

Beneficios:

a) Crear matrices RASCI para cada tarea de un proyecto puede ser complejo, sin embargo, proporciona una visibilidad clara de los involucrados en todo momento.

b) La utilización de esta clase de documentos en conjunto con la implementación de metodologías ágiles (véase "RAC – 3. Metodología para la Administración de Proyectos") para el desarrollo de algunos proyectos puede llegar a ser un diferenciador en el mercado para potenciales clientes o incluso internamente debido al orden y nivel de gestión que puede llegar a generar si se aplica correctamente.
c) Establecer roles permite trabajar bajo algunos principios básicos de ciberseguridad como "Mínimo privilegio" (*Least Privilege*), el cual indica que solo se les darán a los involucrados los recursos necesarios para que desempeñen su labor.

RAC – 3. Metodología para la Administración de Proyectos

Objetivo.

a) Definir una metodología para la administración de proyectos básica que pueda ser implementado en las distintas áreas del negocio.

Procedimiento.

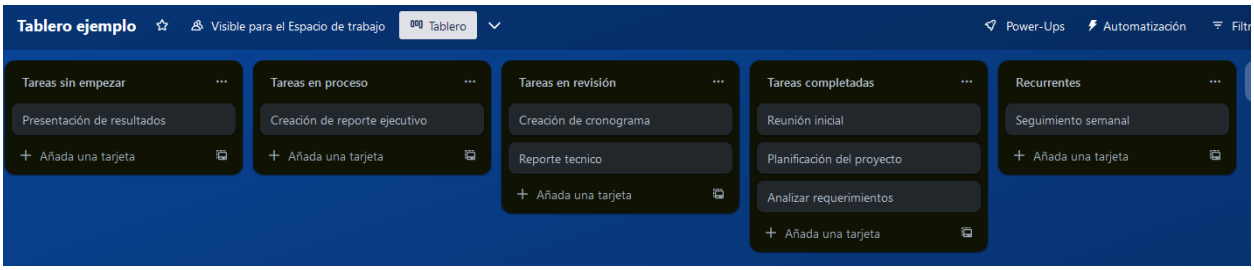
a) Una vez que se haya planes sobre la implementación de un nuevo proyecto se deben definir las metodologías utilizadas durante la totalidad de este.
b) Es recomendable usar metodologías ágiles reconocidas de proyectos como lo es "*Scrum*", a pesar de que esta es usualmente utilizada para proyectos de desarrollo puede ser aplicada en todos los proyectos en general e incluso integrarse y combinarse con otras como "*DevOps", "DevSecOps" o "Kanban*".
c) Definir los roles de todos los involucrados en el proyecto, a través de la matriz RASCI.
d) Designar un "administrador de proyectos" (*Project Manager*), este tendrá la función principal de dar seguimiento a las tareas realizadas por el responsable e ir asignando y reportando los porcentajes de avance de las tareas a las partes interesadas, pese a que este se puede considerar como un "responsable" dentro del proyecto, la ejecución de este no recae directamente en él, lo que lo convierte en un "responsable secundario" donde el principal es la persona encargada de la ejecución de este.
e) Una vez aprobado el proyecto se recomienda el uso de "*kanbans*" o notas, las cuales pueden permitir un seguimiento ordenado de las distintas tareas asignadas a los responsables, siendo similar a un tablero de apuntes, estas "notas" se pueden

categorizar según el estado de la actividad y así dar visibilidad de los avances importantes al administrador del proyecto.

- Se pueden utilizar softwares gratuitos como *Trello y Notion* para la administración dinámica de los proyectos.
- Se deben establecer plazos estimados para la finalización de las tareas, donde más de una semana puede significar en un retraso considerable.
- Todos los involucrados deben tener visibilidad en todo momento de sus actividades según le sean asignadas.

Figura 36.

Ejemplo de tablero de Kanbans



Fuente: *Software de Trello/Atlassian* con la cuenta del autor.

f) El administrador puede agendar reuniones a los involucrados cada cierto tiempo (por lo general una semana), en estas puede llevar un control de que se ha hecho durante este tiempo y si el proyecto presenta algún riesgo que pueda hacer que se atrase la entrega o finalización de la tarea.

g) Las nuevas metodologías son cíclicas, y por ende dictan que los proyectos realizados bajo estos métodos sean constantemente actualizados y revisados, según emerjan de forma que se mantengan bajo un principio de "integración continua" de cambios y "entrega continua" de los entregables o productos durante la completitud del proyecto esto se aprecia en las previamente mencionadas "*Scrum"* y *"DevOps*".

Plan de Capacitaciones

Establecer un debido proceso de capacitación e inducción debe ser prioridad para toda empresa, específicamente en esta propuesta se abordará uno de los temas principales a nivel de concientización de usuarios, la ingeniería social, esta es una de las principales metodologías utilizadas por los atacantes debido a que puede ser relativamente sencilla de aplicar, debido a esto se debe realizar una capacitación constante para reducir su probabilidad de ocurrencia.

CAP – 1. Capacitaciones de Ingeniería Social

Objetivo.

a) Definir un proceso de capacitación contra ataques de ingeniería social para los colaboradores de las Pymes.

Procedimiento.

a) Se deben definir aquellas tácticas comúnmente utilizadas por atacantes con el fin de obtener información o hacer que las víctimas realicen alguna otra acción indebida de forma inadvertida.

- *Vishing* (Estafas telefónicas): esta técnica consiste en intentar obtener información de usuarios de una plataforma especifica mediante la personalización de un agente de servicio a través de una llamada telefónica, usualmente estas se hacen pasar por miembros de entidades bancarias, reportando situaciones de alto impacto para las víctimas.
- *Phishing* (Estafas electrónicas): el phishing es un método a través del cual los atacantes envían un correo electrónico con archivos adjuntos u enlaces a sitios web controlados por ellos, con la intensión de que la víctima interactué con los archivos o vínculos adjuntos, como formularios y archivos infectados con *malware.*
- *Wattering Hole* (Pozo de agua): usualmente son sitios web haciéndose pasar por portales réplicas al original con la intención de obtener datos de los usuarios, cambiando únicamente una parte de su funcionalidad y el dominio en el que estas están expuestas, cabe mencionar que para personalizar una página los atacantes realizan un proceso de análisis por los atacantes para identificar que tenga un alto flujo de tráfico e interacción por parte de usuarios externos.
- *Dumpster Diving* (Búsqueda en la basura): a pesar de ser un método poco ortodoxo, algunos atacantes llegan a buscar en la basura de las empresas con el fin de encontrar documentos confidenciales en ella, como archivos bancarios, estados financieros, usuarios y otros archivos de valor.
- *Shoulder Surfing* (Mirar por encima): Es una acción que implica que una persona maliciosa busque formas de observar de forma desapercibida las

acciones de otra persona, identificando contraseñas o usuarios de portales y plataformas personales o empresariales.

- *Tailgating* (Seguir a la persona): Mediante esta acción un atacante no autorizado puede llegar a ubicaciones poco accesibles y privadas fingiendo ser un colaborador que olvidó los accesos, pretendiendo ser un acompañante de un ingresante o incluso personificar a una persona con prisa o con una función tercerizada como empleados de aseo o mantenimiento.

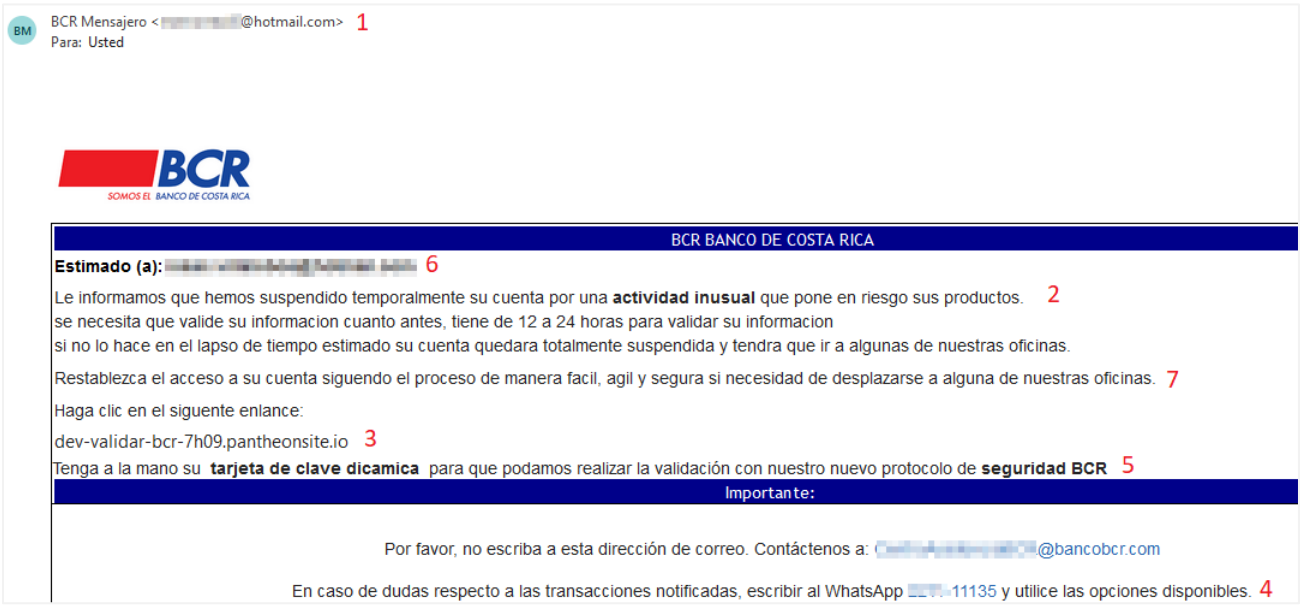
b) Principios de la ingeniería social: según Weiss (2020), los atacantes tienen ciertos principios de actuación para esta clase de ataques, los cuales son:
    - Autoridad: asumen un rol de autoridad sobre las personas, como policías o directores.
    - Intimidación: los atacantes toman un rol amenazante, pueden indicar consecuencias de no seguir sus instrucciones.
    - Consenso: el atacante puede aprovecharse de las conexiones sociales de las victimas para pretender ser parte del grupo de las otras personas.
    - Urgencia: crean condiciones de necesidad en cortos plazos de tiempo para hacer que la víctima tome decisiones rápidas.
    - Familiaridad: un atacante puede usar sus habilidades sociales para crear un nivel de familiarización y confianza con la persona.
    - Confianza: al existir una relación con el atacante, las victimas suelen entrar en una posición de confianza, llegando a mencionar datos privados, según este busque e indague información.
c) Crear en conjunto con las jefaturas de área o socios comerciales una presentación obligatoria para sus colaboradores, se pueden utilizar *softwares* como *PowerPoint* o *Canva* para su elaboración.
d) Dentro de esta presentación se deben incluir los posibles indicadores que se deben observar para reconocer ciertos tipos de ataques de ingeniería social y reducir su nivel de exposición:
    - *Vishing* (Estafas telefónicas): la capacitación y cultura es una de las principales contramedidas, la mayoría de estas estafas se dan debido a

descuidos y falta de información, nunca se deben proveer datos privados por una llamada telefónica.

