Facultad de Ingeniería

Ingeniería de Seguridad y Auditoría Informática

Programa Especial de Titulación:

“MEJORAMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN PARA REDUCIR LOS CIBERATAQUES DEL TIPO PHISHING EN UNA ENTIDAD FINANCIERA”

Alumno: Jou William Jancachagua Vera

Para optar el Título Profesional de

Ingeniero de Seguridad y Auditoría Informática

Asesor: Carlos Daniel Rodriguez Vilcaromero

Lima – Perú

2021

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

La ciberseguridad es un tema relevante en la actualidad, ya que se han incrementado los ciberataques a nivel mundial hacia las organizaciones, sin embargo resulta curioso que en tiempos de pandemia por COVID-19 los ciberdelincuentes también afecten a las personas, que normalmente no es su objetivo. De modo que, dentro del abanico de estrategias con las que cuenta el ciberdelincuente, se ubica el phishing; que usa técnicas de engaño para recolectar usuarios y contraseñas por correo electrónico, donde el éxito o fracaso va a depender en mayor medida de los controles que se tengan en medio, siendo el principal: la capacitación y concientización de las personas.

El presente estudio se realiza en una entidad financiera que se rige bajo los lineamientos de la Superintendencia de Banca, Seguros y AFP (SBS), donde se tiene la exigencia de cumplir con ciertos controles para mantener un nivel óptimo de seguridad de la información y ciberseguridad. Es así que se implementa Gophish para contrarestar los ciberataques del tipo phishing y mejorar los controles existentes. Para cumplir dicho objetivo, se usó la metodología de Project Management Institute (PMI) como buena práctica.

El desarrollo de este trabajo ha sido estructurado en cuatro capítulos. En ese sentido el capítulo I contempla los aspectos generales de la investigación, tales como: el problema que se presente resolver, los objetivos que se cumplirán en el desarrollo, los alcances, las limitaciones que surgieron, la justificación del tema de estudio y el estado del arte como una revisión bibliográfica de antecedentes nacionales e internacionales.

El capítulo II contempla el marco teórico de la investigación, que aborda sobre: seguridad de la información y ciberataques, así como conceptos relacionados con la temática del estudio. Finalmente se aborda el marco legal y metodológico con métodos y técnicas de rigor científico que se usará a lo largo del proceso de investigación.

El capítulo III contempla el desarrollo de la solución Gophish de acuerdo a la metodología establecida, donde se brindará todos los detalles para la implementación y cumplir con los objetivos propuestos.

El capítulo IV contempla la presentación y análisis de los resultados, así como el presupuesto estimado para el desarrollo de la investigación y demostración con instrumentos financieros de la viabilidad económica de forma positiva.

CAPITULO 1

ASPECTOS GENERALES

1.1 Definición del Problema

1.1.1 Descripción del Problema

Según el Foro Económico Mundial (2021) basado en su informe de riesgos globales, indica que los ciberataques están catalogados entre los riesgos de mayor probabilidad durante los próximos 10 años. Es así como se puede apreciar en la Figura1 que se ubica dentro del Top 5 para el rango comprendido del 2012 al 2020. En el año 2012 se ubica en el 4to lugar, en el 2014 se ubica en el 5to lugar, en el 2018 se ubica en el 3er lugar y en el 2019 se ubica en el 5to lugar.

	1st	2nd	3rd	4th	5th
2020	Extreme weather	Climate action failure	Natural disasters	Biodiversity loss	Human-made environmental disasters
2019	Extreme weather	Climate action failure	Natural disasters	Data fraud or theft	Cyberattacks
2018	Extreme weather	Natural disasters	Cyberattacks	Data fraud or theft	Climate action failure
2017	Extreme weather	Involuntary migration	Natural disasters	Terrorist attacks	Data fraud or theft
2016	Involuntary migration	Extreme weather	Climate action failure	Interstate conflict	Natural catastrophes
2015	Interstate conflict	Extreme weather	Failure of national governance	State collapse or crisis	Unemployment
2014	Income disparity	Extreme weather	Unemployment	Climate action failure	Cyberattacks
2013	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Water crises	Population ageing
2012	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Cyberattacks	Water crises

Figura1. Top 5 de riesgos globales de mayor probabilidad.

Nota: Recuperado de The Global Risk Report 2021 (p. 14), por World Economic Forum, 2021.

Por lo que se refiere al phishing, como un tipo ciberataque; Microsoft en su informe del 2020 manifiesta que bloquearon más de 13000 millones de correos malintencionados, donde una cantidad mayor a 1000 millones eran ataques de phishing con direcciones URL incrustadas, con el objetivo de robar credenciales. Así mismo, afirma que con el comienzo de COVID-19, como una pandemia global; aumentó el volumen de phishing sobre esta temática en el mes de marzo de 2020 y que disminuyó en los próximos meses manteniéndose estable, según se puede observar en la Figura2 (Microsoft, 2020).

Figura2. Ataques de phishing con temática de COVID-19.

Nota: Recuperado de Microsoft Digital Defense Report (p. 10), por Microsoft, 2020.

De la misma forma, el diario Peru21 publica estadísticas de delitos informáticos proporcionados por la división especializada de la Policía Nacional del Perú, donde se tienen registrados 2125 denuncias por delitos informáticos en el 2019, de los cuales 1761 corresponden a casos de fraude informático. Así mismo, presenta una actualización con fecha de corte 02/12/20, donde se tiene un total de 2354 denuncias por delito informático, de los cuales 1771 corresponden a casos de fraude informático. Finalmente, el diario muestra que las modalidades más usadas por los ciberdelincuentes para delito informático es el phishing, smishing, vishing y SEO posicionamiento (Perú21, 2020).

Por otro lado, se tiene registrado por la entidad reguladora un comunicado con fecha 17 de agosto del 2018, en donde informan que se suspenden las actividades de los bancos temporalmente como manera preventiva, ante el ciberataque dirigido al sistema financiero, que tuvo gran relevancia (Reuters, 2018). Como consecuencia, el sector bancario fue afectado paralizando sus operaciones tanto en los canales presenciales como digitales.

A la fecha ninguna entidad bancaria ha comunicado cómo se inició el ataque y que información resultó expuesta, sin embargo, los expertos señalan que el origen pudo ser un ransonware que explotó las vulnerabilidades de los sistemas expuestos a internet, mientras que otros discrepan que pudo ser un ransomware propagado mediante phishing.

Con respecto a la entidad financiera donde se aplica la presente investigación, inicia sus operaciones en septiembre de 1999 y actualmente ofrece servicios micro financieros de

ahorros y créditos, en sus más de 50 oficinas distribuidas en 12 departamentos a nivel nacional.

De igual importancia se tiene un alcance definido para el Sistema de Gestión de Seguridad de la Información (SGSI) que cubre toda la empresa y fue implementado bajo la circular G-140 que fue emitido por la entidad reguladora. Si bien el estándar de facto para seguridad de la información es la ISO 27001:2013, este no es exigible para las entidades financieras, sin embargo, es adoptado por muchas como buena práctica. Es así como se tiene una brecha entre ambas normas, ya que los enunciados de la circular G-140 son muy genéricos por ello es conveniente realizar un alineamiento hacía la ISO 27001 (Aquije y Jave, 2012).

Debido a ello el investigador identifica que los controles de seguridad implementados en la empresa objeto de estudio tienen un nivel de madurez bajo porque no se encuentran alineados a la ISO 27001, lo que conlleva entre otras cosas: carencia del talento humano en la unidad de seguridad de la información y una inadecuada segregación de funciones respecto al monitoreo de las plataformas de seguridad. Por consiguiente, los controles de seguridad implementados no se monitorean de forma adecuada, y en algunos casos no se realizan, por lo que la entidad queda expuesta a ciberataques no detectados y sin el debido tratamiento para mitigarlos. En efecto la entidad financiera fue afectada en el 2018 por ciberataques de phishing con adjuntos maliciosos, que logró vulnerar la información de los clientes, poniendo en tela de juicio la imagen y prestigio de la empresa.

En definitiva, con todos los antecedentes expuestos surge la necesidad de implementar Gophish para mejorar la seguridad de la información ante ciberataques del tipo phishing, con la finalidad de prevenir los riesgos asociados. En ese sentido, y de igual importancia; se identifica las causas y los efectos que existen dentro de la empresa tal como se muestran en la Tabla1 y Figura3.

Tabla1. Causa y efecto.

Causa	Efecto
Los usuarios hacen click al link de un correo phishing.	Los ciberdelincuentes conocen que usuarios se encuentran activos.
Los usuarios envían información al completar un formulario falso del correo phishing.	Los ciberdelincuentes roban las credenciales de los usuarios.
Los usuarios no reportan los correos phishing.	Los ciberdelincuentes infectan las computadoras de los usuarios.

Fuente: Elaboración propia.

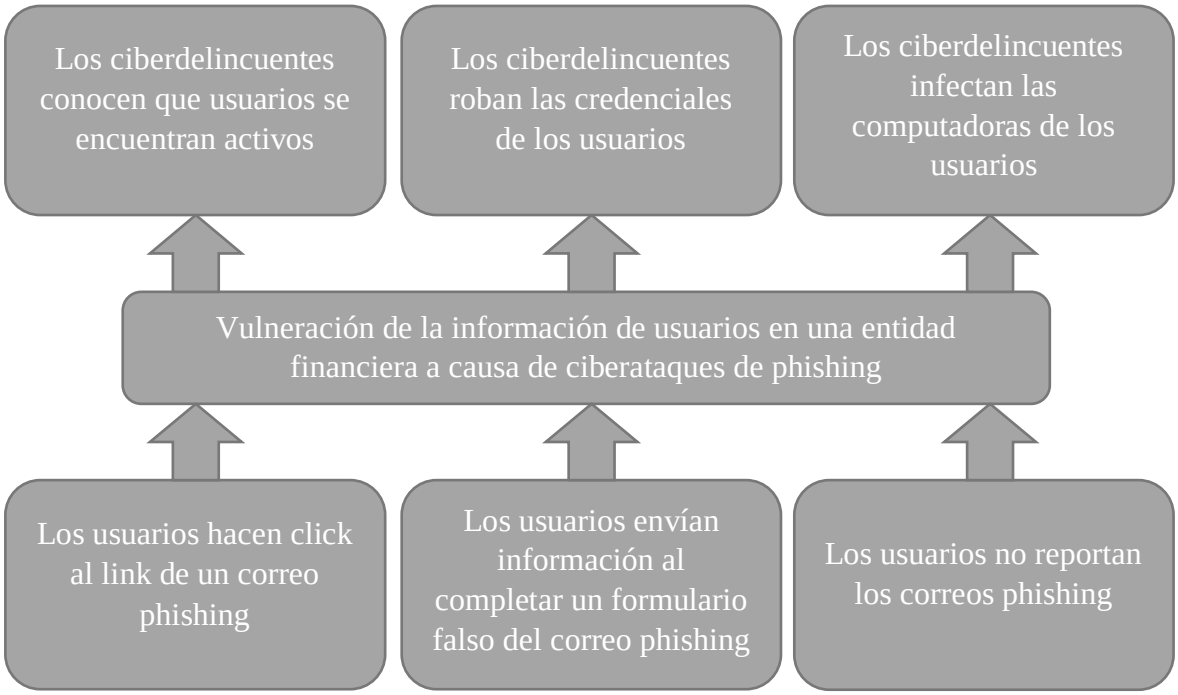


Figura3. Árbol del problema.

