Establecer un manual de seguridad informática para la empresa Recartuchos ubicada en la ciudad de Santiago de Cali

Set computer security manual in a printing support office

Andres Felipe Villa Loaiza[1]
Andres.villa01@usc.edu.co

Lorena Cerón[2]
Dir.sistemasvirtual@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de [Tecnología en sistemas de información] (1)

Resumen

En la actualidad salvaguardar la información de una empresa es una de las tareas que cobran más importancia, con ella se asegura un correcto funcionamiento administrativo y operativo. En esta monografía, se abarca la situación de una compañía caleña llamada RECARTUCHOS, la cual desde el año 2018 viene presentando ataques cibernéticos, siendo el phishing la amenaza común. El phishing es una técnica de ingeniería social, la cual consiste en el envío de correos electrónicos que suplantan la identidad de compañías y solicitan información personal al usuario. Se analizó la problemática, buscando implantar como solución, el establecimiento de un manual de usuario en seguridad informática; el cual consta de dos partes: manual de usuario para administrador de sistemas y manual para usuario final de los equipos de cómputo. Estos documentos buscan guiar a los funcionarios en las acciones encaminadas a proteger la privacidad e integridad de los datos almacenados en las estaciones de trabajo, para garantizar el correcto uso y apropiación de la información.

Palabras clave: Seguridad de la información, riesgos de la información, incidentes de seguridad, herramientas y prácticas de seguridad, phishing, malware, ley 1273 2009, ingeniería social, Norma ISO 27000

Abstract

Nowadays, safeguarding a company's information is one of the most important tasks, as it ensures a correct administrative and operational functioning. In this monograph, the situation of a Cali company called Recartuchos is covered, which since 2018 has been presenting cyber-attacks, being phishing the most common threat. Phishing is a social engineering technique, which consists of sending emails that impersonate the identity of companies and request personal information from the user. The problem was analyzed, seeking to implement as a solution, the establishment of a user manual on computer security, which consists of two parts: user manual for system administrators and manual for end users of computer equipment, these documents seek to guide officials in actions to protect the privacy and integrity of data stored on workstations, to ensure the correct use and appropriation of information.

Keywords: Information security, information risks, security incidents, security tools and practices, phishing, malware, law 1273 2009, social engineering, ISO 27000 Standard

1. INTRODUCCIÓN

A través de los años, las empresas se han convertido en objetivos de ataques cibernéticos y cada vez son más vulnerables, debido al desarrollo de nuevas tecnologías que dejan en exposición sus datos. La ciberseguridad se ha esforzado por proteger los datos que se almacenan en los sistemas informáticos y evitar de cualquier manera su uso no autorizado.

Uno de los objetivos de la ciberseguridad es generar confianza entre clientes, proveedores y el mercado en general. En un mundo hiperconectado, donde la mayoría de nuestras actividades las hacemos a través de la red y dispositivos electrónicos, garantizar la seguridad de las operaciones es una necesidad imperante. Ciberseguridad. (s.f). Sitio web: https://www.infosecuritymexico.com/es/ciberseguridad.html

En el año 2009, el congreso de la república de Colombia modifica el código penal y crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. La ley 1273 de 2009 de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, castiga de forma estricta conductas como: Acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, hurto por medios informáticos y semejantes, transferencia no consentida de activos entre otros, con penas desde 48 a 96 meses de prisión y multas desde 100 a 1.000 salarios mínimos legales mensuales vigentes. Ley 1273 de 2009. De la Protección de la información y de los datos. 5 de enero 2009. D.O. No. 47223