- *Phishing* (Estafas electrónicas): es uno de los métodos más fuertes y comunes en la ingeniería social, siendo este el principal vector de ataque dirigidas a ciertas organizaciones, por lo que es primordial que exista una correcta concientización debido al riesgo que puede significar descargar un archivo infectado de *malware* en una infraestructura de red, a continuación, se muestra un ejemplo de cuales son todos aquellos puntos observables cuando se recibe un correo en general.

Figura 37.

Ejemplo de correo malicioso / Phishing



Fuente: Correo de *phishing* real recibido en el correo del autor.

1. Fuente o remitente: Verificar específicamente el correo de la persona que envío el correo y verificar que el dominio (dígase dominio el “hotmail.com”) sea de un remitente completamente válido y asociado a la entidad personificada
2. Aplicación de principio de urgencia e intimidación: tal y como se mencionó antes, estos principios son utilizados para causar que la víctima se sienta amenazada y asustada y se vea “obligado” a ingresar al enlace.

3. Vinculo: El enlace al que estos atacantes piden entrar no es uno utilizado por la entidad y mucho menos seguro, a veces estos enlaces vienen incluidos en una leyenda de “click aquí”, se recomienda que se coloque el cursor sobre el enlace sin dar el “click” sobre este para ver el enlace al cuál se le estará redirigiendo.
4. Números telefónicos: el número ingresado para “consultas” es completamente inválido, en Costa Rica no se utilizan números telefónicos con más de 8 números.
5. Solicitud de datos: Los datos que se piden son completamente privados y por políticas de algunas entidades, estos no se pueden pedir, se recomienda acudir a los proveedores para consultar qué datos se solicitan en caso de un incidente real.
6. Saludos y comentarios genéricos: El saludo utilizado en el correo únicamente menciona el correo del remitente, lo que lo hace poco realista, muchas entidades utilizan el nombre completo de la persona al ocurrir un evento similar.
7. Faltas ortográficas: en este caso los atacantes cometieron errores de redacción debido a que las palabras “ágil” y “fácil” se tildan, lo que resta credibilidad al correo.

- *Wattering Hole* (Pozo de agua): Verificar siempre los sitios a los cuales se accede, en especial si se busca el mismo a través de Google, ya que no todos los sitios originales aparecen de primero en las búsquedas, los atacantes pueden pagar por publicidad y hacer que su sitio malicioso aparezca de primero, así mismo, si se ingresa manualmente el enlace en el navegador, verificar que este, esté bien escrito.
- *Dumpster Diving* (Búsqueda en la basura): incinerar o desechar apropiadamente todos los documentos que puedan incluir información confidencial, así mismo al desechar equipos, se pueden utilizar *softwares* como DBAN (*Darik’s Boot and Nuke*) para hacer un borrado completo de la información, o bien magnetizar el disco duro.

- *Shoulder Surfing* (Mirar por encima): estar consciente de los alrededores y las personas que pueden o no tener visibilidad a estos, en caso de ingresar a plataformas en lugares públicos, se debe de intentar escribir la contraseña rápidamente y siempre bloqueando con el cuerpo (espalda cabeza) el teclado y la pantalla.
- *Tailgating* (Seguir a la persona): tener conciencia de los colaboradores de la empresa y nunca dejar pasar a una persona sin una autorización previa o sin un carnet válido de la empresa.

e) Estas capacitaciones deben ser impartidas por personas con un nivel alto de concientización y cuidado debido a que algunos de estos ataques son muy difíciles de detectar y prevenir.

f) Realizar capacitaciones al menos dos veces al año a toda la Pyme.

CAP – 2. Fase de Pruebas

Objetivo.

a) Establecer un procedimiento correcto de pruebas, con el fin de corroborar que las capacitaciones son efectivas.

Procedimiento.

a) Plataformas como "*KnowBe4"* o "*ZPhisher*" (ambas son licencias pagas) pueden ser utilizadas para poner a prueba que los colaboradores verdaderamente pongan en práctica los conocimientos recibidos.

b) Se pueden considerar proveedores de pruebas de seguridad (pruebas de penetración) para realizar esta clase de pruebas

c) Antes de realizar estas pruebas es recomendable haber impartido capacitaciones a la empresa como mínimo dos meses antes y máximo seis meses.

d) De ser posible incluir dentro del ejercicio a toda la organización.

e) Definir escenarios que realmente se puedan materializar (correos pretendiendo ser de áreas de recursos humanos, tecnologías de información u ofreciendo beneficios o incentivos).

f) Exigir al proveedor de servicios (en caso de haber seleccionado uno) un reporte técnico detallando la cantidad de personas que cayeron y los datos ingresados por estos, esto para evaluar la efectividad de las capacitaciones brindadas.

Consideraciones. Debido a los altos precios que pueden llegar a tener esta clase de pruebas es recomendable que las mismas sean efectuadas por Pymes con tamaños e ingresos considerables, siempre realizando un estudio del mercado previamente para establecer un presupuesto.

Políticas y Buenas Prácticas

Toda empresa, independientemente de su tamaño o ingresos debe crear sus propias políticas y procedimientos internos para delimitar el alcance de los roles y establecer formas esperadas de comportamiento, así mismo, aplicar buenas prácticas utilizadas mundialmente, puede evitar que se den eventos que pueden resultar en la materialización de un riesgo.

POL – 1. Políticas de Contraseñas

Objetivo.

a) Diseñar la estructura de una política de contraseñas robusta, estableciendo el proceso para su cambio, longitud, repeticiones y complejidad, según los mejores estándares.

Procedimiento.

a) La política de contraseñas debe ser aplicada a todos aquellos colaboradores que formen parte activamente de la empresa.
b) Como mínimo una contraseña segura debe de contar con los siguientes requerimientos:
    - 11 a 14 caracteres como mínimo.
    - Combinar letras, caracteres especiales y números.
    - Utilizar letras mayúsculas intercaladas en la contraseña.
    - Utilizar al menos dos caracteres especiales.
    - No repetir palabras o números.
    - Evitar usar palabras o frases muy conocidas como “password” o “a1b2c3d4…”
        i. Ejemplos (Estas son solo de ejemplo y no deben de utilizarse): “DirectivaEmpresarial/2023/Adm1n”, “ReglasDeC0mportamiento19783-”
c) En caso de que se manejen una gran cantidad de contraseñas o con un grado de complejidad muy elevado es recomendable optar por una solución de gestión de contraseñas como Kaspersky, LastPass, entre otras.

d) Una contraseña no se debe repetir al menos en un año.
e) Realizar un cambio obligatorio de contraseñas como máximo cada tres meses, este plazo comenzará a aplicar desde el momento en el que se enrola el usuario en el directorio activo de la empresa, de forma que los cambios de contraseñas son completamente independientes entre usuarios.
    - Esta es una política que se puede configurar en las "políticas de grupo" de un directorio activo.

Beneficios. Contar con una alta rotación de contraseñas, así como incrementar su complejidad aplicando las medidas mencionadas anteriormente puede evitar que en el caso de que se hayan dado filtraciones previas de datos, se genere algún incidente, así mismo esta clase de políticas puede hacer más complejo el proceso de descifrado a un atacante real.

POL – 2. Políticas de Endurecimiento de Equipos

Objetivo.

a) Crear una lista de configuraciones básicas seguras que deben de implementarse internamente, basadas en vectores de ataques comúnmente analizados por un atacante.

Configuraciones Comunes.

a) Versión utilizada del protocolo SMB: en algunos equipos se utiliza por defecto la versión 1 de este protocolo (utilizado comúnmente para compartir recursos en la red), es imperativo utilizar la versión más reciente, esta corresponde a la 3.1.1.
b) Contraseñas: Considerar la implementación de las medidas detalladas en "POL – 1. Políticas de Contraseñas" no solo en cuentas de dominio, si no a nivel general para todos los usuarios utilizados.
c) Cuentas por defecto: Muchos equipos de red, como *routers* y *firewalls* vienen con usuarios preconfigurados por defecto, es importante cambiar las contraseñas de estos o bien desactivar el usuario del todo.
d) Protocolos de resolución de nombres: el uso de protocolos como LLMNR y NBT-NS es considerado inseguro debido a las vulnerabilidades asociados a ellos, presentes usualmente en redes *Windows*, por lo que es recomendable desactivarlos del todo, en caso de no ser posible, se deben de implementar redes de control de acceso o "NAC".

e) Uso de protocolos de certificados obsoletos: usualmente en arquitecturas de aplicaciones internas es común encontrar protocolos como SSL (todas sus versiones) o TLS 1.0 y 1.1, los cuales son consideras inseguros debido a que la interceptación de tráfico encriptado con estos puede llegar a ser descifrada, es recomendable utilizar TLS 1.2.
f) Habilitar la firma obligatoria del protocolo de SMB: pese a que esta vulnerabilidad es catalogada por entidades como FIST y Tenable con una criticidad “Media”, una explotación exitosa, permite el compromiso completo del equipo y de la red en general, aunque requiere de ciertas condiciones para poder ser explotada. Usualmente encontrada en equipos de trabajo como laptops y máquinas virtuales que no sean servidores.
g) Desactivar protocolos de acceso de Telnet: telnet es un protocolo de acceso remoto en los equipos de red, este se considera inseguro debido a que transmite las credenciales usadas para iniciar sesión, así como tráfico sin protección alguna, en su lugar utilizar SSH, la versión segura de este.
h) Verificar los servicios activos: Solo se deben tener activos los servicios y puertos necesarios para el funcionamiento básico del servidor, muchos servicios habilitados por defecto como “hecho” pueden representar un riesgo en el servidor
i) Actualizaciones de seguridad de *Microsoft* (Boletines): este es una de las primeras cosas que verifican los atacantes al tener acceso a la red, ya que una gran mayoría de estos boletines son considerados críticos e imperativos, entre los que se encuentran ataques muy reconocidos como *WannaCry, Bluekeep, EclipsedWing y PrintNigthmare.*
j) Actualizaciones de *firmware* y *software*: un vector muy común utilizado por atacantes, debido a que es muy común que ciertas empresas no mantengan su infraestructura actualizada, debido a lo que esto conlleva (en ocasiones pérdidas de información) sin embargo, aplicar actualizaciones constantemente es primordial para mantener los equipos seguros.