Fuente: Elaboración propia.

1.1.2 Formulación del Problema

La presente investigación aborda el problema de vulneración de la información de usuarios en una entidad financiera a causa de ciberataques del tipo phishing, por ello se plantea la siguiente pregunta dentro de la empresa:

¿En qué medida el mejoramiento de la seguridad de la información permite reducir los ciberataques del tipo phishing en una entidad financiera?

1.2 Definición de objetivos

1.2.1 Objetivo general

Mejorar la seguridad de la información para reducir los ciberataques del tipo phishing en una entidad financiera.

1.2.2 Objetivos específicos

1. Reducir el porcentaje de los usuarios que hacen click al link de un correo phishing.

2. Reducir el porcentaje de los usuarios que brindan información al completar un formulario falso de un correo phishing.

3. Aumentar el porcentaje de los usuarios que reportan un correo phishing.

1.3 Alcances y limitaciones

1.3.1 Alcances

Se tiene como alcance definido para la presente investigación, el implementar Gophish en una máquina virtual para una entidad financiera, dimensionado tecnológicamente para un total de no más de 1000 usuarios, sin embargo, el alcance está dirigido para 450 usuarios de nuestros principales interesados como Negocios y Operaciones que se encuentran en las agencias brindando atención al público.

1.3.2 Limitaciones

Las limitaciones que se tiene identificado para la presente investigación se detallan a continuación y están relacionados a:

La disposición de información sensible dentro de la investigación que se encuentra restringida por la entidad financiera, por lo que su uso es mediante información enmascarada. El cual, esta limitante ha sido superado con un permiso previamente gestionado hacia la Gerencia de Seguridad e Inspectoría.

Otra limitación que se identificó para implementar Gophish, fue que al ser software libre no tiene soporte técnico, en ese sentido al presentarse errores no son atendidos por un área especializada. Por el contrario, es solucionado por el investigador, tomando más tiempo en la implementación.

El tiempo ha sido una limitante para el investigador en implementar el modelo propuesto, por consiguiente, se desarrolla aproximadamente en 3 meses. En ese sentido el tiempo para llevar a cabo la investigación fue ajustada, ya que el tiempo de demanda es mayor. Sin embargo, esa limitación ha sido superado debido a que se tiene experiencia en implementaciones previas.

Por otra parte, no se tiene un gap analysis que permita precisar el grado de madurez de los controles existentes y que sirva como una foto del momento para el presente estudio.

1.4 Justificación

La investigación se enfoca en los ciberataques del tipo phishing en una entidad financiera, ya que debido a los errores del factor humano se pone en riesgo a toda una organización. Por lo que para ciberseguridad ese factor sigue siendo el eslabón más débil. Más aún que cada vez estos ciberataques son más elaborados y son confundidos fácilmente, a su vez que se ha incrementado en la empresa de estudio. Por consiguiente, es un desafío en el área de seguridad de la información. Por esa razón se realiza la implementación de Gophish el cual simula ataques de phishing y con los resultados obtenidos se optimiza la seguridad de la información de la empresa.

Por lo tanto, la presente investigación propone un modelo de herramienta contra el phishing, que aporta todos los aspectos técnicos en la implementación del framework de código abierto Gophish en una entidad financiera para mejorar los controles de seguridad de la información existentes, tales como: Concienciación, educación y capacitación en seguridad de la información y notificación de los eventos de seguridad de la información.

Por otra parte, la investigación se justifica económicamente para reducir los costos, debido al uso de un framework de código abierto como Gophish, que para el presente estudio se tiene un presupuesto de S/ 24,728.00 que se encuentra detallado en la gestión de costos del proyecto, frente a una implementación de pago con las mismas dimensiones y características que se estima en S/ 141,200.00. Es así como se obtiene un ahorro significativo de un 82.48%, el cual es viable económicamente para cajas rurales, edpymes y cooperativas, de manera que permite optimizar las finanzas de la organización.

La presente investigación se justifica, además, de forma social al impactar de manera positiva al brindar los conceptos teóricos y prácticos a los trabajadores de una entidad financiera para reconocer un ciberataque de phishing y no caer en la trampa brindando la información solicitada. Esto permite incrementar el compromiso y concientización de los trabajadores, generando confianza a la empresa. Adicional, esto tiene relevancia en tiempos de pandemia por COVID-19, donde hubo ciberataques de phishing para las personas que cobran los diferentes bonos ofrecidos por el estado peruano, es así como los colaboradores de la entidad financiera al estar concientizados en estos temas enseñan a sus familiares lo cual es un efecto multiplicador.

Así mismo se justifica legalmente al ser exigible por la entidad reguladora mediante la circular G-140 en el artículo 4, inciso c) donde textualmente se indica “Desarrollar actividades de concientización y entrenamiento en seguridad de la información”, y en el artículo 5, numeral 5.8, inciso a) donde textualmente se indica “Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información” (SBS, 2009).

1.5 Estado del arte

En el presente capítulo se exponen los antecedentes internacionales y nacionales, relativos a la presente investigación.

Kwak, Lee, Damiano y Vishwanath (2020) describen que, los programas de entrenamiento en ciberseguridad alientan a los usuarios a reportar correos electrónicos de spear phishing, y que además los programas antiphishing proveen interfaces para reportarlos, sin embargo, estudios recientes demuestran que sucede lo contrario, la comunicación es escasa para estos casos. Por ello el objetivo del estudio se centra en determinar porqué más usuarios no reportan correos electrónicos de spear phishing. Es así como los investigadores se apoyan en un marco llamado Teoría Cognitiva Social (TCS) y en Creencias Corporativas de Riesgo Cibernético (CRB) para examinar el comportamiento de los usuarios. En concreto el estudio fue probado mediante encuesta a un total de 386 estudiantes de una universidad del noreste de EE. UU. donde se lograron los siguientes resultados: en primer lugar, las personas no reportan el spear phishing porque son unidireccionales, es decir no reciben una retroalimentación, comentario o beneficio directo. En segundo lugar, existe el temor a los resultados negativos como recriminación, vergüenza y pena.

Conviene subrayar que varios eventos de spear phishing se considera un incidente de seguridad, es así que en la realidad peruana sucede de forma similar en el reporte de incidentes de seguridad, donde las entidades del sector público tienen la obligación de usar las normas de gestión de seguridad de la información desde el año 2004 según lineamientos de la Resolución Ministerial N° 224-2004-PCM, que abarcan entre otros puntos la gestión de incidentes, sin embargo en la encuesta desarrollada por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI, 2010) a un total de 127 instituciones públicas, se observa que un 53.6% de encuestados no reportan los incidentes de seguridad de la información, el cual demuestra que no se cumple con la exigencia normativa y obligatoria. Si bien no se tiene una estadística actual en otros sectores, la experiencia de trabajo del investigador reafirma lo planteado inicialmente: los incidentes de seguridad reportados son escasos.

Sahingoz, Buber, Demir y Diri (2018) describen que, debido al rápido crecimiento de internet, los usuarios cambian la preferencia de compra de un comercio tradicional a uno virtual. Asimismo, en lugar de robar un banco o tienda, hoy en día, los delincuentes intentan encontrar a sus víctimas en el ciberespacio con algunos trucos específicos. Por lo cual, al utilizar la estructura anónima de internet, los atacantes establecieron nuevas técnicas, como el phishing, para engañar a las víctimas con el uso de sitios web falsos para recopilar su información sensible, como IDs de cuenta, nombres de usuario, contraseñas, etc. En concreto, los autores mencionan que comprender si una página web es legítima o phishing es un problema muy desafiante debido a su estructura de ataque basado en la semántica, que explota principalmente las vulnerabilidades de los usuarios. Por otra parte, los autores mencionan que, aunque las empresas de software lanzan nuevos productos anti-phishing, que utilizan listas negras, heurística, enfoques visuales y basados en aprendizaje automático, estos productos no pueden prevenir todos los ataques de phishing. Por ello el objetivo de estudio es proponer un sistema anti-phishing en tiempo real, que utiliza siete algoritmos diferentes de clasificación y basado en características del procesamiento del lenguaje natural (NLP). En efecto, el sistema tiene las siguientes propiedades distintivas de otros estudios de la literatura científica: independencia del idioma, uso de una gran cantidad de phishing y datos legítimos, ejecución en tiempo real, detección de nuevos sitios web, independencia de servicio de terceros y uso de clasificadores con muchas funciones. Para medir el rendimiento del sistema, los autores construyeron un nuevo conjunto de

datos y probaron los resultados experimentales. Es así como, de los siete algoritmos implementados, el algoritmo Random Forest brinda el mejor rendimiento con una tasa de precisión del 97.98% para la detección de URLs de phishing.

Dentro del abanico de activos de información, las personas son tan importantes como el software, infraestructura, plataformas, etc., sin embargo, a pesar de los controles existentes, son los más vulnerables y por tanto el principal blanco de ciberataques, como el phishing, que cambia constantemente adecuándose a la realidad, siendo cada vez más personalizados. Es así como los ataques dirigidos de phishing que incluyen una URL de una página falsa tienen un tiempo de vigencia de lanzado el ataque. Los atacantes compran el dominio de la URL falsa que permanecerá activo en promedio siete días antes de ser dado de baja. De esa manera, los atacantes tienen ventaja y sacan provecho de ello para robar los datos de los usuarios, antes que los sistemas anti-phishing los detecte y anule. Por tanto, para minimizar el riesgo, es importante la capacitación constante y periódica de los usuarios para reconocer cuando un correo o una URL es un phishing.

Baykara y Ziya (2018) describen que, el phishing es una forma de delito cibernético en el que un atacante imita a una persona o institución real promocionándola como persona o entidad oficial a través de un e-mail. Es así como, en este tipo de ataque cibernético, el atacante envía enlaces o archivos adjuntos maliciosos a través de correos electrónicos de phishing que pueden realizar varias funciones, entre ellas: la captura de las cuenta y contraseña de la víctima. Concretamente estos correos electrónicos dañan a las víctimas debido a la pérdida de dinero y el robo de identidad. Por ello el objetivo del estudio es desarrollar un software llamado "Anti-Phishing Simulator", que se integra con el cliente de correo electrónico y verifica el contenido del cuerpo del correo entrante, es así como determina si el mensaje contiene elementos de phishing o algún otro contenido peligroso. El sistema desarrollado usa un algoritmo de clasificación bayesiano que sincroniza con palabras de phishing que fueron agregadas a una base de datos y en base a la puntuación dada, percibe si un correo es o no phishing.

Por otra parte, el investigador del presente estudio tiene una postura diferente respecto al programa desarrollado "Anti-Phishing Simulator", que se retroalimenta con palabras comunes o más frecuentes del tipo phishing cargadas en una base de datos. Es sabido que un correo de phishing contiene en gran medida las mismas palabras que el correo de un usuario normal, por lo que una base de datos o lista de palabras no sería la mejor solución debido a que existiría falsos positivos, es decir se catalogaría correos válidos como phishing. Frente a estos casos, lo adecuado sería tener una lista negra que contenga correos de remitentes o dominios frecuentes de phishing. Cabe aclarar que para ello se debe realizar un análisis previo para identificar si el presunto correo phishing ha tenido contacto anteriormente, sólo así, habiendo identificado que no exista algún vínculo previo, se procede a incorporar en una lista negra.