En lo que va del año 2022, el sector público colombiano ha venido implementando diferentes normativas enfocadas al cumplimiento de buenas prácticas para el aseguramiento de la información, la protección de los datos y la gestión de riesgos en el entorno digital. Así lo asegura el Estudio trimestral de ciberseguridad de ataques a entidades del gobierno elaborado por Fortinet y Crowdstrike. El documento revela que en 2021 se presentaron 41 billones de intentos de ataques cibernéticos en el mundo y siete billones en Colombia. Los autores del estudio señalan que los cibercrímenes generan cada vez más rentabilidad para los atacantes y, en este sentido, se necesitan herramientas para contrarrestarlos y estar protegidos. De lo contrario, los ataques seguirán creciendo. Duran, S. (15 abril 2022). 7 billones de ciberataques se registraron en Colombia durante 2021. Sitio web: https://dplnews.com/7-billones-de-ciberataques-se-registraron-en-colombia-durante-2021/

Sumado a esto, se debe reconocer que también existe en todas las empresas del mundo, un recurso inseguro que guarda información confidencial: la mente humana, además, hoy en día, todavía no se destinan recursos adecuados para capacitarse sobre el tema.

Al realizar esta monografía, se tiene como objetivo general, establecer un manual de usuario de seguridad informática, el cual consta de dos partes, la primera para el administrador de sistemas cuyas responsabilidades que se han establecido es de otorgar claves, crear, modificar, eliminar perfiles y el segundo para el usuario que está a cargo de un equipo de cómputo en la oficina administrativa.

El manual de seguridad informática se debe establecer porque la empresa Recartuchos tiene trabajadores que en este momento no poseen conocimientos básicos en el área de tecnología y se deben concientizar que desde una llamada telefónica hasta el abrir un correo con remitente sospechoso se corre un alto porcentaje de riesgo. La función de este documento es alfabetizar tanto al personal que está en la empresa como al que ingresa nuevo a ella, deben de leerlo y tener en cuenta todas las recomendaciones para no sufrir un incidente de seguridad informática el cual lleve a la perdida de la información y de dinero como es el caso presentado en una oportunidad por valor de $50.000.000

De acuerdo con la investigación, otras compañías caleñas, como es el caso de SuperGiros, contratan proveedores de servicios tecnológicos, estos proveen y realizan capacitaciones, la empresa paga una mensualidad acordada.

Todas estas empresas abarcan este tema desde el contrato de trabajo, en este orden de ideas, al momento del trabajador firmar el documento, se debe comprometer a realizar la capacitación y evaluación final que este proceda. La alfabetización

presencial o virtual se debe realizar con el desarrollo de talleres enfocados al tema de seguridad informática, donde se permite evaluar la lógica de la persona desde lo más sencillo hasta los riesgos más complejos.

A la empresa Recartuchos, ubicada en Santiago de Cali, quién presentó ataque de tipo: Phishing, se le da a conocer la opción de uso gratuito con uno de los proveedores con mayor conocimiento en el tema de Ciberseguridad a nivel mundial, hablamos de Fortinet, el cual desde el año 2022, lanzó para toda Latinoamérica un servicio gratuito que permite evaluar el nivel de madurez de Ciberseguridad en los ambientes de tecnología. A partir de esta evaluación, Fortinet provee una consultoría individual para identificar los riesgos y mejoras prácticas para elevar el nivel de protección de todo lo que abarca la tecnología. En el siguiente enlace se realiza la evaluación: https://www.fortinetcybersecuritylevel.com/es/home

Para entender la intencionalidad del establecimiento de este manual, se debe tener claro 3 conceptos muy conocidos al momento de percibir un ataque cibernético, los cuales describo a continuación:

1.1.1 Phishing

El phishing es un método de ingeniería social que se fundamenta en engañar a una persona haciéndole creer que está ingresando a un sitio seguro.