Consideraciones.

a) Aplicar esta clase de configuraciones deben ser supervisadas por profesionales o personas que tengan conocimiento del tema, así como establecer puntos de

restauración y respaldos, esto debido a que una implementación sea exitosa o fallida puede resultar en otras vulnerabilidades asociadas e incluso afectar el funcionamiento de los servicios internos resultando en fallos en integraciones con otras aplicaciones y en pérdidas de información.

b) Es recomendable crear documentación de todas las configuraciones de líneas base (*hardening*) e instalaciones presentes en los equipos o aplicaciones importantes para el negocio.

POL – 3. Políticas de Escritorio Limpio

Objetivo.

a) Detallar los apartados mínimos por incluir en una política de escritorio limpio.

Procedimiento.

a) Una política de "escritorio limpio" se refiere a que en el espacio de trabajo del colaborador de únicamente debe haber aquellos documentos requeridos para su trabajo.
b) En el momento de levantarse el colaborador de su zona de trabajo debe de ocultar los documentos privados con los que estuviese trabajando.
c) Evitar dejar la máquina de trabajo desbloqueada y accesible para cualquier otra persona en caso de levantarse y abandonar temporalmente su zona de trabajo.
d) No se debe permitir el uso de "notas" adhesivas con contraseñas o usuarios en zonas expuestas como monitores, teclados o escritorio, estas deben ser igual de resguardados que los demás documentos y en caso de contar con él, usar un gestor de contraseñas.
e) No se debe permitir que los colaboradores usen vasos sin tapa o botellas sin tapa en su zona de trabajo.
f) El colaborador debe mantener su zona de trabajo completamente limpia y sin residuos de comida o demás basura como envolturas, migajas papeles, entre otros.

POL – 4. Políticas de Uso Aceptable de Cuentas

Objetivo.

a) Detallar los apartados mínimos a incluir en una política de uso aceptable de cuentas laborales.

Procedimiento.

a) Se le debe asignar una cuenta corporativa al usuario, esto incluye la creación de este en el directorio activo e incluye creación de correo corporativo y usuario de dominio.
    - Estas cuentas deben realizarse siguiendo una nomenclatura predefinida, ejemplo: para el usuario Ryan Martínez de la empresa Pymex se tiene que el correo es: "ryan.martinez@pymex.com" (nombre.apellido@dominio.com), y su usuario de dominio: "rmartinez" (inicial del nombre + primer apellido).

b) Se espera que la cuenta (específicamente el correo) sea únicamente utilizada para fines laborales.

c) El correo corporativo no debe ser utilizado para crear cuentas en redes sociales sin previa autorización y únicamente debe ser autorizado en casos especiales como colaboradores de áreas de *marketing.*

d) El correo corporativo debe mantenerse privado y no debe ser compartido públicamente.

e) Crear cuentas específicamente para el manejo de servicios (como redes sociales) o comunicaciones generales con potenciales clientes u otras áreas internas.
    - Por ejemplo: marketing@pymex.com, ventas@pymex.com.

f) No utilizar el correo corporativo como método de traslado de información a cuentas personales, esta acción es penalizable y en caso de ser definida así en "

g) POL – 10. Acuerdos de Confidencialidad (NDA)" puede ser una justa causa de despido, si se detecta una filtración de información confidencial.

h) Evitar utilizar cuentas de plataformas asociadas al correo corporativo con fines personales, a menos que estas sean plataformas de autoestudio u otras como licencias de Office (estas no deben ser utilizadas o accedidas desde máquinas ajenas a la organización, sin una previa autorización).

POL – 5. Políticas de Contrataciones y Finiquitos Laborales

Objetivo.

a) Detallar los apartados mínimos por incluir en las políticas de contrataciones administrativas y finiquitos de contrato.

Procedimientos de Contratación de Personal.

a) Se pueden utilizar diversos *sitios web* para promover la búsqueda de contrataciones laborales
b) Se reciben y analizan las solicitudes acompañadas de las hojas de vida (CV).
c) Para cada uno de los perfiles tomados en cuenta se deben investigar la experiencia y antecedentes penales (pueden existir otros asuntos relevantes).
d) Realizar una serie de entrevistas con el personal encargado de realizar la contratación (recursos humanos y el área para la que se busca el puesto directamente).
e) En caso de que este sea contratado, se deben firmar acuerdos de confidencialidad para evitar una posible exfiltración de datos, así como una carta de responsabilidad de activos, en esta última se define que los colaboradores deben velar por el cuidado y seguridad de los activos utilizados.
f) Asignar y acordar una fecha de ingreso junto con el futuro colaborador.
g) Se debe realizar un proceso de inducción a la empresa, así como recibir las capacitaciones de cuáles serán sus funciones métricas establecidas, así como otras inducciones en material de ciberseguridad.

Procedimientos para Realizar Finiquitos de Contratos.

a) Se considera un periodo de tres meses como un plazo de prueba, por lo que es posible que, durante este lapso, el empleador pueda tomar la decisión de rescindir de las funciones de los colaboradores.
b) Después de los tres meses, si se decide despedir al colaborador se pagan todos los dividendos correspondientes a la cesantía, preaviso, aguinaldo y vacaciones en caso de que se dé un despido sin justa causa laboral, en caso de que haya una justa causa, únicamente se pagan aguinaldo y vacaciones.
c) En caso de que se dé un despido los accesos otorgados a este usuario a todas las distintas plataformas y servicios de la empresa deben ser desactivados.

POL – 6. Políticas para el Provisionamiento de Permisos

Objetivo.

a) Diseñar un correcto procedimiento para el provisionamiento de accesos y permisos internos a los usuarios.

Procedimiento.

a) Junto con el equipo técnico de la Pyme se deben crear los accesos y usuarios correspondientes al nuevo colaborador en caso de haberlo.
b) Asignar una máquina de trabajo (en caso de requerirlo) al nuevo colaborador y actualizar el documento de inventario de activos.
c) Aprovisionar el usuario previamente creado con todos aquellos privilegios necesarios para realizar su trabajo siguiendo el principio de ciberseguridad de "*least privilege*" o privilegio mínimo, lo que indica que únicamente se deben asignar recursos si su labor diaria realmente lo necesita.
d) Toda asignación de permisos debe ser bien segmentada, definiendo roles de administrador sobre ciertas plataformas a la menor cantidad de personas posibles, en especial en áreas de tecnologías de información.
e) No se deben asignar privilegios específicamente basados en puestos altos, las personas que tengan puestos de jefaturas o ejecutivos como socios del negocio no deben tener acceso a todas las plataformas o equipos de la empresa, ya que estos son usualmente buscados por atacantes para ejercer un método variante del "*phishing*", el conocido "*whale phishing*" el cuál se enfoca exclusivamente en las personas ejecutivas de la Pyme.
f) En el momento en el que una persona abandona o adjudica a su puesto dentro de la empresa todo acceso que este haya tenido junto con su equipo asignado deben ser revocado, la información contenida en el o los equipos asignados no debe ser borrada del equipo por parte del colaborador.

POL – 7. Políticas para el Trabajo Remoto

Objetivo.

a) Diseñar un correcto procedimiento para la creación de una política para permitir el trabajo desde ubicaciones remotas a las oficinas de la Pyme.

Procedimiento.

a) El trabajo remoto se ha vuelto tendencia, en especial después de la pandemia del Covid-19, lo que dio como resultado que las empresas opten por esta clase de forma de trabajo para reducir una posible exposición y afectación del virus.

b) Dependiendo del tamaño, el foco de negocio de la Pyme y la función del colaborador puede que esta opte por evitar gastos de operación adicionales como el mantenimiento de servidores físicos, servicios de misceláneos (mantenimiento y limpieza), entre otros, estos presupuestos son ahorrados y utilizados para mejorar áreas y servicios que la empresa provee.
c) Crear una conexión VPN a la red interna de la organización, esta configuración técnica debe ser realizada por una persona con conocimientos técnicos debido a la complejidad de su configuración.
d) Configurar este acceso para que el proceso de autenticación requiera de un factor múltiple de autenticación conocido como" MFA" (*Multi-Factor-Authentication*).
e) Se debe otorgar un acceso o cliente VPN a los colaboradores que puedan ejercer su trabajo de forma remota, siempre con los principios descritos anteriormente.
f) El colaborador beneficiado debe mantenerse activo y alcanzable durante la jornada laboral, así mismo se debe garantizar conexión a internet estable y continua.
g) El colaborador debe comunicar la ubicación principal desde la cual estará laborando (su casa o alguna otra locación), en caso de que este labore desde otra ubicación distinta deberá comunicarlo a su superior.
h) Debe ser obligatorio en caso de trabajar conectado a redes de internet públicas, conectarse a la red VPN de la empresa para evitar posibles ataques de *Man-in-the-Middle* (Intercepción de datos).

POL – 8. Políticas para el Manejo de la Información

Objetivo.

a) Definir los niveles de clasificación de la información y cómo debe ser manejada por los colaboradores.

Procedimiento.

a) La información puede ser clasificada en cuatro distintos niveles o clasificaciones: Confidencial Externa, Confidencial Interna, Operativa y Publica.
    - Confidencial externa: es toda aquella información que debe mantenerse estrictamente privada o confidencial y únicamente debe ser vista por las partes interesadas como clientes, proveedores y otros miembros de la Pyme que

estén involucrados en el proyecto, por lo general los documentos con esta clasificación tienen una marca de agua.