Bermúdez y Moreira (2020) describen que, la ingeniería social es conocida como el arte del engaño ya que los atacantes logran conseguir información de los usuarios, estableciendo un vínculo al menor descuido. Asu vez los autores mencionan que los atacantes realizan una investigación previa por redes sociales, tales como Facebook, LinkedIn, Instagram y Twitter, por lo que el usuario es responsable por la información que

publica en estas plataformas. Por consiguiente, el objetivo del estudio se centra en examinar las incidencias de los ataques de ingeniería social con el fin de dar a conocer el impacto que estos ataques pueden causar en los estudiantes de una carrera de ingeniería en Guayaquil. En concreto el estudio fue probado mediante encuesta a un total de 144 estudiantes de dicha universidad, donde se lograron los siguientes resultados: el 75% de los estudiantes desconocen el término de ingeniería social y están propensos a ataques informáticos mediante técnicas de manipulación, por otro lado, el 16.4% de los estudiantes se conectan a una red wifi pública para realizar transacciones bancarias y el 87.9% para revisar las redes sociales, lo que conlleva a que un atacante informático mediante un sniffer de red puede ver sus credenciales y contraseñas. Igualmente, el 11.2% de los estudiantes descargan generadores de clave (keygen) para usarlo en programas de versión pagada, sin saber que estos son programas maliciosos que pueden propiciar a la larga extracción de su información.

El investigador del presente estudio identifica desde su experiencia que una de las causas del problema planteado por Bermúdez y Moreira, es la falta de conocimiento de los estudiantes sobre temas de ciberdelitos, las técnicas y los métodos usados, y que esto conlleva a un aumento en el porcentaje de incidencia, por el cual concluye que el porcentaje de incidencia de los ataques informáticos es inversamente proporcional al desconocimiento de los usuarios. Así mismo, las redes sociales se han vuelto relevantes en los últimos años, no sólo para las personas donde comparten información sobre su vida privada de forma pública, sino también para las empresas que participan de forma activa en este sistema sin el filtro debido tanto en la publicación de información o archivos, así como en las respuestas de los chats. Por esta razón, para los ciberdelincuentes las redes sociales es un medio fácil de búsqueda de información expuesta. Por ello, es fundamental como un control preventivo, la concientización de los usuarios que tiene redes sociales y conviven con ellas.

Montenegro (2017) describe que, el uso de las redes sociales exhibe a los usuarios a problemas de seguridad del tipo ingeniería social o afectación a su privacidad, debido a la información que estos publican y comparten, a su vez que es un tema poco abordado por la investigación científica. Asimismo, describe que los atacantes informáticos que tienen en la mira una empresa, canalizan sus esfuerzos en obtener información de los empleados que tienen un perfil en una red social, siendo esto un medio para el objetivo final que es introducir malware en los teléfonos o computadoras de los empleados que fueron víctimas de la ingeniería social. Por ello el objetivo del estudio se centra en elaborar una metodología para evaluar la seguridad de los usuarios que tienen redes sociales, contra ataques de ingeniería social. Es así como el autor propone un metodo de evaluación denominado ISASNET (Information Security Assessment on Social Networks) que considera los siguientes puntos: en primer lugar, se evalúa el perfil de un usuario que tiene una red social, por ejemplo, la fecha y lugar de nacimiento, estado civil, lugar de trabajo, lista de amigos, entre otros. En segundo lugar, se realiza un análisis de las publicaciones que efectúa el usuario, por ejemplo, un estado o foto que se encuentre visible para todos. En tercer lugar, se evalúa las configuraciones de seguridad de la cuenta, por ejemplo, una contraseña débil, códigos de recuperación, entre otros.

De acuerdo con el autor, resulta de gran importancia entrar en conciencia respecto de la información privada que las personas publican en las redes sociales, ya que los atacantes informáticos podrían sacar provecho y usarlo en su contra. Por ejemplo, es sabido que, para restablecer una contraseña, cualquier sistema te solicita unas preguntas de seguridad como validación de que eres la persona quien dice ser, es aquí donde los atacantes usan la información recopilada de las redes sociales para obtener acceso. Por lo general las redes sociales más comunes para obtener información son: Facebook y LinkedIn. Es más, en la actualidad, las empresas usan una red social del tipo empresarial que fue desarrollada por Facebook, el cual se llama Workplace, donde los atacantes tendrían la información de primera mano de los trabajadores, por ejemplo, fotos de su espacio de trabajo, documentos compartidos, relación de trabajadores y jefes directos, números de teléfono, entre otros.

Quispe (2020) describe que, existe un alto índice de ciberataques de phishing en la entidad financiera objeto de estudio por lo que los colaboradores menos concientizados se encuentran expuestos, por lo que resulta necesario adquirir una solución Security Awareness, que a su vez surge como una recomendación de una auditoría externa donde expusieron la oportunidad de mejorar y elevar las capacidades de ciberseguridad de la entidad financiera. Por ello el objetivo del estudio se centra en implementar Wombat Security Awareness para reducir ciberataques de phishing del personal de la entidad financiera. Los módulos implementados por el autor fueron los siguientes: CyberStrength para las capacitaciones de seguridad en formato virtual, ThreatSim para el envío de correos simulados de phishing y PhishAlarm que es un complemento del Outlook para reportar los correos de phishing. Se realizó una prueba de una campaña de phishing dirigido a 13,248 usuarios, donde 5,144 usuarios abrieron el mensaje, 953 usuarios hicieron click en el enlace del phishing y 682 usuarios lo reportaron.

En el sector financiero los ciberataques de phishing son cada vez más usuales y son difíciles de detectar por los colaboradores debido a que no cuenta con una concientización del riesgo que puede causar en la organización, sumado a la falta de capacitación, así como al reporte o comunicación del incidente en el momento que se presenta. Por ello es importante la implementación de soluciones de seguridad como un mecanismo de control y protección frente a las amenazas de ciberseguridad con alto índice de ataque como el phishing. Por ello de acuerdo con el autor, lo investigado explica la importancia de la implementación de una solución pagada llamada Wombat Security Awareness de la empresa Proofpoint, con los módulos de CyberStrength para las capacitaciones con cursos de seguridad, el módulo de ThreatSim para la simulación de un phishing, y una extensión del correo electrónico denominada PhishAlarm que sirve como un botón para reportar los casos de phishing.

CAPITULO 2

MARCO TEÓRICO

2.1 Fundamento teórico

2.1.1 Seguridad de la información

En líneas generales se encarga de preservar la confidencialidad, integridad y disponibilidad de la información. También abarca otros atributos como no repudio y trazabilidad, sin embargo, no se los considera como principales según las fuentes bibliográficas que fueron consultadas.

Se apoya de un Sistema de Gestión de Seguridad de la Información (SGSI) para definir el alcance, identificar los activos principales, evaluar los riesgos e implementar los controles, como parte de un sistema de mejora continua.

2.1.1.1 Pilares de seguridad de la información

2.1.1.1.1 Confidencialidad

Se define a confidencialidad como un atributo inherente a la información, donde sólo es accesible por las personas que fueron previamente autorizadas. Por poner un ejemplo, un acta de comité de riesgos, donde participan los directores y se definen las estrategías para el negocio, debe ser restringido mediante el sello de confidencial únicamente a los involucrados de dicha reunión. Cabe resaltar que este documento no es catalogado como interno, ni público mucho menos.

No obstante, según Prowse (2018) propone un ejemplo, donde el autor menciona que para las personas, un dato confidencial, son los números de seguro social (u otra identificación específica del país), información de la licencia de conducir, cuentas bancarias y contraseñas, etc. Así mismo, menciona que para las organizaciones, un dato confidencial puede incluir toda la información anterior, pero en realidad denota la privacidad de los datos. Para finalizar el autor concluye que los datos son confidenciales, cuando la organización trabaja arduamente para asegurarse de que sólo las personas autorizadas puedan acceder a ellos.

2.1.1.1.2 Integridad

Se define a integridad como un atributo inherente a la información, donde permanece intacta y sin alteraciones, bien sea parcial o total. Por poner un ejemplo, la descarga de un software pagado viene firmado y tiene una cantidad de bytes establecidos, así como la fecha de creación. En ese sentido, la página web de descarga, publica el resultado de la ejecución del algoritmo hash MD5 o bien SHA1, SHA2 o SHA3, que es un número que verifica la integridad del archivo, entonces una vez decargado el software se ejecuta el mismo algoritmo hash donde el resultado debe ser el mismo número, lo que significa que el programa no ha sido alterado.

Según la ISO 27000, define integridad como la propiedad de exactitud e integridad (ISO, 2014).

En cambio, según Prowse (2018) menciona que la integridad significa que los datos no se han manipulado. Por otro lado, la autorización es necesaria antes de que los datos se puedan modificar de alguna manera. En particular, el autor aclara que si una persona elimina un archivo requerido, ya sea de forma maliciosa o inadvertida, se viola la integridad de ese archivo. En efecto, debe haber permisos para evitar que la persona elimine el archivo.

2.1.1.1.3 Disponibilidad

Se define a disponibilidad como un atributo inherente a la información, donde debe estar accesible y disponible en el momento que se necesite. Por poner un ejemplo, al realizar pruebas de continuidad del negocio, se busca que sea transparente y no se vea afectado las operaciones, por lo que la información que se usa en las transacciones financieras no se indisponga, por el contrario el proceso debe fluir sin interrupciones.

Por otro lado, según Prowse (2018) menciona que la disponibilidad significa que los datos se pueden obtener independientemente de cómo se almacene, acceda o proteja la información. Así mismo, el autor aclara que los datos deben estar disponibles independientemente del ataque malintencionado que pueda perpetrarse en ellos.

En efecto, a modo de resumen al dialogar sobre seguridad de la información se viene a la mente los tres pilares, o también conocido como dimensiones o triada de seguridad de la información que son básicamente propiedades que se buscan proteger en un activo de información, según se puede observar en la Figura4.

Figura4. Pilares de seguridad de la información.

Fuente: Elaboración propia.

2.1.2 Ciberataques

Son ataques realizados usando el ciberespacio o mediante internet, donde los delincuentes informáticos usan técnicas y tácticas para afectar cualquier tipo de entidad, bien se universidades, empresas, hospitales e incluso una misma nación. Para hacer frente a esto, cada entidad establece su propio sistema de defensa, tal es el caso de Perú, donde se delega dicha responsabilidad al Comando Conjunto de las Fuerzas Armadas. Por poner otro ejemplo en EE. UU. la agencia encargada de ciberseguridad en toda la nación es USCYBERCOM, que colabora con el pentágono.

En la actualidad existen una gran cantidad de ciberataques y su clasificación se hace extensa por diversos factores, pudiendo agruparse por objetivo de ataque, vector de ataque o técnicas utilizadas. Es así como según MITRE Corporation (2021) desarrolla una base de conocimientos denominada MITRE ATT&CK con las técnicas y tácticas usadas por los ciberdelincuentes, según se puede observar en la Figura5 que la fecha se tiene un total de 206 técnicas de ataque.

Figura5. Matriz de técnicas de ataque.