Los ataques cibernéticos como el phishing, el ransomware y los ataques de denegación de servicio distribuido están en aumento. Cloudflare, empresa de ciberseguridad de EE. UU. que brinda servicios de protección a más de 30% de las empresas de Fortune 500, descubrió que los ataques de este tipo implican abrumar un servidor con una avalancha de tráfico para interrumpir una red o una página web. Aumentaron el año pasado en 79% interanual en el último año. Cajamarca, I. (2023, 19 enero). Los expertos piden una respuesta global ante la tormenta cibernética de seguridad. Diario La República. https://www.larepublica.co/especiales/davos-2023/los-expertos-piden-una-respuesta-global-ante-la-tormenta-cibernetica-de-seguridad-3526375

1.1.2 Ingeniería social

La ingeniería social funciona aprovechando los prejuicios cognitivos de las personas. Un atacante de ingeniería social se hace pasar por alguien simpático, digno de confianza o con autoridad y engaña a la víctima para que confíe en él. Una vez que la víctima confía en el atacante, es manipulada para que revele información privada. Hoy en día, la ingeniería social se produce con frecuencia en línea, incluso a través de estafas en las redes sociales, donde los atacantes se hacen pasar por un contacto de confianza o una figura de autoridad para manipular a las personas para que expongan información confidencial. Bodnar, D. (29 octubre 2020). Ingeniería social y como protegerse. Sitio web: https://www.avast.com/es-es/c-social-engineering

1.1.3 Malware

Es un programa malicioso, realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

En Colombia los tres malware más peligrosos a principio del año 2023 fueron XMRig, que es un software de minería de CPU de código abierto, utilizado para minar la criptomoneda Monero; le sigue Qbot, un troyano bancario y el tercero es una botnet llamada Glupteba, conocida desde 2011. Semana. (2023, 19 febrero). Cuidado: en Colombia, estos son los malware que más atacaron a las empresas. Semana.com Últimas Noticias de Colombia y el Mundo. https://www.semana.com/economia/empresas/articulo/cuidado-en-colombia-estos-son-los-malware-que-mas-atacaron-a-las-empresas/202342/

Esta monografía tiene perspectiva descriptiva, ya que se involucra la encuesta como método de estudio de caso, se realiza sondeo a los usuarios cuyas experiencias especificas en los puestos de trabajo arrojaron datos importantes para la investigación.

El estudio realizado en la oficina administrativa se trabajó bajo la siguiente infraestructura tecnológica

Tabla 1. Infraestructura analizada

Cantidad	Objeto estudiado	Área
1	Equipo de cómputo	Servidor central de información digital
1	Equipo de cómputo	Contabilidad
2	Equipo de cómputo	Facturación

Tabla 2. Tipos de ataques detectados a la infraestructura analizada

Área	Tipo de ataque
Servidor central	Phishing – Rasonware - Malware
Contabilidad	Phishing - Malware
Facturación	Phishing - Rasonware

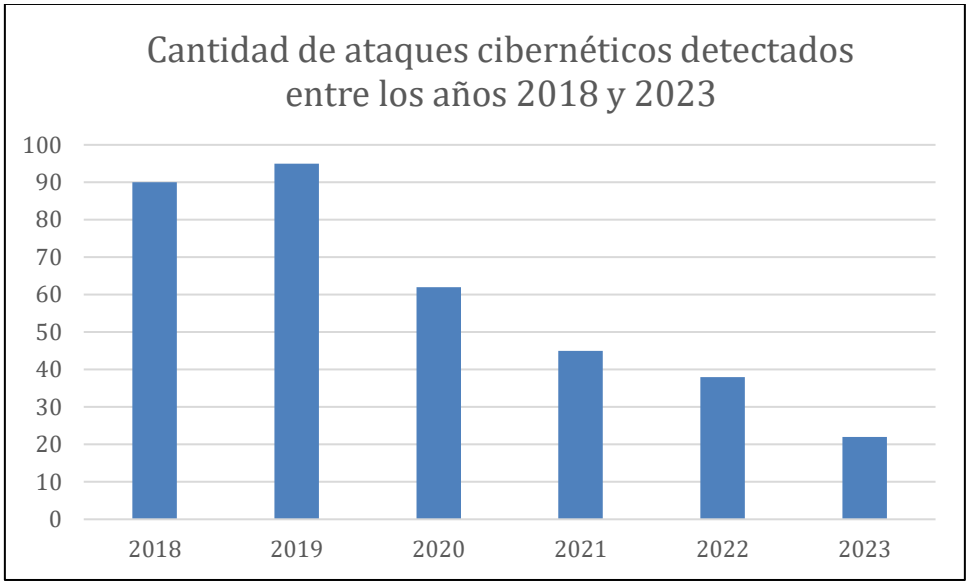
Este estudio, se realiza teniendo en cuenta que se encuestaron 4 personas del área administrativa, las cuales tienen acceso a internet y con permisos restringidos.