- Confidencial interna: se refiere a todos aquellos datos o documentos que deben mantenerse completamente privados dentro de la organización y no deben salir de la empresa, por lo general los documentos con esta clasificación tienen una marca de agua.
- Operativa: es información utilizada diariamente para que los colaboradores cumplan sus funciones, pese a que estos datos son algunos utilizados de forma interna y deben mantener cierto nivel de confidencialidad; no suelen representar un riesgo real si estos son filtrados debido a que no contienen ninguna información de alto riesgo.
- Pública: esta clase de datos son de carácter completamente público y están dirigidas a potenciales clientes o colaboradores, estos no representan riesgo alguno y únicamente son de carácter completamente informativo.

b) Clasificar apropiadamente la información puede evitar las filtraciones de datos accidentales.

c) Si se debe compartir información confidencial interna con otros colaboradores de la empresa, se recomienda aplicar el principio de "*need-to-know*", el cual indica que solo se deben de compartir aquellos datos que sean necesarios para que este complete su función, evitando que este sepa información confidencial de forma innecesaria.

d) En caso de que la Pyme pueda asumir un gasto de esta clase, se pueden configurar soluciones de "DLP" (*Data Loss Prevention*) que pueden evitar que se filtre información a través del intercambio de correos electrónicos según la clasificación asignada al documento.

POL – 9. Estudio de Mercado

Objetivo.

a) Crear una práctica de estudio de mercado para analizar la competencia del negocio.

Procedimiento.

a) Dependiendo del foco de negocio de la Pyme puede que se encuentre muchos adversarios durante el proceso de consolidación y establecimiento.

b) Definir la idea de negocio principal y los productos o proyectos en los cuales la Pyme incursionara.
c) Se debe realizar un estudio local y regional, tomando en cuenta que se pueden analizar los siguientes puntos:
    - Nivel técnico de colaboradores.
    - Movimiento en redes sociales (*Marketing* digital).
    - Promociones y precios promedios.
    - Hacía qué población están dirigidas.
    - Alianzas estratégicas.
    - Experiencia y calidad de la atención, servicio o productos.
d) Se debe priorizar la entrega de calidad en cada uno de los servicios o productos comercializados.
e) Con base en este estudio se puede definir una estrategia comercial, para volver a incursionar dentro del foco de la Pyme, abarcando planes de servicio, atracción de potenciales clientes, mejora de productos o servicios o incluir dentro del catálogo de servicios alguno que no sea encontrado tan fácil dentro de la región inicial.
f) Parte importante de realizar un estudio de mercado incluye aplicar un análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) del negocio como tal:
    - Fortalezas (Internas): En este apartado la Pyme debe de identificar todos aquellos puntos fuertes, los cuales la puedan hacer destacar por sobre la competencia del negocio, estos pueden incluir personal altamente capacitado, mejores precios, alianzas estratégicas.
    - Oportunidades (Externas): Las oportunidades se refieren a todos aquellos puntos explotables de los cuales se pueden aventajar la Pyme para su crecimiento, dentro de estos puntos se incluyen opciones de mejora en sus servicios, mercados poco explorados y potenciales alianzas con otras empresas.
    - Debilidades (Internas): Son todos aquellos puntos que tiene que mejorar la empresa para proveer un mejor servicio o mejorar la calidad de sus productos, estas debilidades pueden llegar a afectar por completo, a la hora de competir contra otras empresas.

- Amenazas (Externas): Las amenazas son todos aquellos puntos que pueden llegar a representar un peligro para la Pyme, sus operaciones y sus finanzas, parte de identificar estos puntos es asociarlas a las debilidades de una forma más externalizada

POL – 10. Acuerdos de Confidencialidad (NDA)

Objetivo.

a) Definir los lineamientos a los cuales aplican los acuerdos de confidencialidad

Procedimiento.

a) Establecer un acuerdo de confidencialidad en el momento de la incorporación de un nuevo colaborador, independientemente de su posición o área a la que pertenece, la información que maneja internamente sobre clientes y otros datos debe mantenerse estrictamente confidencial.
b) Dependiendo del foco de negocio, este debe orientarse a la clase de proyectos que se manejen.
    - Si se dan servicios de *outsourcing* de auditoría, es muy posible que los clientes soliciten la firma de acuerdos de confidencialidad adicionales a los utilizados internos, dándoles a estos la garantía de que sus datos estarán completamente seguros.
c) Hacer obligatoria la firma de estos acuerdos para todos aquellos colaboradores que manejen información privilegiada y confidencial.
d) Algunos de los apartados que deben ser incluidos en esta clase de documentos son:
    - Las partes o los interesados en la firma del documento.
    - Un segmento especificando qué clase de información entregada o recopilada debe mantenerse privada.
    - En caso de que haya alguna exclusión con respecto a los datos se debe indicar dentro del documento.
    - El plazo de tiempo por el cuál será válido el documento.
    - Los usos permitidos de la información.
    - El proceso apropiado por el cual se harán los traslados de la información en caso de requerirlo.

- En el caso de Costa Rica se deben enunciar y citar las leyes correspondientes, esta corresponde a la ley N.7975 de la Procuraduría General de la Republica.
- Resolución de conflictos en caso de que se dé un rompimiento de acuerdos.

POL – 11. Establecimiento de Presupuestos y Metas

Objetivo.

a) Guiar en el proceso de ajuste de presupuestos para las distintas áreas del negocio.

Procedimiento.

a) Inicialmente se debe establecer un periodo de tiempo mínimo de un año, durante el cual se estarán trabajando nuevas ideas.
b) En conjunto con las jefaturas de las áreas de la empresa y la parte ejecutiva debe realizarse una reunión de revisión general, esta debe servir como una generación de nuevas iniciativas para mantener o impulsar el crecimiento Pyme en el periodo definido.
c) Cada área debe crear un plan de crecimiento o de nuevas iniciativas para mejorar su área y por ende a la empresa, dichos planes pueden ser:
    - Nuevos servicios.
    - Contratación de nuevos colaboradores.
    - Alianzas estratégicas
    - Obtener una certificación empresarial (ISO 27001, ISO 9001, "*Best Place for Work*", "esencial Costa Rica", entre otras).
    - Mejoras internas.
    - Metas de ventas o ingresos.
b) En estas metas las áreas pueden solicitar acordar un presupuesto aproximado para cumplirlas y al final del periodo se debe hacer un desglose del gasto de dicho presupuesto en caso de que este fuese aprobado por los directores de la empresa, este monto puede ser aumentado o reducido según el cumplimiento de las metas.
d) Establecer metas de ingresos en mercados muy competitivos puede ser complejo, sin embargo, es recomendable complementar esto con un análisis de mercado de competidores REALES (en la misma categoría tanto de servicios como tamaños aproximados) de la Pyme para obtener una media.

e) Establecer sesiones de seguimiento para medir el nivel de avance y si las metas establecidas al inicio del periodo pueden o no ser alcanzadas.

Beneficios. Mantener este proceso de forma cíclica le permite a la empresa mantenerse aplicando mejoras continuas y convertirse en un competidor real del mercado e incluso expandirse a nuevas regiones según su proyección.

Recuperación a Ataques y Desastres informáticos

Desarrollar un plan de recuperación y de respuesta a incidentes y desastres es algo esencial y variable en toda empresa según su foco de negocio, tomando en cuenta que las empresas cada vez más adoptan metodologías de trabajo remoto y optan por virtualizar su infraestructura para reducir gastos, se procederá a desarrollar únicamente aquellas acciones y planes que se pueden realizar en temas informáticos.

RES – 1. Identificación y Respuesta de Incidentes Informáticos

Objetivo.

a) Crear un proceso para identificar posibles ataques en la red.

Procedimiento.

a) Es importante contar con un *software Antivirus* o *Antimalware* en la red, estos pueden detectar intrusiones en los equipos y prevenir esta clase de eventos, sin embargo, deben mantenerse actualizados y revisados constantemente, debido a los registros que estos generan.
b) Los registros o "*logs*" generados por esta clase de aplicaciones puede permitirle a un analista de red determinar la existencia de un ataque.
c) Si la Pyme cuenta con cierta capacidad técnica y la posibilidad de tener un equipo de ciberseguridad o de tecnologías de información se pueden centralizar estos registros en un *SIEM*, este les permite a los analistas revisar eventos específicos que pueden ser considerados como indicadores de compromiso (IoC), algunos de los que son comúnmente revisados y registrados y alertados son:
    - Tráfico de red, conexiones entrantes y salientes a los equipos.
    - Eventos y acciones auditables.
    - Correo y sus datos o archivos adjuntos.
    - Puntos de conexión de los equipos.
    - Cantidad de conexiones a servicios y a la red.

- Cantidad de intentos de inicios de sesión

d) Dentro de las capacidades del SIEM esta alertar ante la existencia y aparición de los IoCs, estos pueden ser configurados en el sistema, dependiendo del tipo y solución de SIEM, adquirida estas alertas, pueden resultar como falsos positivos molestos (usualmente estos se presentan más frecuentemente en licencias gratuitas o "*Open Source*").
e) En el momento que se detecta y confirma actividad sospechosa, la máquina infectada debe ponerse en cuarentena (desconexión de la red interna de la empresa o VPN en el caso remoto) y el equipo encargado de tratar con el incidente debe indagar una posible propagación en la red y el impacto que este puede tener.
f) En una red aparte se debe analizar el evento y correr múltiples escaneos con herramientas de AntiVirus para sanitizar el equipo.
g) Tras un delicado análisis en la otra red, se puede confirmar si la amenaza fue erradicada o bien si se deben tomar acciones adicionales, en caso de que esta haya sido neutralizada se debe realizar un análisis extra manual en el equipo para remover posibles archivos infectados.
h) Los posibles archivos infectados respaldados por el usuario víctima deben ser puestos en cuarentena y analizar si estos son o no seguros.
i) Si se detecta a tiempo, se debe notificar rápidamente a todos los terceros que pudiesen ser afectados por el ataque.
j) Debe establecerse un plan de continuidad de negocio, el cual le indique a la empresa cuáles acciones tomar para mantener las operaciones del negocio durante el incidente.
k) Es recomendable crear "*playbooks*" o libros de jugadas, para definir las acciones que se tomarán al materializarse alguno de los eventos definidos, se deben definir estos planes de acción para cada uno de los eventos informáticos que se puedan presentar.
l) En caso de ser posible y que la magnitud del evento lo amerite se pueden optar por servicios de examinación forense informático.

RES – 2. Plan de Recuperación de Desastres Informáticos

Objetivo.

a) Diseñar un plan de recuperación básico ante ataques informáticos

- Un plan de recuperación debe indicarle a la empresa cómo levantar y mantenerse completamente operativa, durante y después de un incidente sin afectar sus negocios actuales.