Nota: Recuperado de ATT&CK Matrix for Enterprise [Imagen], por MITRE Corporation, 2021. Recuperado de https://attack.mitre.org/matrices/enterprise/

2.1.2.1 Phishing

El phishing es conocido como pesca de información, debido a que se usa técnicas de ingeniería social, como el engaño, para persuadir a la víctima y tratar de recolectar su usuario y contraseña mediante correo electrónico. El atacante puede persuadir de diferentes formas usando el cuerpo o asunto del correo, donde se puede redactar de tal forma que la víctima sienta: temor, inferioridad o urgencia. Por lo general se usan links para que el usuario haga click y cargue una página web falsa de cualquier establecimiento, pudiendo ser del: banco, video streaming, redes sociales, entre otros.

Igualmente, Hornetsecurity (s.f.) menciona que “el phishing es un intento de fraude electrónico en el que se envía al destinatario un correo electrónico falso, que a menudo no reconoce como tal a primera vista. Este método de ataque, en forma de un correo

electrónico de aspecto profesional, a menudo está diseñado de tal manera que el destinatario puede ser persuadido a revelar datos confidenciales. Esto se refiere, por ejemplo, a los datos personales. En este caso, los atacantes recurren a empresas o instituciones de renombre que, por ejemplo, están situadas en el sector financiero o comercial. El término phishing proviene del mundo angloparlante y en principio se refiere a un viaje de pesca. Un correo electrónico especialmente diseñado para el ataque sirve de cebo para el cibercriminal, que lo reenvía varias veces a sus posibles víctimas, como los empleados de una empresa."

2.1.2.1.1 Tipos de phishing

2.1.2.1.1.1 Phishing tradicional

Según Welivesecurity (2015) es uno de los más sencillos de analizar técnicamente, ya que generalmente está asociado a la copia idéntica de un sitio web conocido por la víctima, donde la URL es falsa y los datos ingresados son enviados al ciberdelincuente, tal como se puede apreciar en la Figura6.

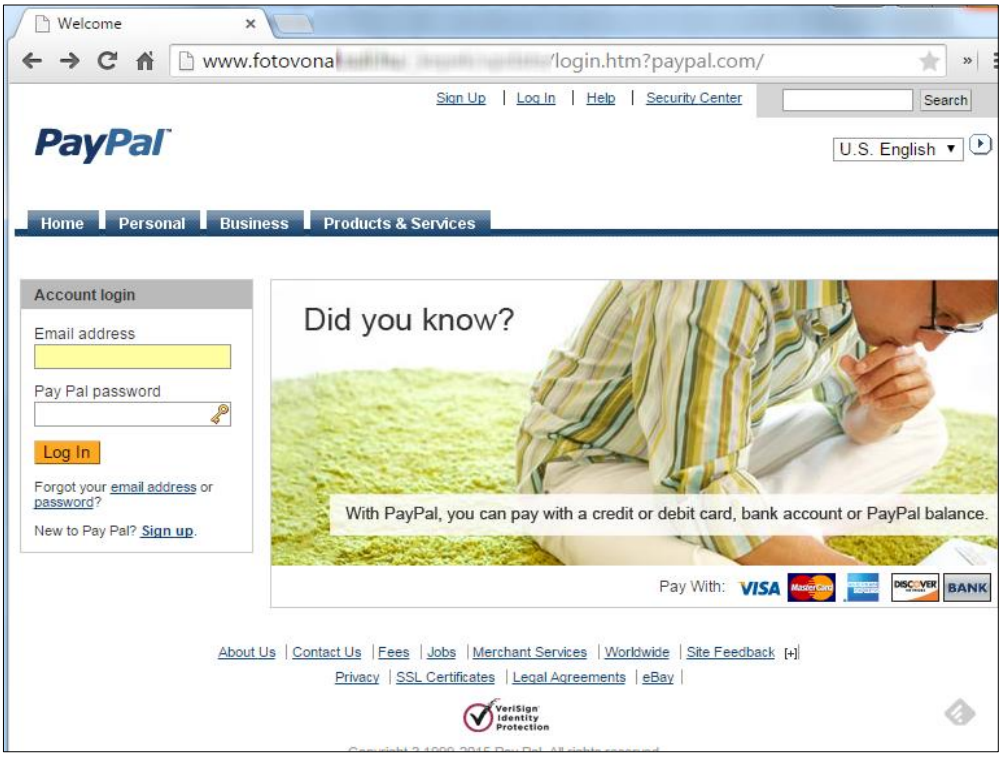


Figura6. Phishing tradicional.

Nota: Recuperado de 5 tipos de phishing en los que no debes caer [Imagen], por Welivesecurity, 2015. Recuperado de https://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing/

2.1.2.1.1.2 Phishing redirector

Según Welivesecurity (2015) es una técnica usada en campañas masivas, lo que conlleva a un menor porcentaje de víctimas afectadas y credenciales comprometidas.

La preparación del phishing cuenta con un mayor nivel de complejidad y por lo general usan acortadores URL en los mensajes, para extender el tiempo que toman a las plataformas de seguridad encontrar y suprimir el contenido de los sitios fraudulentos, tal como se puede apreciar en la Figura7.

Figura7. Phishing redirector.

Nota: Recuperado de Cuidado: Correo "Consultas Clientes" es phishing [Imagen], por AntiPhishing Latinoamérica, 2020. Recuperado de https://twitter.com/AntiPhishing_La/status/1213209089104330757/photo/1

2.1.2.1.1.3 Spear phishing

Según Welivesecurity (2015) se diferencia al estar orientado a personas o grupos reducidos. Es así como las campañas son más personalizadas y con mayor cantidad de víctimas debido a que estos ataques apuntan a personas con pocos conocimientos técnicos de informática y por lo general son correos que generan empatía y confianza.

No es usual que se vean casos de afectación a entidades bancarias, debido a que no se busca ser masivo, por el contrario, está dirigido a personas con perfiles definidos, tal como se aprecia en la Figura8.

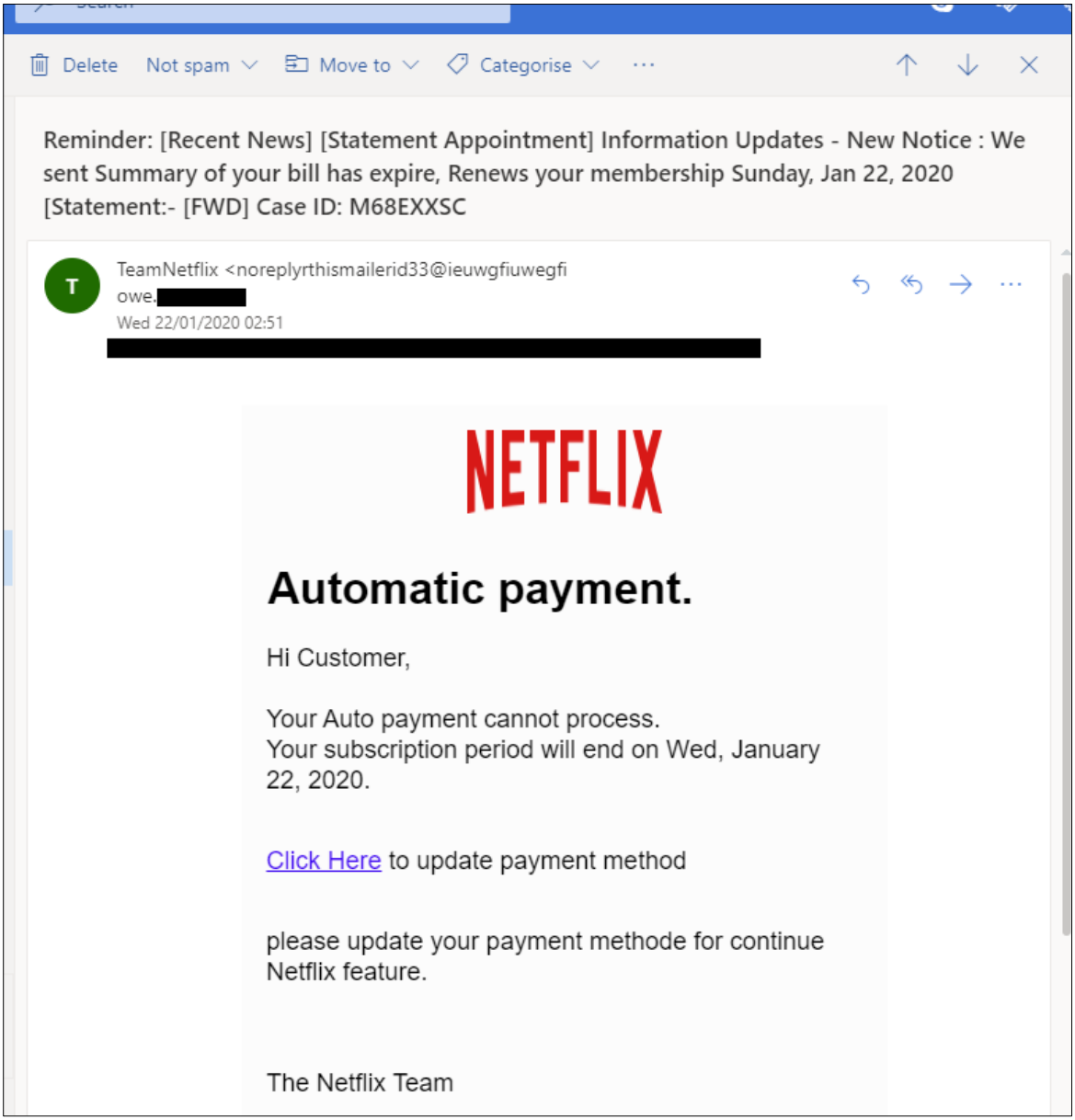


Figura8. Spear phishing.

Nota: Recuperado de Spear Phishing 101: lo que necesitas saber [Imagen], por Malwarebytes, 2020. Recuperado de https://malwarebytes.antimalwares.es/890-2

2.1.2.1.1.4 Smishing

Según Welivesecurity (2015) es un tipo de estafa donde los ciberdelincuentes se hacen pasar por entidades conocidas y envían un mensaje de texto advirtiendo a la víctima de que ha ganado un premio. Es así como usualmente la víctima realiza al menos uno de los siguientes: hace click en un hipervínculo, llama a un número de teléfono o responde el mensaje de texto, tal como se visualiza en la Figura9.

Figura9. Smishing.

Nota: Recuperado de Una campaña de phishing que suplanta al banco Santander se propaga por correo y SMS [Imagen], por Protegerse, 2019. Recuperado de https://blogs.protegerse.com/2019/06/04/una-campana-de-phishing-que-suplanta-al-banco-santander-se-propaga-por-correo-y-sms/

2.1.2.1.1.5 Vishing

Según Welivesecurity (2015) es un tipo de estafa donde los ciberdelincuentes montan falsos centros de atención telefónica para realizar llamadas.

Por lo general está relacionado con otro ataque, para complementar y lograr una mayor credibilidad y así lograr engañar a la víctima de forma más sencilla y eficaz.

Por otro lado, BBVA (2019) indica que este ataque consta de 02 pasos: en primer lugar, el ciberdelincuente obtiene información previa mediante phishing. Es en este momento donde se necesita una clave digital o token para realizar y validar una operación financiera. En segundo lugar, el ciberdelincuente contacta al cliente haciéndose pasar por personal del banco, argumentando que la cuenta presenta actividad sospechosa por lo que es necesario su clave digital o token.