En el año 2018, se registró el caso más grave de phishing en el área de contabilidad, esto sucedió al ingresar a una página web maligna, se registraron los datos bancarios de la compañía, dejando como saldo una pérdida de más de $50.000.00 COP

El estudio también arrojó, que en el transcurso de cinco años del 2018 al 2023 han disminuido los ataques, esto se debe a que la empresa ha destinado recursos financieros por valor de $10.000.000 COP para adquirir software y hardware como Router, para administrar la red privada de la empresa y tener estricto control de las conexiones, software licenciado como Microsoft Office y sistema operativo Microsoft Windows 10, esto para evitar la instalación de software pirata y así prevenir la propagación de malware, antivirus de pago Avira, para así mantener los equipos de cómputo protegidos. Por recomendación del personal experto se realizó el cambio de administrador de hosting a CloudTech en el año 2021, el cual garantiza filtros antispam en correos corporativos, dejando así de utilizar cuentas Hotmail y Gmail.

Figura 1.

Cantidad de ataques cibernéticos detectados a la compañía Recartuchos entre el 2018 y 2023

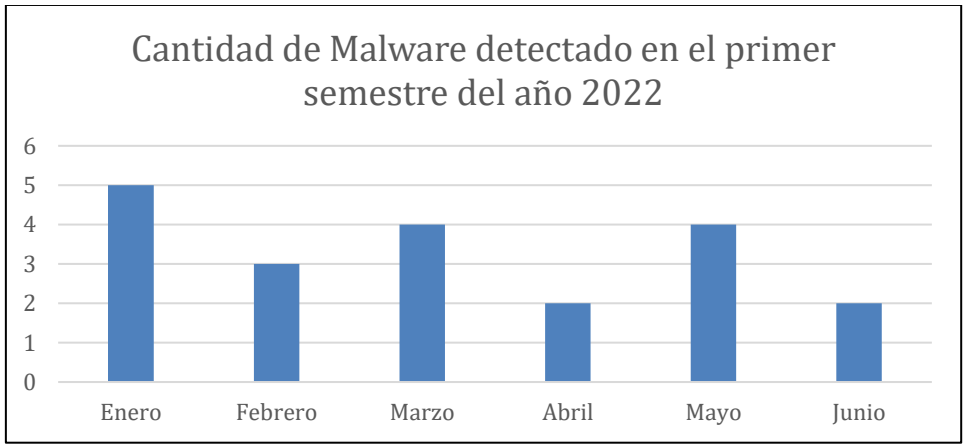


Sin embargo, adquirir infraestructura tecnológica no es lo único que se necesita para disminuir los ataques cibernéticos o tener seguridad en la red interna de la empresa. Por lo tanto, se debe concientizar al personal, de los peligros que implican abrir correos de dudosa procedencia, descargar archivos maliciosos, entregar información sensible vía telefónica, entre otras prácticas.

En esta monografía, se analizó el primer semestre del año 2022 sobre el malware encontrado en el equipo de cómputo servidor, fueron 20 las alarmas detectadas en este intervalo de tiempo, la causa se genera, porque se comparten una serie de programas que son utilizados para desbloquear equipos de impresión y que el sistema detecta como posible virus: troyanos, a esto se le da solución incluyendo los programas en una serie de excepciones. Es un porcentaje que no sobrepasa el 5%, esto debido al control que se ejerce con el antivirus y la seguridad tanto lógica como física, debido a que el equipo se encuentra vigilado con cámara de seguridad y protegido con dos contraseñas de administrador.

Figura 2.