Procedimiento

a) Tras haber detectado el ataque hay que tomar medidas inmediatas, mencionadas en el punto “Desarrollar un plan de recuperación y de respuesta a incidentes y desastres es algo esencial y variable en toda empresa según su foco de negocio, tomando en cuenta que las empresas cada vez más adoptan metodologías de trabajo remoto y optan por virtualizar su infraestructura para reducir gastos, se procederá a desarrollar únicamente aquellas acciones y planes que se pueden realizar en temas informáticos.

b) RES – 1. Identificación y Respuesta de”,

c) Al crear esta clase de planes se recomienda establecer libros de jugadas o “*playbooks*”, abarcando la forma aprobada por la empresa para manejar riesgos o desastres probables en los cuales la información o servicios se puedan ver comprometidos, comúnmente en estas guías se incluyen los siguientes apartados:

    - Roles: se identifican todos aquellos involucrados dentro del proceso, usualmente son gerentes de área y personal técnico de la empresa.
    - Preparación: son todas aquellas previsiones que se toman para evitar que se materialice el riesgo, pueden ser soluciones de *hardware* o de *software*.
    - Identificación: se define el proceso para concluir que la amenaza se materializo y está afectando los sistemas o activos.
    - Contención: se establecen los lineamientos para mantener el alcance de la amenaza limitada y contenida.
    - Mitigación: todos los esfuerzos que se deben realizar para eliminar y neutralizar la amenaza.
    - Recuperación: son todas aquellas prácticas realizadas por la empresa para reestablecer sus operaciones a un punto aceptable, incluyendo la aplicación de respaldos y levantar todos los servicios afectados inicialmente.
    - Lecciones aprendidas: al concluir este proceso de recuperación y respuesta se debe realizar un último paso que debe definir cuáles fueron las situaciones que

pudieron haber sido mejor abordadas durante la ejecución y recibir una retroalimentación de todos los involucrados.

d) Siguiendo buenas prácticas se recomienda establecer inicialmente un equipo de respuesta a incidentes, usualmente este se conoce como CSIRT, un equipo de este tipo puede implicar inversiones elevadas, para efectos de una Pyme, se pueden detallar aquellas personas que estarán a cargo de poner en práctica el plan desarrollado.
    - Usando el ejemplo del organigrama detallado en "RAC – 1. Definición de roles y puestos internos" dentro de este equipo se involucran los gerentes del área de TI, el director general y el director de la o las áreas que puedan verse afectadas.

e) Responder ante un incidente puede implicar la incorporación o la tercerización de un equipo de otra empresa externa (proveedores) mediante tratados de SLA (*Service Level Agreements*), esto puede ayudar a la empresa durante la respuesta y su recuperación ante un evento, especialmente si esta no cuenta con conocimientos del tema.

f) En cuanto se logre contener el ataque conviene cuantificar y dimensionar la magnitud del impacto en términos financieros, identificando cuál puede ser el costo aproximado de recuperar los activos, ya sean información u equipos como tal.

g) Analizar todos los respaldos de información disponibles, con el fin de recuperar la mayor cantidad de información en caso de que esta se haya visto integralmente afectada.
    - Aplicando los respaldos fuera de línea o locales realizados, si eventualmente los respaldos en línea de la Pyme, según lo definido en "ILR – 6. Metodología de Respaldo de Información".

h) Buscar restaurar todos los sistemas a un punto de respaldo en la que no haya existido una infección (en caso de que haya sido un evento de este tipo).

i) Si el evento se da a conocer públicamente, la reputación de la Pyme se puede ver afectada drásticamente, llegando incluso a situaciones de alto impacto como la permanencia en el mercado.
    - Definir cuáles son las acciones correspondientes en el caso de que este evento se haga público, esto conviene involucrar directamente a todos los clientes,

cuyos datos privados pudiesen verse afectados, dándoles la mayor claridad de los eventos.

j) Posterior al incidente se analizarán todas las acciones realizadas que resultaron fallidas, exitosas y cuáles se llevaron a cabo o no.

Consideraciones.

a) Desarrollar un plan completo de recuperación de desastres y de respuesta a incidentes puede ser muy complejo para empresas que estén iniciando, sin embargo, siempre es importante definir cuáles son las acciones por tomar y tener contactos en caso de que un riesgo se materialice.

b) El desarrollo de estos planes es recomendable realizarlos con el acompañamiento de profesionales en el área y analizando siempre el foco de negocio de la Pyme, si bien este puede resultar en costos elevados y en una inversión a plazo, estos pueden aportar un gran valor según el crecimiento de la empresa.

c) Según se dé el crecimiento de la Pyme, parte de crear un proceso de recuperación ante un desastre o ataque es establecer RTOs (*Recovery Time Objective*) y RPOs (*Recovery Point Objective*), los cuales son plazos de tiempo y puntos de respaldo de la empresa para recuperar y poner en marcha sus operaciones

RES – 3. Ejercicios de Simulación

Objetivo.

a) Crear ejercicios para poner a prueba los planes de respuesta y recuperación de incidentes informáticos.

Procedimiento.

a) Una vez definido un plan de recuperación y respuesta ante ataques informáticos, este debe ponerse a prueba.

b) Poner a prueba las "*playbooks*" creadas mediante ejercicios de "*tabletop*", estos se pueden definir como una especie de simulación que busca recrear escenarios de riesgo que se puedan dar a nivel organizacional, si bien pueden existir una gran cantidad de "*playbooks*" es recomendable solo realizar ejercicios constantemente y aquellos con mayores probabilidades de materializarse.

c) Para realizar estos ejercicios de forma efectiva se recomienda reunir los involucrados en el plan, en distintos equipos, especialmente el área de TI para discutir y simular estos eventos.
    - Estas simulaciones incluyen ejercicios de crisis, por ejemplo, el *ransomware*, el cuál puede ser uno de los ataques más críticos a nivel informático, debido a la afectación que puede significar, así mismo la denegación de servicios en caso de tener aplicaciones web o móviles públicos de ofrezcan alguna clase de servicio adicional, como compras en línea.
    - Efectuar esta clase de prácticas sin un previo aviso puede poner a prueba la capacidad de la Pyme para poner en práctica sus "*playbook*s" y planes de recuperación, en una situación aún más realista y de esta forma validar que los procesos de respaldo de información se estén realizando constantemente.
    - Realizar esta clase de ejercicios constantemente (trimestralmente o por cuatrimestres).
d) Dependiendo de la capacidad financiera de la Pyme se pueden cotizar ejercicios de *red-team* con empresas de terceros, estos, aunque costosos pueden simular lo que un atacante real podría realizar en la red interna y externa de la empresa, el objetivo principal de esta clase de ejercicio (a diferencia de una prueba de penetración normal) es evaluar la capacidad de respuesta de los controles perimetrales y lógicos establecidos por la empresa.
    - Adicionalmente, existen pruebas de *purple-team* la cuál es un ejercicio controlado en la cual se enfrentan los equipos rojos/red (atacantes) y azules/blue (defensores).

Consideraciones.

a) Las pruebas de penetración, *red-team* o *purple-team* tienen costos elevados en el mercado, por lo que es importante aplicarlas en caso de contar con una infraestructura de red muy amplia o según se vaya dando el crecimiento en la empresa y su foco de negocio, siempre y cuando la empresa o Pyme puedan permitirse esta clase de simulaciones y haya asignado un presupuesto a esta clase de pruebas.
b) Los ejercicios de "*tabletop*" son una práctica importante aplicable desde tempranas etapas de la Pyme, sin embargo, debe existir un área de tecnologías de información.

Vulnerabilidades y Parámetros en Aplicaciones Móviles y Web

Desarrollar aplicaciones se ha vuelto más sencillo a lo largo de los años debido a la gran cantidad de tecnologías y marcos de trabajo utilizables, sin embargo, muchas veces durante el proceso de desarrollo no existe una debida noción de lo importante que es realizar un "desarrollo seguro" y de las repercusiones que esta falta de cultura y conocimiento pueden tener en la aplicación y sus datos.

WEB – 1. OWASP

Uno de los principales exponentes en temas de vulnerabilidades en aplicaciones móviles, web y microservicios es OWASP (*Open Worldwide Application Security Project*), una fundación sin fines de lucro creada con el fin de mantener la seguridad de aplicaciones reconocida mundialmente, sirviendo como asesor y base de datos educacionales. A lo largo de los años OWASP ha desarrollado múltiples guías, recomendaciones, artículos y aplicaciones que son de gran utilidad para poner a prueba el desarrollo de aplicaciones de forma segura

Como bien se mencionó previamente OWASP ha desarrollado múltiples herramientas para propiciar el desarrollo seguro de aplicaciones de todos los tipos, en ciberseguridad (específicamente en las áreas de pruebas técnicas o *pentest*) es reconocida por sus importantes aportes investigativos, determinando cuáles fueron las top 10 vulnerabilidades con más incidencias en un lapso de tres a cuatro años.

Según OWASP (s.f. b), la publicación más reciente de este top ataques realizados datan del año 2021 y se ordenan de forma descendente, a continuación, se listan y resumen dichos vectores:

- A01:2021 – Fallos en el control de acceso: Se refiere a todas aquellas acciones que pueda realizar un atacante para abusar de los privilegios de la aplicación.
- A02:2021 – Fallas criptográficas: Un atacante puede interceptar y visualizar los datos utilizados y enviados por una aplicación no están cifrados o utilizan protocolos y algoritmos de cifrados débiles.
- A03:2021 – Inyección: Este tipo de vulnerabilidades pueden ser explotadas por un atacante si las entradas de texto o archivos no son validadas por la aplicación resultando en la exfiltración de información o demás consecuencias.