2.2 Marco conceptual

2.2.1 Gophish

Vallejo (2020) define el término como: “Gophish es opensource y una potente herramienta de phishing, el cual facilita la realización de pruebas a las organizaciones expuestas a ataques de phishing. Gophish permite definir los objetivos, lanzar la campaña y hacer seguimiento de los resultados” (p.23).

Igualmente, Bermúdez y Moreira (2020) indican que Gophish es una herramienta multiplataforma de código abierto basada en lenguaje de GO, la cual está diseñada para realizar pruebas de penetración en ataques de phishing.

Así mismo, Pirocca, Allodi y Zannone (2020) describen a Gophish como uno de los marcos de código abierto más populares y ampliamente utilizados para probar la conciencia de seguridad de las organizaciones y su exposición al phishing. Por otra parte, mencionan que ofrece una arquitectura cliente servidor que conecta a una base de datos para almacenar información de la víctima y la campaña. Además, Gophish proporciona las principales funcionalidades para realizar una campaña de phishing, tales como: interfaz gráfica, página de aterrizaje, correo personalizado, captura de eventos y evaluación.

En efecto Gophish es un framework de seguridad muy versátil que tiene todas las funcionalidades necesarias para implementar una campaña de phishing a medida, por ello dentro del mundo open source es uno de los más usados y recomendados. Dentro de la literatura científica se indica que Gophish es útil principalmente para empresas categorizadas como PYMES por el bajo presupuesto que le asignan para temas de

seguridad de la información, muy por el contrario que paras las empresas grandes pueden comprar una solución similar en versión pagada, con el soporte y apoyo que ello conlleva. Finalmente, para aclarar que Gophish sirve para preparar a los usuarios, mediante simulaciones de ciberataques de phishing, y saber cómo actuar frente a un ataque real.

2.2.2 Sistema de Gestión de Seguridad de la Información (SGSI)

Aquije y Jave (2012) definen el término como: “Parte del sistema gerencial general basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Se debe tener en cuenta que, el sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos” (p.106).

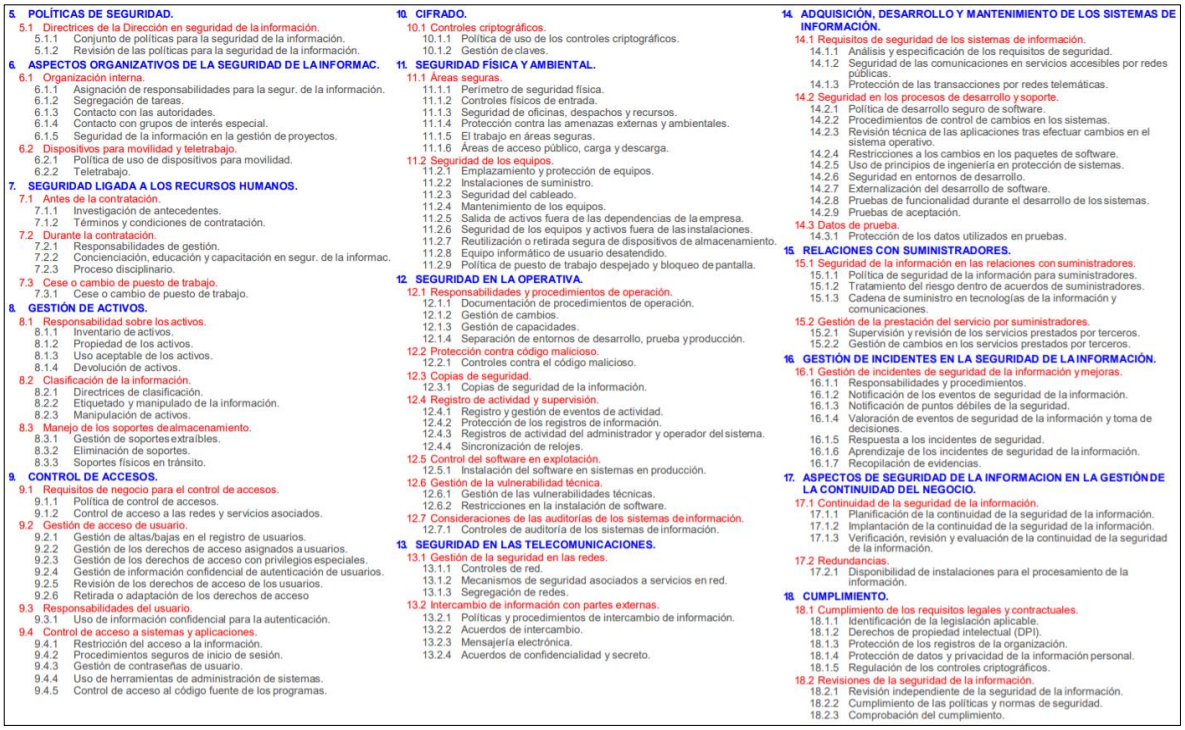
Por otra parte, Gómez y Fernández (2015) mencionan que: “Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.

Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada” (p.11).

2.2.3 Controles de seguridad de la información

Según Reciprocity (2019) son medidas que se toman para reducir los riesgos de seguridad de la información, tales como: violaciones de los sistemas de información, robo de datos y cambios no autorizados en la información o los sistemas digitales. Estos controles de seguridad están destinados a ayudar a proteger la confidencialidad, integridad y disponibilidad de la información, y generalmente se implementan después de una evaluación de riesgos de seguridad de la información.

Tomando como referencia la ISO/IEC 27002 se indica que los controles de seguridad son implementados, después de: haber identificado los requisitos de seguridad de la información, evaluar los riesgos para los activos de información y tratamiento de riesgos. En ese sentido la norma ofrece orientación sobre una amplia gama de controles que se aplican en muchas organizaciones mediante114 controles, agrupados en 14 dominios y 35 objetivos de control, según se puede apreciar en la Figura 10.



5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

Figura10. Controles de ISO/IEC 27002:2013.

Fuente: Elaboración propia.

2.2.3.1 Concienciación, educación y capacitación en seguridad de la información

Según la ISO 27002 (2015) define el control como: “Todos los empleados de la organización y, cuando corresponda, los contratistas, deberían recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo” (p.20).

Por otra parte, en la norma se menciona una guía de implementación que toca varios puntos, entre los más resaltantes respecto a que el programa de concienciación debe estar alineado a la función que realizan los empleados y que cubra aspectos entre otros de: notificación de incidentes de seguridad de la información; seguridad de las contraseñas; controles de software malicioso y escritorio limpio. Así mismo, se precisa que el programa debe estar en consonancia con las políticas y los procedimientos relevantes de seguridad de la información de la organización, teniendo en cuenta la información de la organización que ha de protegerse y los controles que se han implantado para proteger dicha información.

2.2.3.2 Notificación de los eventos de seguridad de la información

Según la ISO 27002 (2015) define el control como: “Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible” (p.85).

Por otra parte, en la norma se menciona una guía de implementación que toca varios puntos, entre los más resaltantes respecto a que todos los trabajadores, contratistas y terceros deben conocer su responsabilidad de comunicar cualquier evento de seguridad de la información lo antes posible. Así mismo, debe conocer el procedimiento de comunicación de eventos de seguridad de la información y el punto de contacto.

En concreto, los siguientes puntos son válidos para comunicar los eventos de seguridad cuando existan situaciones de: control ineficaz de la seguridad; quebrantamiento de las expectativas de integridad, confidencialidad y disponibilidad de la información; errores humanos; incumplimiento de políticas o directrices; quebrantamiento de las directrices de seguridad física; cambios incontrolados del sistema; disfunciones del software o hardware; violaciones de acceso y finalmente comportamientos anómalos del sistema que puede ser un indicador de un ataque de seguridad o una brecha de seguridad.

2.3 Marco legal

Se precisa que la normativa actual que es exigible por la SBS es la circular G-140, que será derogada el 01 de julio de 2021, fecha que entra en vigencia la Resolución SBS N^0 504-2021-Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, que profundiza en temas de ciberseguridad y resulta necesario debido al contexto que atraviesa el país por COVID-19, sumado a la creciente interconectividad y mayor adopción de canales digitales para la provisión de los servicios, debido a las medidas dispuestas por el gobierno para el confinamiento, así como la virtualización de algunos productos del sistema financiero, de seguros y privado de pensiones, lo que hace necesario que las empresas de dichos sistemas supervisados fortalezcan sus capacidades de ciberseguridad y procesos de autenticación.

2.3.1 Estándares Internacionales

- ISO/IEC 27001:2013 Tecnología de la información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información (SGSI) – Requisitos.

- ISO/IEC 27002:2013 Tecnología de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información.

2.3.2 Normativas Nacionales

- Circular G-140-2009-Gestión de la seguridad de la información.

2.4 Marco metodológico

2.4.1 Enfoque de la investigación

De acuerdo con la naturaleza de la investigación el estudio tiene un enfoque cualitativo, es así como Hernández, Fernández y Baptista (2014) indican que dicho enfoque “utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación” (p.7).

2.4.2 Alcance de la investigación

De acuerdo con el fenómeno de la investigación el estudio tiene un alcance descriptivo, es así como Hernández et al. (2014) indica que:

> Se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas. (Hernández et. al, 2014, p.92)

2.4.3 Diseño de la investigación

De acuerdo con el objeto de la investigación el estudio tiene un diseño no experimental, es así como Hernández et al. (2014) indica que:

> Podría definirse como la investigación que se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios en los que no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para analizarlos. (Hernández et. al, 2014, p.152)

2.4.4 Metodología de desarrollo del proyecto

La presente investigación se desarrolla bajo las buenas prácticas del Project Management Institute (PMI), tomando en consideración el PMBOK respecto a 05 grupos de procesos: inicio, planificación, ejecución, monitoreo y control, y cierre, según se puede observar en la Figura11.

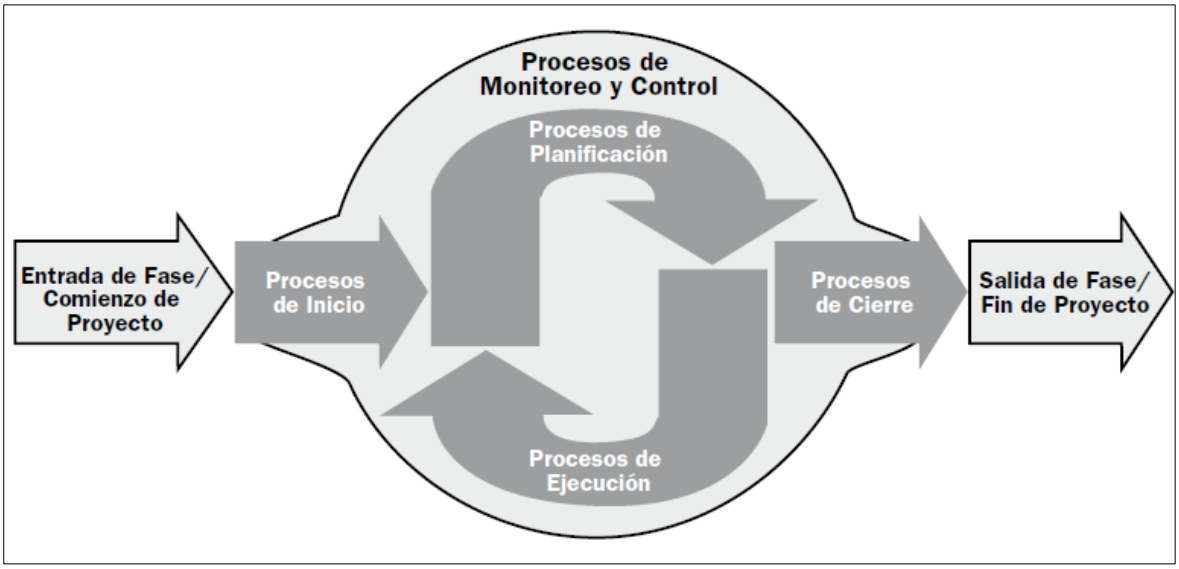


Figura11. Grupo de procesos de la dirección de proyectos.