Cantidad de Malware detectado en equipo de cómputo servidor en el primer semestre del año 2022



El lunes 28 de abril del 2022, el equipo de cómputo de facturación, recibió un mensaje en la cuenta de correo corporativo, el enlace fue abierto por la asistente administrativa a las 10:45 a.m. Luego de analizar el sitio web con personal experto, se concluyó que el ataque fue de tipo Phishing, al solicitar contraseña de correo electrónico y de las cuentas bancarias de la empresa.

Figura 3.

Captura de pantalla de mensaje enviado a correo corporativo.

1.3.4 NORMA ISO IEC 27001:2013

La familia de NORMAS ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora del sistema de gestión de la seguridad de la información.

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo. Organización Internacional de Normalización (ISO, 2013)

Como medio de apoyo a esta monografía, se cita la NORMA ISO 27001, en ella se especifican los requisitos que se necesitan cumplir para abordar el Sistema de Gestión de Seguridad Informática SGSI, esta norma es la más importante de la familia ISO 27000 y con base a ella, se busca establecer el manual de usuario administrador TI y para usuarios finales de los equipos de cómputo de la empresa RECARTUCHOS, teniendo en cuenta la lista de controles y objetivos, por mencionar algunos:

Roles y responsabilidades de los usuarios

Separación de deberes

Terminación o cambio de responsabilidades del empleo

Toma de conciencia, educación y formación en la seguridad de la información

Inventario de activos

Uso aceptable de los activos

Clasificación de la información

Transferencia de medios físicos

Política de control de acceso

Acceso a redes y a servicios en red

Gestión de derechos de acceso privilegiado

Retiro de los derechos de acceso de usuarios

Restricción de acceso a la información

Perímetro de seguridad física

Mantenimiento de equipos

Política de escritorio y pantalla limpios

Registro de eventos

Restricción sobre la instalación de software

Separación en las redes

Control de mensajería electrónica

Esta monografía, se basó en el establecimiento de un manual de usuario, el cual recopiló aspectos básicos y esenciales de la ciberseguridad de la empresa y de la ingeniería social.

Consta de dos partes, manual de usuario para Administrador TI de la oficina, en él, se explica desde la configuración correcta del Router para evitar intrusos en la red interna de la compañía, hasta estructurar el proceso de instalación de software licenciado como antivirus y sistema operativo. La otra parte, es el manual para usuario final del equipo de cómputo, aquí se incluyen las medidas preventivas que se deben tener al momento de navegar en internet, desde el navegador que se debe utilizar, hasta tener la máxima sospecha en correos no deseados. Es orden de gerencia de la empresa Recartuchos, aplicar los métodos aquí explicados, de lo contrario se incurrirá en anotaciones a la hoja de vida del personal que no cumpla con las normas establecidas en el manual.

Teniendo en cuenta estos datos, se debe establecer el manual de usuario el cual busca proteger los activos más importantes de la empresa tales como: base de datos de clientes, cuentas bancarias de la empresa, documentos personales de los trabajadores, entre otros. También se busca analizar el desempeño de los empleados del área administrativa en temas de seguridad de la información, organizando un calendario de planeación y actualización del manual mensualmente con nuevas amenazas y métodos de protección.

Entregar el manual va a permitir que la persona se apropie de la compañía y se comprometa a seguir las sugerencias para salvaguardar el activo más importante de la empresa que es la información.

2. ROLES Y RESPONSABILIDADES

2.1 Objetivo

Realizar una descripción detallada acerca de las responsabilidades de los usuarios actores de la información, buscando mantener y controlar el proceso de seguridad de la información y ciberseguridad en RECARTUCHOS.

2.2 Alcance

Este documento contiene los roles y responsabilidades de seguridad de la información y ciberseguridad definidos para RECARTUCHOS y aplica para todos sus colaboradores, clientes, proveedores y usuarios que tengan acceso a los activos de información de RECARTUCHOS.