- A04:2021 – Diseño inseguro: Son todos aquellos fallos realizados durante el proceso de desarrollo, como falta de documentación y el uso de funciones que no están mapeadas o identificadas.
- A05:2021 - Configuración de seguridad incorrecta: Aspectos a nivel de servidor, son todos aquellos puntos asociados a *hardening* o endurecimiento, servicios innecesarios en ejecución y mal manejo de errores en la aplicación.
- A06:2021 - Componentes vulnerables y desactualizados: las librerías y extensiones y componentes adicionales de la aplicación presentan vulnerabilidades asociadas a funciones específicas de este, que pueden ser explotadas por atacantes.
- A07:2021 - Fallas de identificación y autenticación: Se utilizan credenciales débiles o por defecto, así como falta de sanitización en los parámetros utilizados, permitiéndole a un atacante reutilizar *tokens* de inicio de sesión o *cookies* interceptados para acceder como un usuario autenticado en la aplicación.
- A08:2021 - Fallas en el *software* y en la integridad de los datos: no es una vulnerabilidad que permita la extracción de datos, pero sí su modificación, alterando su contenido original, usualmente ocurre si se utilizan librerías u otros componentes de desarrollo que no sean confiables.
- A09:2021 - Fallas en el Registro y Monitoreo: sin la implementación de herramientas que puedan detener ataques y generar registros o "*logs*" se vuelve imposible detectar actividades o tráfico inusual de red, estos registros deben generarse para cualquier evento que implique acciones importantes del lado de los usuarios.
- A10:2021 - Falsificación de Solicitudes del Lado del Servidor: comúnmente conocido como SSRF (*Server-Side-Request-Forgery*), esta vulnerabilidad le permite a un atacante que controle un servidor malicioso, interceptar una petición de recursos de la aplicación a otra aplicación y alterarla para que esta utilice los recursos del servidor malicioso, con el aumento del uso de integraciones entre aplicaciones, esta vulnerabilidad se vuelve aún más probable y critica.

WEB – 2. Análisis de Código Estático y Dinámico

WSTG (web) y MASTG (móviles) en el Análisis de Código. Adicionalmente al top de vulnerabilidades detallado anteriormente el equipo de analistas de OWASP diseño dos guías específicas para poner a prueba el desarrollo seguro de las aplicaciones mediante ejercicios de

pentest, dichas guías corresponden a la WSTG (*Web Security Testing Guide*) y a la MASTG (*Mobile Application Security Testing Guide*), las cuales son completamente gratuitas y accesibles a través de las publicaciones de OWASP en GitHub.

Estas indican los puntos principales que se deben tomar en consideración para poder tener una aplicación "segura" de forma pública en internet, la creación de estos "*checklists*" ha derivado en una cultura de "desarrollo seguro", así como en distintas metodologías de pruebas que sirven para medir la efectividad de los controles, configuraciones y código que puedan tener las aplicaciones, el análisis de código estático y dinámico, así mismo estas pueden ser utilizadas como un proceso de QA (*Quality Asssurance*) adicional al usarla como una guía de que cosas deben de ser verificadas en la aplicación.

Análisis de Código Estático. El análisis de código estático o SAST (*Static Application Security Testing*) es un escaneo automatizado realizado para identificar fallos y malas prácticas durante el desarrollo que pueden resultar en posibles vulnerabilidades cuando la aplicación sea puesta en ejecución. A diferencia de un análisis dinámico, este se hace con todos los archivos del código en reposo y no requiere de una habilidad de explotación de vulnerabilidades, pese a que este proceso es completamente automatizado, siempre es importante revisar y validar los hallazgos ya que por lo general estas herramientas tienen índices de falsos positivos (vulnerabilidades detectadas que no aplican a la evaluación), algunos de los analizadores más utilizados son *Veracode y Kiuwan*, estos por lo general tienen un costo de licenciamiento elevado, por lo que se puede optar por opciones gratuitas y más accesibles como SonarQube.

Análisis de Código Dinámico. Las evaluaciones dinámicas requieren que la aplicación esté en funcionamiento para su ejecución, adicionalmente implican un nivel más técnico en habilidades de explotación de vulnerabilidades ya que abarcan tanto pruebas manuales como automatizadas, este tipo de pruebas es recomendable realizarlas antes de liberar la aplicación a un entorno de producción, especialmente si la información manejada es financiera (datos bancarios).

Dentro de las actividades que se realizan durante una evaluación DAST (*Dynamic Application Security Testing*) esta es una evaluación de vulnerabilidades mediante pruebas de penetración, la cual pone a prueba el desarrollo seguro de la aplicación, algunas de las herramientas utilizadas para esta clase de pruebas son: *Burp Suite, Nessus, Veracode, MobSF*.

Metodología de pruebas. Estas pruebas usualmente cuentan de cuatro pasos básicos que se desarrollan de forma cíclica según se vayan aplicando actualizaciones en la aplicación, manteniendo un proceso de constante retroalimentación.

a) Reconocimiento: El analista o técnico encargado, se dedica a hacer un reconocimiento en la aplicación o código, con el fin de familiarizarse con él y poder decidir si los hallazgos posteriores pueden ser falsos positivos.

b) Análisis de la aplicación: Es esta fase se realiza la revisión del código o la aplicación, el analista realiza las pruebas o escaneos necesarios para detectar vulnerabilidades, en la gran mayoría de los casos estas se basan en las guías desarrolladas por *OWASP (WSTG y MASTG).*

c) Revisión y presentación de los hallazgos: El analista debe reportar todos los hallazgos considerados como críticos (inyección y ejecución de código remoto, filtrados de información…) según se vayan identificando, finalmente al terminar las pruebas hay que crear un reporte de alto nivel explicando las acciones realizadas y las implicaciones de los hallazgos.

d) Remediación o mitigación: Al recibir este reporte de hallazgos el equipo de desarrolladores debe poner sus esfuerzos en mitigar las vulnerabilidades, priorizando aquellas catalogadas como críticas y altas, durante este proceso el analista encargado de las pruebas puede verse involucrado con un rol de soporte.

WEB – 3. Buenas Prácticas para el Desarrollo Seguro

Durante el proceso de desarrollo de una aplicación, es importante adoptar una postura defensiva, esto con el fin de crear en los desarrolladores de *software* una cultura de "desarrollo seguro", mediante la capacitación constante y aplicando algunas prácticas que permiten crear un código libre de vulnerabilidades, por lo que a continuación se mostraran un top 10 de las mejores prácticas identificadas por el autor:

a) Seguridad en la gestión de errores: Es normal que en el flujo de trabajo de una aplicación se puedan generar errores como descuidos del usuario al ingresar información o incluso intentar realizar o acceder a recursos y funciones que no están asignadas al usuario, para esto lo principal es hacer que la aplicación muestre mensajes de error genéricos al usuario y genere "*logs*" o registros internamente de lo sucedido.

b) Aplicación de principios de seguridad: basarse en puntos clave mencionados previamente como "*least privilege*" y "*need-to-know*" donde solo se le dan permisos al usuario de hacer las funciones mínimas necesarias, así como limitar el acceso a la información confidencial de la aplicación.
c) Pruebas de penetración y evaluaciones constantes: Es importante establecer un programa de pruebas técnicas (en caso de que la Pyme lo puede afrontar económicamente, tercerizándolo o con personal calificado) donde se evalúe la aplicación cada cierto tiempo (al menos un año) o cuando se apliquen actualizaciones o cambios importantes en la aplicación, véase "WEB – 2. Análisis de Código Estático y Dinámico".
d) Capacitación constante: Se debe de procurar que el equipo de desarrollo de *software* se mantenga en una constante capacitación de buenas prácticas para el desarrollo seguro y nuevas tecnologías.
e) Bibliotecas y componentes actualizados: Mantener todos aquellos componentes utilizados por la aplicación debidamente actualizados debe ser prioritario, es importante recalcar que no todos los componentes de aplicaciones reciben actualizaciones constantes, por lo que es prioritario realizar una investigación previa de los boletines de seguridad y vulnerabilidades que pueda o no tener previo a seleccionarlo.
f) Validación y sanitización en las entradas de datos: toda entrada de datos o "*input*" de la aplicación debe de ser verificado y validado, verificando que los datos ingresados por el usuario sean los esperados, limitando de esta forma los archivos o datos que este pueda cargar.
g) Configuración de sesiones y *cookies*: Las *cookies* son una forma en la que la aplicación puede guardar información de la sesión de un usuario para su correcto funcionamiento, estas *cookies* y variables de sesión deben guardar únicamente la información necesaria para su funcionamiento, así mismo a estas se les aplicará configuraciones seguras mediante atributos como "SECURE".
h) Almacenamiento y gestión segura de credenciales: Todas las credenciales requeridas por la aplicación deben ser cifradas, convertidas en un "*hash"* y ser trasladadas a través de protocolos seguros de red como lo es https, durante el proceso de validación

interna del servidor no se deben almacenar estas credenciales como variables de sesión, así mismo, evitar agregar los usuarios y contraseñas de otros servicios o usuarios en texto claro dentro del código fuente de la aplicación.

i) Metodologías ágiles: Utilizar metodologías ágiles durante el proceso de desarrollo permite una mejor gestión de los cambios y actualizaciones que se deban aplicar y usar metodologías como "*DevSecOps",* puede resultar ventajoso al aplicar capas de seguridad durante todo el proceso de desarrollo de una aplicación, adicionalmente otro punto a favor de esta clase de metodologías de desarrollo es que permite la integración con otras, creando variantes como "*Scrum + DevSecOps*" aplicando así procesos de ambas.

j) Endurecimiento del servidor: Por lo general las *aplicaciones web*, están publicadas o cargadas en un servidor remoto público en internet, este servidor hay que mantenerlo siempre configurado de forma segura aplicando los puntos mencionados en "POL – 2. Políticas de Endurecimiento de Equipos".

WEB – 4. Punto de Vista de un Atacante

Objetivo.

a) Proveer a los desarrolladores de *software* la perspectiva de un "*hacker*" real al orquestar un ataque dirigido hacia una página web.
    - Crear parámetros defensivos para que el desarrollador los aplique en el desarrollo seguro de aplicaciones.

Escenario. Para una mejor comprensión se trabajarán los ejemplos de los puntos clave y parámetros verificados por un atacante basado en el siguiente escenario: Existe una aplicación que está presente en la dirección URL "https://www.app1pymes.com/" con la siguiente estructura:

- https://www.app1pymes.com/login
- https://www.app1pymes.com/login/crearcuenta
- https://www.app1pymes.com/login/olvidarcontraseña
    - https://www.app1pymes.com/cuenta?c=1
        - https://www.app1pymes.com/cuenta/admin?c=1
        - https://www.app1pymes.com/cuenta/consulta?c=1&d=2
    - https://www.app1pymes.com/portaladmin

- https://www.app1pymes.com/portaladmin/gestion_usuarios

a) La aplicación esta puesta en producción sin haber sido sometida a pruebas técnicas.
b) Realiza conexiones a bases de datos internas.
c) Permite la carga de archivos.
d) No se revisó la versión del servidor web utilizado (presenta vulnerabilidades)
e) Hay puertos abiertos innecesarios.
f) Uno de los componentes utilizados para la generación de reportes PDF presenta vulnerabilidades.
g) No valida sesiones abiertas.
h) La página de "*portaladmin"* tiene credenciales por defecto, y no hay un vínculo o referencia a él en toda la aplicación.