Nota: Recuperado de Guía de los fundamentos para la dirección de proyectos (Guía del PMBOK) (p. 50), por Project Management Institute, 2013.

CAPITULO 3

DESARROLLO DE LA SOLUCIÓN

3.1 Caso de negocio

En la presente investigación se describe de forma detallada la problemática de la empresa objeto de estudio y la solución para mejorar la seguridad de la información frente a ciberataques del tipo phishing, el cual impacta positivamente respecto a la misión, visión y metas del negocio, el cual se alinea a los objetivos estratégicos del proyecto.

Misión

“Acompañamos el desarrollo de sus emprendimientos proporcionando servicios y productos financieros oportunos y adecuados a sus necesidades”.

Visión

“Contribuir al desarrollo de las familias y personas emprendedoras del Perú, facilitando los servicios y productos financieros que demanden”.

Metas del Negocio

A continuación, se identifican dos metas del negocio con sus respectivas métricas para evaluar su cumplimiento:

1. Gestión de riesgo de negocio:

a. Porcentaje de objetivos de negocio y servicios críticos cubiertos por la evaluación de riesgos.

b. Proporción de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes.

c. Frecuencia de actualización del perfil de riesgo.

2. Continuidad y disponibilidad del servicio del negocio:

a. Número de interrupciones del servicio al cliente o procesos de negocio que han causado incidentes significativos.

b. Coste de incidentes para el negocio.

c. Número de horas de procesamiento de negocio perdidas debido a interrupciones del servicio no planificadas.

d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados.

Objetivos estratégicos del proyecto

- Mejorar la seguridad de la información ante ciberataques del tipo phishing en un 54.83% para una entidad financiera.

Organigrama

La presente investigación se desarrolla en una entidad financiera que tiene el siguiente organigrama establecido, el cual se aprecia la Unidad de Seguridad de la Información dentro del Departamento de Seguridad e Inspectoría en la esquina inferior derecha, según se puede observar en la Figura12.

Los cargos establecidos en la Unidad de Seguridad de la Información con los siguientes:

- Gerente de Seguridad e Inspectoría – César Lavalle.
- Jefe de Seguridad de la Información – Wilfredo Malla.
- Analista de seguridad de la Información – Jou Jancachagua.

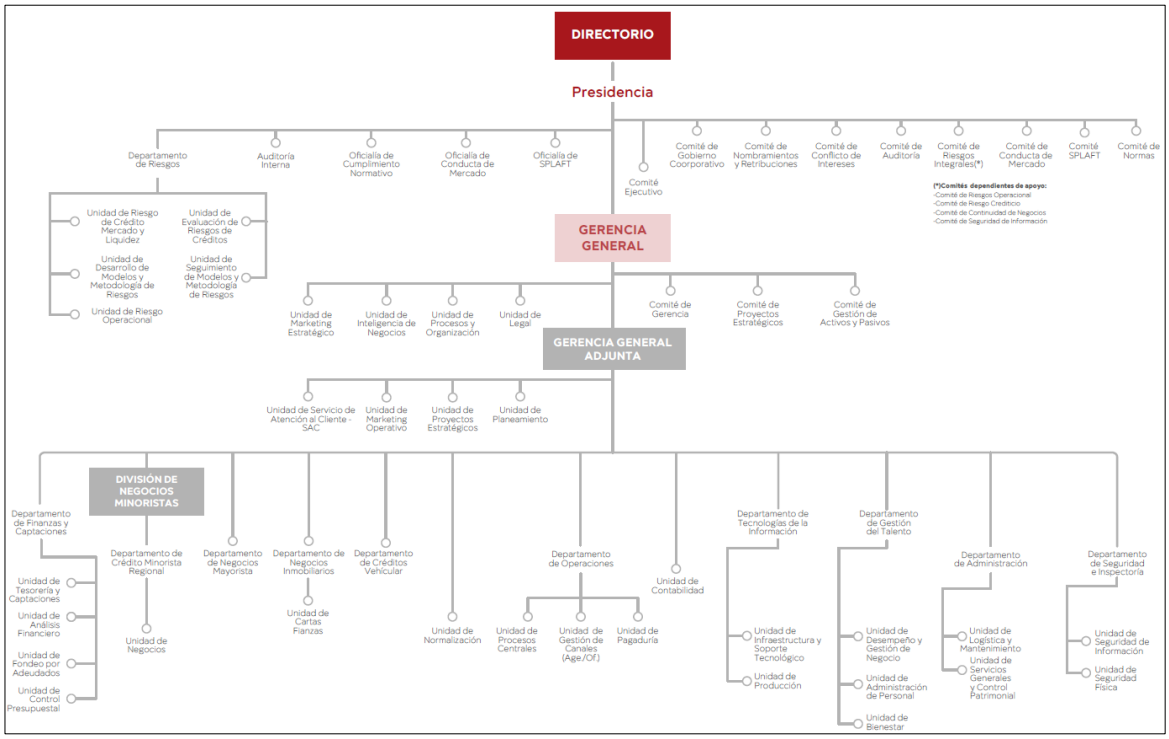


Figura12. Organigrama de la entidad financiera.

Fuente: Elaboración propia.

3.2 Gestión del desarrollo de la solución

Según la metodología de desarrollo del proyecto, la gestión se ejecuta siguiendo la guía de buenas prácticas de PMBOK, considerando las siguientes áreas del conocimiento que se detallan a continuación: gestión del alcance, gestión del tiempo, gestión del costo, gestión de la calidad, gestión de las comunicaciones, gestión del riesgo, gestión de adquisiciones, gestión de interesados y gestión de la integración del proyecto.

3.2.1 Gestión del alcance

3.2.1.1 Plan de gestión del alcance

En cuanto al plan de gestión del alcance para el proyecto de implementación de Gophish en una entidad financiera, se considera el proceso de definición del alcance, proceso de EDT, proceso de verificación del alcance y proceso de control del alcance, según se detalla a continuación.

Proceso de definición del alcance

La definición del alcance del proyecto de implementación de Gophish en una entidad financiera, se ejecutará de la siguiente manera:

- En reunión de equipo de proyecto, tanto el equipo del proyecto como el sponsor, definirán lo siguiente: el alcance del proyecto, el procedimiento de atención de cambios del alcance y las personas autorizadas para solicitar cambios en el alcance, las personas autorizadas de analizar los cambios y las personas que validarán los cambios.

Proceso de elaboración de la Estructura de Desglose de Trabajo (EDT)

La elaboración de la EDT del proyecto de implementación de Gophish en una entidad financiera, se ejecutará de la siguiente manera:

- La EDT será elaborada por el equipo del proyecto mediante la herramienta WBS Chart Pro, tomando en cuenta los principales entregables del proyecto.

Proceso de verificación del alcance

La comprobación del alcance del proyecto de implementación de Gophish en una entidad financiera, se ejecutará de la siguiente manera:

Cada entregable, será verificado por el sponsor del proyecto, y de ser aceptado se remitirá al Gerente de Seguridad e Inspectoría, caso contrario se tendrá las observaciones para su respectiva corrección.

Proceso de control del alcance

El proceso de verificación del alcance del proyecto de implementación de Gophish en una entidad financiera, se ejecutará de la siguiente manera:

- El Project Manager será el responsable de verificar el cumplimiento de los entregables de acuerdo con lo acordado en el acta de reunión 001. Si el entregable es aprobado es enviado al Gerente de Seguridad e Inspectoría, caso contrario el entregable será devuelto a su responsable, precisando las consideraciones para ser mejoradas.

- El Gerente de Seguridad e Inspectoría podrá presentar sus observaciones relativos a los entregables. Para ello promoverá una reunión con el Project Manager, y presentar sus requerimientos de cambio. De ser aceptado la solicitud del cambio, se establecerá un acta de cambio.

3.2.1.2 Enunciado del alcance del proyecto

En cuanto al enunciado del alcance para el proyecto de implementación de Gophish en una entidad financiera, se considera los objetivos del proyecto, descripción del alcance del proyecto, requerimientos del proyecto, requerimientos del producto, exclusiones del proyecto entregables del proyecto, criterios de aceptación del producto y restricciones del proyecto que se detallan a continuación.

Objetivos del proyecto

Con relación al objetivo del proyecto de implementación de Gophish en una entidad financiera, se tienen los siguientes:

- Implementar Gophish en una entidad financiera de acuerdo con las características técnicas, estipuladas en el acta de reunión 001, que refiere al cumplimiento del alcance, tiempo y costo.

- Mejorar la seguridad de la información ante ciberataques del tipo phishing en un 54.83% para una entidad financiera.

Descripción del alcance del proyecto

El alcance del proyecto se refiere a la implementación de Gophish para una entidad financiera, ubicada en el distrito de San Isidro. El proyecto es implementado bajo Linux, en un entorno aislado del ambiente de producción, dimensionado para un total de no más de 1000 usuarios.

La implementación integral del proyecto comprende: Interfaz web; acceso con usuario y contraseña; dashboard; menú de campaña; menú de usuarios y grupos; menú de plantilla de email; menú del landing page; menú de configuración.

Requerimientos del proyecto

Con relación al requerimiento del proyecto de implementación de Gophish en una entidad financiera, se tienen los siguientes:

- Configurar una máquina virtual con Linux.
- Habilitar un módem inalámbrico con plan de internet ilimitado.
- Habilitar una posición por el tiempo que durará el proyecto.
- Habilitar una laptop como mínimo con procesador core i7, ram de 16 GB, disco de 500 GB.
- Crear 05 cuentas de correo gratuito en Gmail.
- Contar con los correos electrónicos de todos los colaboradores.

Requerimientos del producto

El proyecto de implementación de Gophish en una entidad financiera estará compuesto por una página web de administración compuesto por los siguientes módulos como principales entregables que se distribuyen de la siguiente manera:

- **Dashboard**: Se presenta el resumen de la campaña de phishing, la cantidad de correos enviados, la cantidad de correos abiertos, la cantidad de usuarios que hacen click al link del phishing, la cantidad de usuarios que fueron víctimas del phishing, la cantidad de correos reportados por los usuarios, el histórico de las campañas recientes, la fecha de creación de campaña y el estado actual.
- **Campañas**: Se presenta el nombre de la campaña de phishing, la fecha de creación, la plantilla para crear una nueva campaña, una plantilla de email, el diseño del landing page, la dirección URL, la programación para la fecha de envío del phishing, una prueba de salida del correo phishing y lista de usuarios o grupos para enviar el phishing.
- **Grupos y usuarios**: Se presenta los usuarios enrolados al sistema, los nombres y apellidos, cargo, correo, así como la cantidad de miembros, la fecha de modificación y la posibilidad de importar usuarios.
- **Plantilla de correo**: Se presenta una plantilla de correo para modificar el asunto, el cuerpo del correo en html y adjuntar archivos.