2.3 Funciones

Según los roles y responsabilidades definidos en la estructura organizacional de RECARTUCHOS y en las responsabilidades descritas en este documento perteneciente a la gestión de tecnologías de información y comunicaciones de RECARTUCHOS, este documento busca:

- La asignación de las responsabilidades de seguridad de la información, la cual se debería articular de acuerdo con las políticas de la seguridad de la información y ciberseguridad aprobadas.
- Que ninguna persona pueda acceder, modificar o usar activos sin autorización ni detección.
- Al diseñar los controles, se debería considerar la posibilidad de afectar los conflictos de interés, para este caso se deberían considerar otros controles, tales como el seguimiento de actividades, los rastros de auditoría y la supervisión de la dirección.

2.4 Definición de rol

Un rol es un conjunto de permisos. Normalmente, los permisos de un rol definen una actividad concreta que puede realizar un usuario. Un usuario puede tener asignado más de un rol. El número de roles y permisos depende del usuario.

2.5 Responsabilidades

- Revisión de la actualización y aprobación de la política de seguridad de la información y ciberseguridad definida.
- Establecer estrategias corporativas para la gestión de los riesgos de la Seguridad de la Información y ciberseguridad.
- Evaluar la efectividad de las medidas y controles a los riesgos y tomar decisiones al respecto.
- Definir el presupuesto necesario para la ejecución de planes y/o proyectos de Seguridad de la Información.
- Fomentar la comunicación entre los procesos corporativos de RECARTUCHOS a cerca de las medidas, roles y responsabilidades con los activos de información.

2.6 Líder de Ciberseguridad

2.6.1 Rol

Empleado que reporta a la gestión directiva de RECARTUCHOS, quien es responsable de planificar, diseñar, implementar, colocar al servicio, proponer y evaluar las herramientas de seguridad requeridas para la aplicación y medición de la eficiencia de los controles y/o salvaguardas implementadas en seguridad de la información y ciberseguridad, lo mismo de reportar el

resultado de los análisis realizados.

El líder de seguridad de la información es responsable de la implementación y del correcto funcionamiento del sistema de gestión de seguridad de la información y ciberseguridad alineados con los requerimientos del negocio y bajo las directrices del comité de seguridad de la información de la organización.

2.6.2 Nivel de autoridad

- Aprobar o denegar solicitudes y/o requerimientos en relación con la seguridad de la información y ciberseguridad.
- Enviar a descargos y/o procesos disciplinarios a funcionarios que incumplan políticas o que generen incidentes o eventos de seguridad.

2.6.3 Responsabilidades

- Monitorear del cumplimiento de las normas, políticas y procedimientos de seguridad de la información y ciberseguridad.
- Desarrollar las revisiones de efectividad de los controles de seguridad de la información y ciberseguridad, con el fin de establecer acciones correctivas, preventivas y/o de mejoramiento de dichos controles.
- Participar en la definición y actualización de la estrategia y la planeación de la gestión de seguridad de la información y ciberseguridad, con el fin de asegurar la definición y programación de proyectos, actividades y recursos para la solución de los requerimientos y expectativas de la organización.
- Apoyar al Comité de Seguridad en el establecimiento y desarrollar programas de formación, sensibilización, marco de gobierno y comunicación para la gestión corporativa de la seguridad de la información y ciberseguridad.

2.7 Auxiliar administrativo

2.7.1 Rol

Persona que reporta a la alta dirección y encargada de toda la protección física y del entorno de la organización donde exista procesamiento de información.

2.7.2 Nivel de autoridad

- Asignar, denegar y/o revocar controles referentes a la seguridad física

2.7.3 Responsabilidades

- Gestionar las actividades de protección de las CUSTODIAS DE LA INFORMACIÓN y áreas de resguardo de información.

- Llevar un control e identificación de los Empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio.
- Apoyo en la gestión de identificación, clasificación y valoración de activos que referencien riesgos potenciales de continuidad y afecten los procesos de RECARTUCHOS
- Determinar las acciones de respuesta para contener el impacto a los riesgos materializados o escenarios de riesgos desarrollados antes de que sucedan estos.
- Apoyar en la identificación de evidencias que determine acciones legales y/o disciplinarias sobre los involucrados en incidentes de seguridad de la información y ciberseguridad.