Narrativa de ataque o puntos claves.

a) Inicialmente un atacante realiza un reconocimiento general sobre la plataforma, analizando su función, público, defensas, controles y todo lo que puede realizar como un usuario sin autenticación, algunos puntos "pasivos" que suelen ser verificados son:
    - Encabezados de seguridad en la aplicación.
    - Atributos de *cookies.*
    - Protocolos *web* utilizados y si estos son cifrados o no.
    - Puntos de inyección de datos (campos de entradas de texto o archivos).
    - Ubicación geográfica del servidor de la aplicación.
    - Registros de DNS o "*Domain Name System*", estos son los nombres asociados a las direcciones IPs, por ejemplo: registro DNS: app1pymes.com y la IP publica vinculada es la: 192.168.1.231.
b) Usando métodos de OSINT (Búsqueda de información en fuentes públicas), identifica documentos, usuarios, correos electrónicos, personal y aspectos o partes del código fuente de la aplicación, esto para encontrar datos que puedan ser de utilidad para acceder a la plataforma, al cargar documentos públicos se debe velar porque no haya datos embebidos en ellos (metadatos).
c) De igual forma, mediante técnicas de OSINT es posible "armar" un navegador con componentes o *plugins* que identifiquen metadatos y las versiones de las tecnologías

y lenguajes utilizados por la aplicación (*WhatWeb y Wappalyzer*, son algunos ejemplos).

d) Un atacante real busca generar la menor cantidad de trafico de red malicioso, por lo que primero realiza esta clase de acciones "pasivas" que no involucran escaneos o pruebas en la aplicación, al concluir esta etapa de pruebas pasivas, un atacante puede haber logrado obtener información para una posterior explotación o incluso, en caso de haber habido información relevante en los puntos mencionados previamente el compromiso y acceso a una cuenta ajena.

e) En las pruebas más activas un atacante realiza más "ruido" en el tráfico a la aplicación, es importante acotar que con la incorporación de un *firewall* se pueden bloquear algunos de estos ataques, aunque la página sea vulnerable.

f) Se realiza una evaluación de vulnerabilidades mediante algunas herramientas como *"Nessus" y "Burp Suite*", estas identifican posibles configuraciones y versiones de componentes utilizados tanto por el servidor como por la aplicación que puedan servir como un vector de ataque.

    - Según el ejemplo, mediante este análisis se identificó el servicio de base de datos utilizado y las vulnerabilidades del *servidor web*.

g) Con el fin de obtener acceso a sitios de la aplicación no referenciados, se pueden realizar ataques de "*fuzzing*", estos buscan acceder a páginas de las aplicaciones ocultas o que no deberían de ser accesibles cambiando o agregando palabras a la URL, planteando un ejemplo basado en el escenario propuesto anteriormente, el atacante accedió a "*portaladmin"* usando una lista de palabras conocidas en la cual esta palabra está presente.

    - La estructura usada fue "https://app1pymes/<palabras_de_la_lista>"
    - Habiendo accedido a este portal, lo seguido es realizar una serie de combinaciones entre usuarios y contraseñas comunes en portales de administración como admin/admin, debido a que no se reajustaron los accesos cuando la aplicación fue puesta en producción el atacante logró acceder a este.

h) Si en la URL hay algún parámetro como "*varible=dato*" se puede intentar alterar este con el fin de acceder a otros datos, siendo este otro tipo de *fuzzing*.

- Según el ejemplo planteado, si la página no tiene un debido control de las sesiones específicamente en esta dirección: “https://www.app1pymes.com/cuenta/admin?c=1” es posible que un atacante cambie el parámetro del “c=1” y logre acceder al portal de administración de otra cuenta (“Dirb” y “Dirbuster” son herramientas comúnmente utilizadas para esto).
- Otro ataque relacionado a este es la inyección SQL, sabiendo que este dato proviene de una base de datos, el atacante puede intentar alterar este parámetro, por una sentencia SQL, para que la aplicación en lugar de verificar un dato lo devuelva, mostrando todos los datos del usuario y la base de datos *(“sqlmap”* es una excelente alternativa para probar de forma sencilla este dato).

i) Las entradas de datos es uno de los puntos que siempre son analizados, ya que una mala validación de los datos puede resultar en múltiples eventos, como:

- Filtrado de información a través de mensajes de error, al no tener una pantalla de error por defecto, la aplicación simplemente cae en un error y muestra el código de este y un fragmento del *backend* donde se originó el error, generar esta clase de eventos puede hacer que la aplicación sufra de una caída a nivel de ejecución y le brinda información adicional al atacante.
- En caso de que ese campo de datos tenga alguna interacción directa con la base de datos, sin una previa validación del “*query*” o consulta, puede que la aplicación sea vulnerable a inyección SQL, esta puede permitirle al atacante extraer datos e incluso omitir controles de acceso, dado el escenario anteriormente planteado, si en la página de “https://www.app1pymes.com/login” no existe una verificación en ambas direcciones (servidor y cliente), un atacante puede intentar crear estas sentencias para obtener acceso.
- Una mala depuración y validación de datos, también puede permitirle al atacante agregar funcionalidades a la aplicación mediante la inyección de código HTML o JavaScript, esto se conoce comúnmente como “*Cross-Site-Scripting*”.

j) Los encabezados de seguridad de una aplicación usualmente son afectados a través de ingeniería social, estos previenen que atacantes puedan cargar la aplicación dentro de otra aplicación controlada por ellos mismos, esta técnica es conocida como "*clickjacking*" y lo que hace principalmente es incitar al usuario a cargar sus datos en un portal aparentemente legítimo, pero controlado completamente por un atacante.
k) El manejo de sesiones debe ser rigurosamente estricto, mediante ataques de "*replay*" un atacante podría llegar a replicar la sesión de un usuario si consigue "robar" su *token* o identificador único, esto mismo puede suceder al utilizar *cookies*, estas pueden ser robadas para intentar obtener la información embebida en estas.

Beneficios. Tener la perspectiva de cuáles serían aquellos puntos que usualmente son verificados por los atacantes reales, puede crear mejores prácticas al aplicar el "desarrollo seguro", pensar de ambas formas, defensiva ("WEB – 3. Buenas Prácticas para el Desarrollo Seguro") y ofensiva (el presente punto) puede evitar que estos comentan errores comunes durante la creación o actualización de una aplicación.

REFERENCIAS

Arimetrics. (s.f.). Obtenido de Arimetrics.com: https://www.arimetrics.com/glosario-digital/campana

Calvo, L. (16 de diciembre de 2022). Obtenido de GoDaddy: https://es.godaddy.com/blog/que-es-una-app-y-para-que-se-utiliza/

Cámara de comercio de Costa Rica. (8 de Julio de 2022). Obtenido de Cámara de comercio de Costa Rica: https://camara-comercio.com/la-importancia-de-las-pymes-en-costa-rica-2/

Caser. (s.f.). Obtenido de https://www.caser.es/glosario-seguros/comercio/ataque-informatico

CCSS. (30 de Julio de 2018). Obtenido de Caja Costarricense del Seguro Social [CCSS]: https://www.ccss.sa.cr/arc/actas/2018/07/8981.pdf

Chavez, J. J. (2 de Junio de 2023). Obtenido de Delta Protect: https://www.deltaprotect.com/blog/vulnerabilidad-informatica

Chen, C. (15 de Octubre de 2020). Obtenido de Significados: https://www.significados.com/marco-de-referencia/

Clavijo, C. A. (Junio de 2006). Obtenido de Redalyc.org: https://www.redalyc.org/pdf/2654/265420388008.pdf

Cloudflare. (s.f.). *Cloudflare.* Obtenido de https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/

Editorial Etecé. (5 de Agosto de 2021). Obtenido de Concepto de: https://concepto.de/organizacion/

estrategiaynegocios.net. (25 de Marzo de 2021). Obtenido de estrategiaynegocios.net: https://www.estrategiaynegocios.net/tecnologia-cultura-digital/vishing-ransomware-y-whaling-los-ciberataques-para-costa-rica-en-2021-LBEN1452393

European Knowledge Center for Information Technology. (5 de Diciembre de 2022). *tic.portal.* Obtenido de https://www.ticportal.es/glosario-tic/servidores

Gonzàlez, L. (15 de Diciembre de 2022). Obtenido de emagister.com: https://www.emagister.com/blog/que-hace-un-ingeniero-de-sistemas/

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la Investigación* (Vol. VI). México: McGrawHill.

IBM. (s.f.). Obtenido de IBM: https://www.ibm.com/es-es/topics/attack-surface

IBM. (s.f.). Obtenido de https://www.ibm.com/mx-es/services/business-continuity/disaster-recovery-plan

IBM. (3 de Febrero de 2023). Obtenido de IBM: https://www.ibm.com/docs/es/qradar-on-cloud?topic=vulnerabilities-common-vulnerability-scoring-system-cvss

IBM Services. (25 de Noviembre de 2020). Obtenido de IBM: https://www.ibm.com/mx-es/services/business-continuity/plan

INA [Instituto Nacional de Aprendizaje]. (s.f.). Obtenido de INA: https://www.ina-pidte.ac.cr/pluginfile.php/15090/mod_resource/content/10/idm-2/pdf/pdf-formulas.pdf

Kaspersky. (s.f.). Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kaspersky. (s.f.). Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Martins, J. (19 de Octubre de 2022). Obtenido de Asana: https://asana.com/es/resources/efficiency-vs-effectiveness-whats-the-difference

Microsoft. (4 de abril de 2023). Obtenido de Microsoft: https://learn.microsoft.com/es-es/dotnet/visual-basic/programming-guide/language-features/procedures/differences-between-parameters-and-arguments

Ministerio de trabajo y seguridad social. (23 de diciembre de 2022). Obtenido de mtss: https://www.mtss.go.cr/temas-laborales/salarios/LISTA%20DE%20SALARIOS%20MINIMOS%20%20ANO%202023.pdf

Ortega, C. (s.f.). Obtenido de Question Pro: https://www.questionpro.com/blog/es/metodos-de-muestreo/

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

OWASP. (s.f.). *OWASP*. Obtenido de https://owasp.org/www-project-top-ten/

Pérez, C. C. (27 de Junio de 2022). Obtenido de El Financiero: https://www.elfinancierocr.com/pymes/gerencia/los-datos-claves-de-las-mipymes-de-costa-rica-en/FWDLWB7GIVHEFCQYQUCHFQKUHE/story/

Pons, L. (15 de Junio de 2015). Obtenido de ICM: https://www.icm.es/2021/06/15/que-son-endpoints/

Ramos, Y., Urrutia, O., Ordoñez, D., & Bravo, A. (25 de Julio de 2017). *Revistas UTP*. Obtenido de Universidad Tecnológica de Panamá: https://revistas.utp.ac.pa/index.php/memoutp/article/view/1475

RockContent. (18 de Julio de 2019). *RockContent*. Obtenido de https://rockcontent.com/es/blog/matriz-raci/

Sampieri, R. H., Fernández Collado, C., & Babtista Lucio, P. (2014). *Metodología de la investigación.* México D.F: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Sampieri, R. H., Valencia, S. M., Torres, C. M., & Romo, A. C. (2017). *Fundamentos de investigación.* Ciudad de México: Estas variables o unidades de medida se utilizan en diversos campos, como la ciencia, la investigación, la estadística, la física, la economía, entre otros.