- **Landing page**: Se presenta una plantilla para clonar una página web mediante la URL, así como su modificación en html.

- **Perfil de envío**: Se presenta un módulo para indicar el correo de origen, el host del servidor de correo, así como el usuario y password del correo y un test de envío de correo.

- **Configuración**: Se presenta un módulo para crear un usuario y password de administración, así como colocar una contraseña nueva.

Exclusiones del proyecto

Con relación a las exclusiones del proyecto de implementación de Gophish en una entidad financiera, se tienen los siguientes:

- Se excluye de las pruebas a los directores, asociados y accionistas que tengan correo de la entidad financiera.

- Se excluye de las pruebas a los proveedores o contratistas que tengan correo de la entidad financiera.

Entregables del proyecto

Los entregables del proyecto está dimensionado en el diagrama de desglose de trabajo – EDT, que comprende en:

- **Gestión del proyecto**, incluye los siguientes entregables: plan de gestión del alcance, enunciado del alcance del proyecto, EDT, cronograma de actividades, presupuesto, plan de calidad, matriz de comunicaciones, matriz de riesgo, matriz de adquisiciones, registro de interesados, reunión de seguimiento, registro del valor ganado del proyecto, acta de cierre del proyecto y acta de conformidad.

- **Análisis**, incluye los siguientes entregables: diagrama de actividades.

- **Diseño**, incluye los siguientes entregables: listado de requisitos funcionales.

- **Pruebas**, incluye los siguientes entregables: reporte de fallas.

- **Implementación**, incluye los siguientes entregables: documentación de usuario.

Criterios de aceptación del producto

Los criterios de aceptación del proyecto contemplan los siguientes:

- La implementación de la interfaz web debe cumplir al 100% con las características técnicas establecidas en el acta de reunión 001.

Restricciones del proyecto

Las restricciones del proyecto están basadas en los siguientes componentes:

- **Alcance**: Cumplir con el alcance definido para la implementación de Gophish en una entidad financiera.
- **Tiempo**: Cumplir el proyecto en el plazo solicitado por el cliente.
- **Costo**: Cumplir con el presupuesto estimado del proyecto.

3.2.1.3 EDT

En este ítem se presenta de manera detalla el EDT del proyecto de implementación de Gophish en una entidad financiera, donde se visualiza todos los entregables a ser desarrollados durante el proyecto, tal como se puede observar en la Figura13.

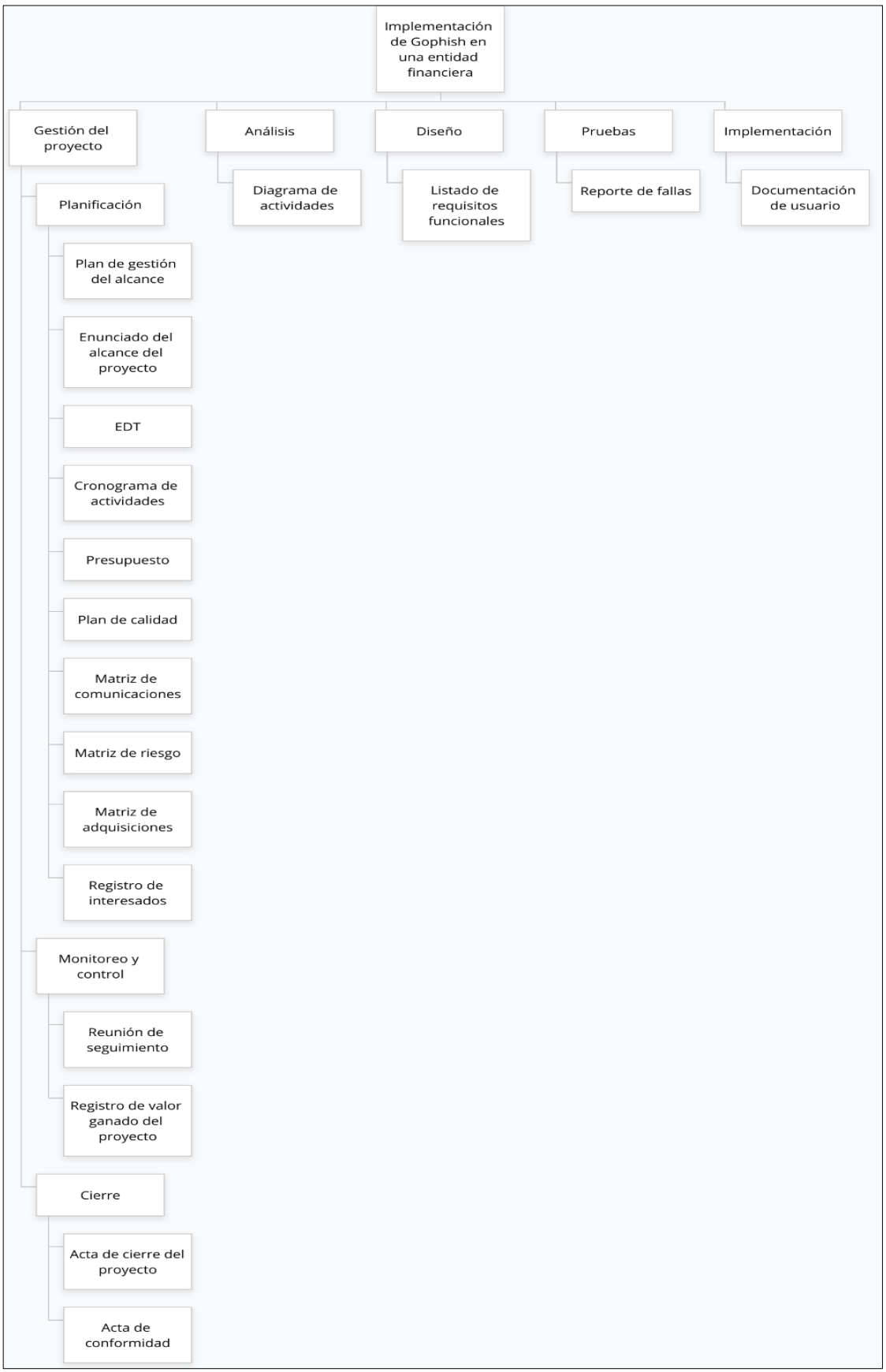


Figura13. EDT.

Fuente: Elaboración propia.

3.2.2 Gestión del tiempo

La presente investigación duró 03 meses desde octubre a diciembre del 2019, por tal motivo a continuación se presenta el cronograma del proyecto con todas las actividades implementación, tal como se puede observar en la Figura14.

N°	Nombre de la tarea	2019											
		Octubre				Noviembre				Diciembre			
		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
1	Gestión del proyecto												
1.1	Planificación												
1.1.1	Elaborar el plan de gestión del alcance	X											
1.1.2	Elaborar el enunciado del alcance del proyecto	X											
1.1.3	Elaborar el EDT	X											
1.1.4	Establecer el cronograma de actividades		X										
1.1.5	Establecer el presupuesto		X										
1.1.6	Elaborar el plan de calidad		X										
1.1.7	Establecer la matriz de comunicaciones			X									
1.1.8	Establecer la matriz de riesgo			X									
1.1.9	Establecer la matriz de adquisiciones			X									
1.1.10	Establecer el registro de interesados				X								
1.2	Ejecución												
1.2.1	Establecer el listado del equipo de trabajo				X								
1.3	Monitoreo y control												
1.3.1	Elaborar el acta de reunión de seguimiento				X								
1.3.2	Establecer el registro de valor ganado del proyecto				X								
1.4	Cierre												
1.4.1	Elaborar el acta de cierre del proyecto												X
1.4.2	Elaborar el acta de conformidad												X
2	Análisis												
2.1	Establecer el diagrama de actividades					X							
3	Diseño												
3.1	Establecer el listado de requisitos funcionales					X							
4	Pruebas												
4.1	Establecer un reporte de fallas						X						
5	Implementación												
5.1	Descargar un sistema operativo linux							X					
5.2	Descargar Gophish y Ngrok							X					
5.3	Instalar una maquina virtual con linux								X				
5.4	Instalar Gophish y Ngrok en la máquina virtual con linux								X				
5.5	Cargar una lista de usuarios con email a Gophish									X			
5.6	Generar el landing mediante clonación de una página web									X			
5.7	Redactar la plantilla de email										X		
5.8	Ejecutar el envío del phishing											X	
5.9	Preparar la documentación de usuario											X	

Figura14. Cronograma del proyecto.

Fuente: Elaboración propia.

3.2.3 Gestión de la calidad

3.2.3.1 Plan de calidad

En cuanto al plan de calidad para el proyecto de implementación de Gophish en una entidad financiera, se considera la descripción del plan de calidad, aseguramiento de la calidad y control de la calidad según se detalla a continuación.

Descripción del plan de calidad

El plan de calidad especifica que procesos, procedimientos y recursos deben aplicarse en la implementación del presente proyecto, quien debe aplicarlo y cuando debe aplicarse para cumplir con los requisitos del alcance, tiempo y costo. Por ello, el plan aborda todas las fases del proyecto relativos a los entregables para cumplir con las expectativas de los interesados.

Aseguramiento de la calidad

En esta etapa se tienen un conjunto de actividades importantes para garantizar el cumplimiento con el acta de reunión 001, según se puede apreciar en la Figura15 el detalle del aseguramiento de la calidad:

- **Fecha de inicio y fin:** Es el hito más importante para identificar el inicio y fin del proyecto.
- **Hitos:** Son puntos importantes como los entregables, que se revisan a lo largo de proyecto.
- **Fases del proyecto:** Se presenta a modo lineal para identificar visualmente el aseguramiento y control de calidad del proyecto.
- **Aseguramiento de la calidad:** Se realiza de forma incremental para las actividades importantes según las 05 fases definidos para el proyecto.

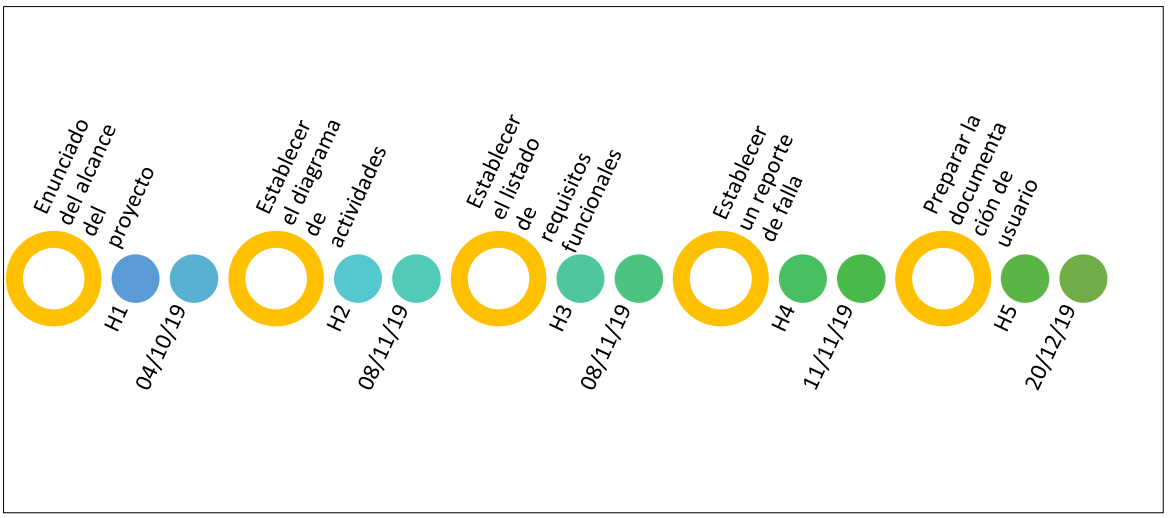


Figura15. Aseguramiento de la calidad para las actividades del proyecto.