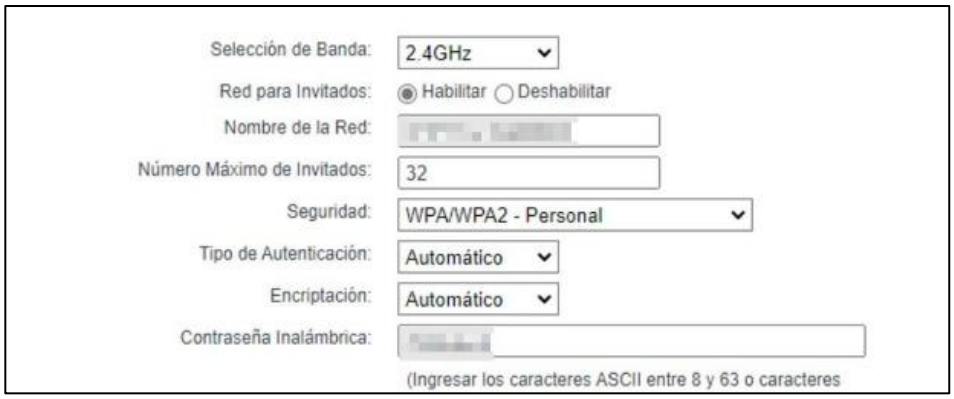
3. MANUAL

3.1 Manual administrador TI

3.1.1 Configuración de la red local y wifi

- Como primera medida de seguridad para la oficina, se debe configurar el Router que otorga acceso a internet y a la red local. Es necesario tener activo el cifrado WPA2 para otorgar complejidad a la contraseña para generar conexión a internet.

Figura 4.
Cifrado WPA2 activo



- Aislar la red para invitados, es prioridad en toda la oficina, puesto que en algún momento se recibirán visitas de clientes, proveedores entre otros y requieren conexión a internet, separar esta red es una forma de protección, porque no tendrán acceso a la red interna. Se observa en la figura 5 como es la correcta parametrización del Router, para garantizar el aislamiento de la red wifi para clientes y/o proveedores.

- El administrador TI debe tener total control de los equipos que se encuentran conectados a la red, por tal motivo es necesario filtrar las conexiones Wifi mediante la MAC de cada equipo, al activar esta opción, así el usuario tenga la contraseña no lo dejará navegar al no estar registrada su MAC en el Router.

3.1.2 Configuración de equipos de cómputo

- Como primera medida de seguridad, se debe garantizar que el equipo cuente con software antivirus, este se encargará de proteger el equipo mientras se navega por internet, el programa tiene como misión, bloquear cualquier conexión no autorizada al equipo, en este caso se recomienda el antivirus AVIRA, de origen alemán, el cual en los últimos años ha sido calificado con altas puntuaciones debido a su elevado porcentaje de detección de malware, además en la versión free se adicionan plugin para hacer más seguro el navegador web.

- Una de las funciones del administrador TI es crear dos perfiles en cada computador, un usuario administrador con todos los privilegios y un usuario estándar con privilegios delimitados, con esto se garantiza que, el usuario estándar no instalará, modificará o eliminará programas o carpetas.

- Configurar y aprovechar todas las opciones de seguridad que brinda Microsoft Windows, es necesario para cerrar la brecha ante una posible fuga de información o infección del equipo de cómputo, se deberá tener activo el cortafuegos o firewall, este software supervisa todo el tráfico de red y tiene permisos para identificar y bloquear el tráfico no deseado.

Figura 5.
Seguridad de Windows

- Se toma la decisión de utilizar el navegador Tor, puesto que el método de direccionamiento que este utiliza no revela la dirección IP a los sitios web que se visitan, bloqueo de rastreadores, bloqueo de anuncios y asegura anonimato en la red.