Siles, A. (23 de enero de 2023). Obtenido de LaRepublica: https://www.larepublica.net/noticia/ciberataques-de-conti-en-costa-rica-figuran-entre-los-seis-mas-agresivos-en-2022

Spitzner, L. (12 de Enero de 2016). Obtenido de SANS: https://www.sans.org/blog/leveraging-the-human-to-break-the-cyber-kill-chain/

Team Asana. (9 de Octubre de 2022). Obtenido de Asana: https://asana.com/es/resources/risk-matrix-template

Weiss, M. M. (2020). *CompTIA Security+ SY0-601* (6 ed.). Hoboken: Pearson IT Certification.

APENDICES

Guía de entrevistas

Para realizar las entrevistas se utilizará principalmente la plataforma de Microsoft Teams, de modo que las reuniones sean completamente virtuales para facilitar este proceso, adicionalmente los profesionales deben de ser profesionales de seguridad, y lo que se busca con este proceso es indagar y obtener opiniones sobre la ciberseguridad, Pymes y que aspectos consideran importantes que puedan ser agregados a la guía, a continuación, se detallan las preguntas planteadas.

1. ¿Cuál es su nombre?
2. ¿A qué se dedica en su trabajo actual?
3. ¿Con qué clase de situaciones o actividades se ve involucrado diariamente?
4. ¿Está familiarizado usted con el concepto de Pymes? ¿Cómo lo definiría?
5. ¿Labora usted o está involucrado en actividades relacionadas con Pymes?
    a. ¿Qué tipo de actividades?
6. ¿Cada cuanto acude usted a emprendimientos o Pymes?
7. A partir de su conocimiento con las Pymes, ¿cree que estas aplican ciberseguridad en su día a día?
    a. ¿Por qué?
8. ¿Cuáles cree usted que serían las principales recomendaciones para tomar en cuenta para las empresas Pymes de Costa Rica?
9. ¿Considera usted las políticas y los procedimientos como un punto de mejora para las Pymes?
10. A partir de su conocimiento de las Pymes, ¿cuáles considera usted que son las principales debilidades presentes en ellas?
    a. Y cuáles son los principales vectores de ataque
11. ¿Considera usted que son un “Blanco fácil” para los ciber atacantes? ¿Por qué?
12. ¿Qué sugerencias tiene usted para que una Pyme realice un proceso de recuperación de desastres?
13. ¿Ve usted de valor el desarrollo de una guía de ciberseguridad para las Pymes?

14. ¿Qué consideraciones o puntos clave cree que deberían de tomarse para realizar dicha guía?

Al ser una entrevista semi estructurada dependiendo de las respuestas del entrevistado pueden realizarse preguntas adicionales, con el fin de obtener información más a profundidad, dependiendo de la disposición de la persona, se le mencionaran los puntos a tratar dentro de la guía para que los pueda categorizar de mayor a menor según su importancia.

Guía de observación

Durante el desarrollo de las encuestas a las Pymes, se buscará contactar con las más grandes de forma presencial, con el fin de realizar un recorrido por las instalaciones evaluando controles físicos, estado de los equipos y políticas de escritorio limpio.

- Visibilidad y accesibilidad a un punto de acceso de red.
- Visibilidad y accesibilidad a los equipos utilizados
- Comportamientos y lenguaje corporal de los encuestados durante el proceso, así como la coherencia de las respuestas.
- Escritorio limpio (Sin contraseñas o datos importantes alrededor)
- Cámaras u otros de controles de seguridad física

Guía de encuestas

Las encuestas serán realizadas mediante un enlace que dirigirá hacia la plataforma de Microsoft Forms, esta tendrá dos modalidades, una de ellas será virtual, el enlace se les hará llegar mediante una plataforma electrónica y la segunda será presencial, lo que también servirá para realizar las observaciones pertinentes, se busca principalmente medir un nivel de conocimiento de ciberseguridad en Pymes y que tanta disposición existe para acatar o seguir a modo de referencia la guía, las preguntas serían las siguientes:

1. ¿Cuánto tiempo lleva el negocio activo?
    a. Menos de 1 año
    b. Entre 1 año y 3 años
    c. Entre 3 y 5 años
    d. Más de 5 años
2. ¿En su lugar de trabajo actual existe un correo electrónico dedicado exclusivamente a asuntos laborales?
    a. Sí

   b. No
3. ¿En su lugar de trabajo actual se utilizan dispositivos (computadoras, tablets, teléfonos, etc) estrictamente para su uso laboral?
   a. Sí
   b. No
4. ¿En su lugar de trabajo actual utilizan redes sociales para promocionar sus artículos?
   a. Sí
   b. No
5. ¿En su lugar de trabajo actual se acepta el SINPE móvil o transferencia bancaria como un método de pago?
   a. Sí
   b. No
6. ¿Valida usted o su empresa que los pagos hayan sido debidamente acreditados?
   a. Siempre
   b. Regularmente
   c. Casi nunca
   d. Nunca
7. ¿Qué nivel de conocimiento tiene usted de los conceptos de seguridad informática?
   a. Avanzado
   b. Intermedio
   c. Básico
   d. Ninguno
8. ¿Ha tomado usted o sus compañeros de trabajo alguna capacitación o curso sobre la ciberseguridad?
   a. Sí (Diríjase a la pregunta 8)
   b. No (Diríjase a la pregunta 9)
9. ¿De qué tipo de empresa recibió la capacitación o curso?
   a. Finanzas (Bancos, Cooperativas)
   b. Empresas de seguridad

c. Gobierno
d. Autoestudio

10. ¿Ha sido usted o su empresa víctima de estafas telefónicas, correos de phishing, suplantación de identidad o alguna perdida de información?
    a. Sí
    b. No
    c. No lo se
11. ¿Está familiarizado con alguno de los siguientes conceptos?
    a. Phishing (Correos maliciosos).
    b. Virus.
    c. Troyanos.
    d. Ransomware (Secuestro de información).
    e. Ingeniería social.
    f. Ataques informáticos.
12. ¿Qué clase controles de seguridad física tienen implementados en su empresa?
    a. Cámaras o sistemas de seguridad.
    b. Guardias de seguridad.
    c. Bitácora de ingreso para colaboradores y visitantes.
    d. Asistente de recepción.
    e. Ninguna
13. ¿Cuenta su empresa con algún tipo de software de seguridad como Antivirus o Cortafuegos?
    a. Sí
    b. No
    c. No lo sé
14. ¿Cuál es el estado en general de los equipos tecnológicos utilizados en su empresa?
    a. Excelente
    b. Regular
    c. Malo
15. ¿Cada cuanto se realizan respaldos de la información en su empresa?

a. Siempre
b. Regularmente
c. Casi nunca
d. Nunca
e. No lo sé

16. ¿Conoce usted, sobre algún marco de referencia que sirva de apoyo para establecer procesos y políticas en las Pymes?
    a. Sí
    b. No
17. ¿En su empresa se aplican políticas de uso aceptable de las cuentas laborales, escritorio limpio (Tener el escritorio únicamente con lo necesario para trabajar y restringir el acceso a documentos confidenciales) y políticas sobre la complejidad y cambio de contraseñas?
    a. Sí
    b. No
    c. No lo sé
18. ¿En su empresa utilizan un gestor de contraseñas?
    a. Sí
    b. No
    c. No lo sé
19. ¿En su lugar de trabajo actual, existe una página web o aplicación móvil?
    a. Sí (Diríjase a la pregunta 20)
    b. No (Diríjase a la pregunta 23)
20. ¿Recibe usted soporte del fabricante de la aplicación?
    a. Sí
    b. No
21. ¿La aplicación es transaccional o informativa?
    a. Sí
    b. No
22. ¿Conoce usted si alguna vez dicha aplicación/es fue sometida a pruebas de seguridad (Pruebas de penetración)?

a. Sí, si lo fue
b. No, no lo fue
c. No lo se

23. ¿Cuenta su empresa con un equipo o personal de soporte técnico (áreas de TI) para sus equipos y activos informáticos?
    a. Sí
    b. No
24. ¿Los equipos y aplicaciones tecnológicos utilizados y adquiridos por la empresa (computadoras, antivirus, aplicaciones) cuentan con un licenciamiento valido del proveedor?
    a. Sí
    b. No
    c. No lo se
25. ¿Tiene usted o su empresa una infraestructura de redes interna?
    a. Sí
    b. No
    c. Desconozco
26. ¿Podría indicar mediante cuales formas accede a esta red?
    a. VPN
    b. Ethernet (Cableado)
    c. WiFi (Inalámbrico)
27. ¿Tiene aplicada alguna política de endurecimiento de configuraciones (Hardening) en servidores y equipos de red?
    a. Sí
    b. No
    c. No lo sé
28. ¿Cada cuanto revisa y aplica su empresa las actualizaciones de sus equipos?
    a. Siempre
    b. Regularmente
    c. Casi nunca
    d. Nunca

29. ¿Sabe si su empresa lleva un inventario de los activos (Datos, equipos, etc)?
    a. Sí
    b. No
    c. Desconozco
30. ¿Considera usted de valor una guía que le indique que medidas puede seguir para mejorar la postura de seguridad informática de su empresa?
    a. Sí (Diríjase a la pregunta 30)
    b. No (Concluye la encuesta)
31. ¿Qué detalles o puntos específicos quisiera que se profundicen en la guía?
    Pregunta abierta _____