3.2 Manual de usuario para personal administrativo

- Como primera medida se debe garantizar que el puesto de trabajo se encuentre limpio y libre de cualquier documento que contenga información sensible como contraseñas, también cada que se retire del puesto se debe cerrar sesión en el equipo cómputo o en su defecto bloquearlo.

- La configuración del equipo de cómputo no se debe modificar por ningún motivo, no instalar aplicaciones no autorizadas, no conectar dispositivos como USB o memorias portables no confiables.

- No se debe divulgar información sensible de la empresa si no se conoce quien es el receptor de esta, destruir información confidencial que se encuentre en papel, no mantener conversaciones con información privada en lugares públicos o donde puedan ser oídas por terceros.

- No se compartirá credenciales de acceso al equipo de cómputo como: contraseñas y usuarios, no se debe utilizar las credenciales corporativas para equipos personales.

- No abrir correos electrónicos de origen desconocido, se debe bloquear el remitente y eliminar inmediatamente.

- No se debe contestar mensajes por correo electrónico que se crea sospechoso.

- Se debe evitar acceder a páginas web no confiables.

- En los siguientes puntos se da a conocer una serie de recomendaciones que se deben tener en cuenta al momento de navegar en la red de internet:

- Comprueba el nombre exacto de la página web, de ser necesario se debe escribir letra por letra, el cambio de una de estas o un digito de un sitio web te puede dirigir a un sitio malicioso. Se debe tener en cuenta, visualizar el icono del candado seguido del certificado SSL en la barra de navegación superior izquierda, si no se observan estas dos condiciones es probable que el sitio en el que se está navegando no sea seguro.

- La policía nacional de Colombia, en su portal web https://cc-csirt.policia.gov.co/Sandbox
  brinda una serie de servicios gratuitos que permiten analizar archivos y direcciones url sospechosas.

4. CONCLUSIONES

Desde el panorama de los hallazgos, se logra determinar que, al establecer el manual de seguridad informática en la empresa RECARTUCHOS, la ventaja que se obtendrá es la disminución de los ataques informáticos a las áreas aplicadas.

La seguridad siempre será un objetivo en movimiento, ya que los ciberdelincuentes todos los días avanzan más, los empleados deben hacer de la seguridad informática algo primordial en su día a día. El administrador TI debe estar actualizado de las últimas tendencias en ataques, así como también de la manera en cómo prevenirlos para replicarlo en las áreas críticas como: administrativa y facturación.

Este trabajo es el inicio para la continuidad de mi carrera como profesional, en este intervalo de tiempo se realizará la implementación, evaluaciones constantes y auditorias para así generar un reporte del impacto obtenido.

5. REFERENCIAS

Bodnar, D. (29 octubre 2020). Ingeniería social y como protegerse.
https://www.avast.com/es-es/c-social-engineering

Duran, S. (15 abril 2022). 7 billones de ciberataques se registraron en Colombia durante 2021.
https://dplnews.com/7-billones-de-ciberataques-se-registraron-en-colombia-durante-2021/

Ley 1273 de 2009. De la Protección de la información y de los datos. 5 de enero 2009. D.O. No. 47223
https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Ciberseguridad. (s.f).
https://www.infosecuritymexico.com/es/ciberseguridad.html

Organización Internacional de Normalización. (2013). Tecnología de información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos (ISO 27001)

Cajamarca, I. (2023, 19 enero). Los expertos piden una respuesta global ante la tormenta cibernética de seguridad. Diario La República.
https://www.larepublica.co/especiales/davos-2023/los-expertos-piden-una-respuesta-global-ante-la-tormenta-cibernetica-de-seguridad-3526375

Semana. (2023, 19 febrero). Cuidado: en Colombia, estos son los malware que más atacaron a las empresas. Semana.com Últimas Noticias de Colombia y el Mundo. https://www.semana.com/economia/empresas/articulo/cuidado-en-colombia-estos-son-los-malware-que-mas-atacaron-a-las-empresas/202342/