Fuente: Elaboración propia.

Control de la calidad

A continuación, en la Tabla2, se detalla las estrategias para el control de calidad de las actividades importantes según las 05 fases definidos en el proyecto para cumplir con los requisitos de alcance, tiempo y costo.

Tabla2. Control de la calidad para las actividades del proyecto.

Fases	Objetivo	Actividades	Pruebas	Criterios de aceptación	Frecuencia	Medios de aceptación	Responsable
Gestión de proyecto	Asegurar el cumplimiento del control de calidad	Enunciado del alcance del proyecto	Evaluar el avance del proyecto según lo establecido en el acta de reunión 001	Elaborado al 100%	Según los hitos establecidos	Informe de avance del proyecto	Project Manager
Análisis	Asegurar el cumplimiento del control de calidad	Establecer el diagrama de actividades	Evaluar el avance del proyecto según lo establecido en el acta de reunión 001	Elaborado al 100%	Según los hitos establecidos	Informe de avance del proyecto	Project Manager
Diseño	Asegurar el cumplimiento del control de calidad	Establecer el listado de requisitos funcionales	Evaluar el avance del proyecto según lo establecido en el acta de reunión 001	Elaborado al 100%	Según los hitos establecidos	Informe de avance del proyecto	Project Manager
Pruebas	Asegurar el cumplimiento del control de calidad	Establecer un reporte de falla	Evaluar el avance del proyecto según lo establecido en el acta de reunión 001	Elaborado al 100%	Según los hitos establecidos	Informe de avance del proyecto	Project Manager
Implementa	Asegurar el cumplimiento del control de calidad	Preparar la documentación de usuario	Evaluar el avance del proyecto según lo establecido en el acta de reunión 001	Elaborado al 100%	Según los hitos establecidos	Informe de avance del proyecto	Project Manager

Fuente: Elaboración propia.

3.2.4 Gestión de las comunicaciones

Para el desarrollo del proyecto se tiene definido una comunicación formal al interno del proyecto y de forma vertical para satisfacer las necesidades de todos los interesados. Es así como a continuación se presenta la Tabla3 donde se aprecia la matriz de comunicaciones del proyecto de implementación.

Tabla3. Matriz de comunicaciones del proyecto.

Tipo de comunicación	Objetivo de la comunicación	Método	Periodo	Responsable	Audiencia
Reunión inicial	Determinar el alcance, tiempo y costo del proyecto. Conocer al equipo encargado del proyecto. Definir el compromiso de todos los participantes del proyecto.	Reunión y presentación. Acta de reunión con acuerdos.	Al inicio del proyecto	Project Manager	Gerente de Seguridad e Inspectoría. Jefe de seguridad de la información.
Reunión de seguimiento	Revisar que se cumpla el alcance, tiempo y costo definidos para el proyecto. Conocer las limitaciones, fallas o cambios para mejora del proyecto.	Reunión y exposición. Acta de reunión con acuerdos.	A la mitad del proyecto	Project Manager	Gerente de Seguridad e Inspectoría. Jefe de seguridad de la información.
Reunión de cierre	Entregar la documentación del proyecto. Conocer los resultados proyectados vs. los reales.	Reunión y presentación. Acta de reunión con acuerdos.	Al finalizar el proyecto	Project Manager	Gerente de Seguridad e Inspectoría. Jefe de seguridad de la información.

Fuente: Elaboración propia.

3.2.5 Gestión del riesgo

Para el presente proyecto se realiza la gestión del riesgo que cubre la identificación, análisis, estrategia de respuesta y monitoreo de los riesgos identificados. A continuación, en la Figura16 se presenta la categorización de los riesgos según los ejes de probabilidad e impacto y los valores de estimación que varían entre muy baja a muy alta.

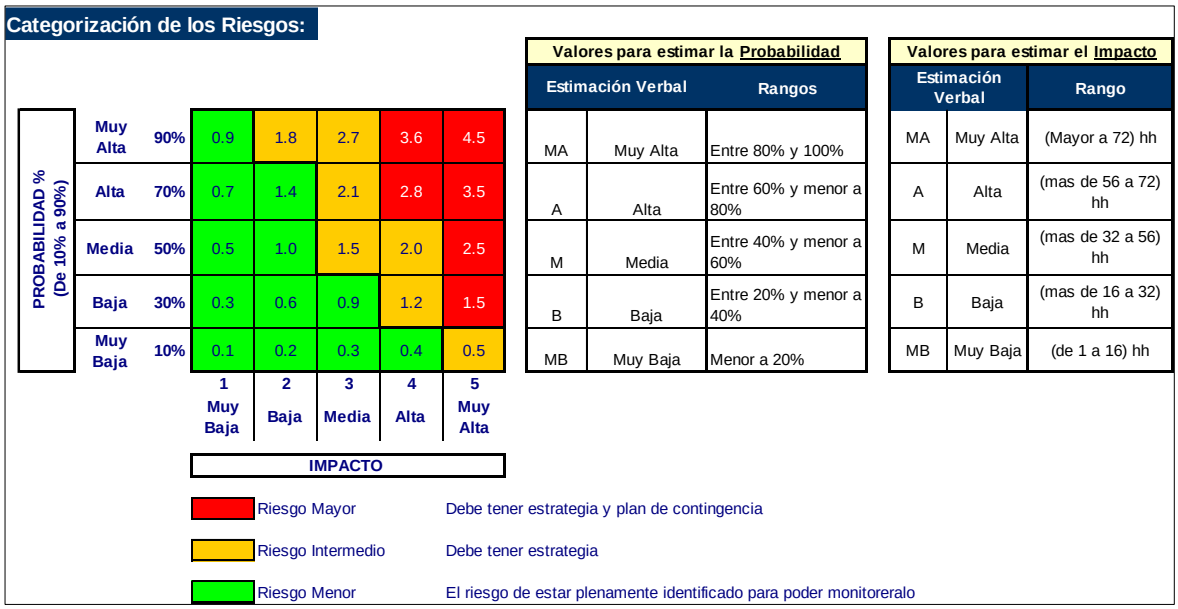


Figura16. Categorización de los riesgos.

Fuente: Elaboración propia.

Para el presente proyecto se identifican 04 riesgos, de los cuales 01 de ellos según el análisis realizado es un riesgo mayor, el cual tiene como código PE 01-GO-R001. Al respecto se debe indicar que de los otros 03 riesgos al tener un umbral menor se tiene como estrategia aceptar el riesgo, según se puede apreciar en la Figura17.

Identificación			Análisis			
Cód. Riesgo	Fecha de registro	Descripción del Riesgo	Prob. %	Impacto (HH)	Impacto (1 al 5)	Exp al Riesgo
PE01-GO - R001	18/10/19	Indisponibilidad del personal técnico asignado al proyecto	70%-Alta	768	5 Muy alta	537.60
PE01-GO - R002	18/10/19	Retrasos en el proyecto por modificación del alcance, tiempo o costo	30% Baja	24	2 Baja	7.20
PE01-GO - R003	18/10/19	Indisponibilidad de los responsables en las reuniones de seguimiento del proyecto	50% Media	12	1 Muy Baja	6.00
PE01-GO - R004	18/10/19	Restructuración del área que lidera o respalda el proyecto	30% Baja	24	2 Baja	7.20

Figura17. Identificación y análisis del riesgo.

Fuente: Elaboración propia.

A continuación, se muestra la estrategia de respuesta y monitoreo de los 04 riesgos identificados, con la finalidad de que, con un adecuado tratamiento, el riesgo residual sea menor y aceptado por el negocio, tal como se aprecia en la Figura18.

Estrategia de respuesta			Monitoreo		
Descripción	Responsable	Acciones realizadas	% de avance	Estado	Fecha de revisión
Mitigar - Capacitar a un personal alterno como contingencia del principal en caso de indisponibilidad del tipo enfermedad, vacaciones o renuncia	Cliente - Analista de Seguridad de la Información	Capacitar a un personal alterno	100.00%	Desaparecio	18/10/19
Aceptar - Pasivamente - Realizar seguimiento al riesgo identificado para que no exceda el umbral	Cliente - Analista de Seguridad de la Información	Realizar seguimiento al riesgo identificado	100.00%	Desaparecio	18/10/19
Aceptar - Pasivamente - Realizar seguimiento al riesgo identificado para que no exceda el umbral	Cliente - Analista de Seguridad de la Información	Realizar seguimiento al riesgo identificado	100.00%	Desaparecio	18/10/19
Aceptar - Pasivamente - Realizar seguimiento al riesgo	Cliente - Analista de Seguridad de la Información	Realizar seguimiento al riesgo	100.00%	Desaparecio	18/10/19

Figura18. Estrategia de respuesta y monitoreo del riesgo.

Fuente: Elaboración propia.

3.2.6 Gestión de adquisiciones

Para el desarrollo del proyecto, se necesita la adquisición de 05 recursos para el total de tiempo que dura el proyecto que es de 03 meses, todos fueron gestionadas mediante orden de compra directa, tal como se aprecia en la matriz de adquisiciones de la Figura19.

Matriz de Adquisiciones						
Proyecto:	Implementación de Gophish en una entidad financiera					
ID:	IGEF-2019					
ID	**Recursos**	**Tipo de Adquisición**	**Modalidad de Adquisición**	**Fechas Estimadas**		**Presupuesto Estimado**
				Inicio	**Fin**	
1	Laptop	Orden de compra	Directa	14/10/2019	18/10/2019	S/ 4,500.00
2	Licencia Windows	Orden de compra	Directa	14/10/2019	18/10/2019	S/ 620.00
3	Modem internet	Orden de compra	Directa	14/10/2019	18/10/2019	S/ 540.00
4	Papel bond	Orden de compra	Directa	14/10/2019	18/10/2019	S/ 20.00
5	Lapiceros	Orden de compra	Directa	14/10/2019	18/10/2019	S/ 10.00
					Total	**S/ 5,690.00**

Figura19. Matriz de adquisiciones.

Fuente: Elaboración propia.

3.2.7 Gestión de interesados

Con relación al desarrollo del proyecto, se tiene definido los interesados que pueden afectar o ser afectados por el proyecto, tal como se aprecia en la matriz de interesados de la Figura20.

ID	Nombre	Posición organizacional	Rol en el proyecto	Nivel de interés	Nivel de poder
1	Jou Jancachagua	Analista de seguridad de la información	Proyect Manager	Alto	Bajo
2	Wilfredo Malla	Jefe de seguridad de la información	Supervisor	Alto	Bajo
3	Cesar Lavalle	Gerente de seguridad e inspectoría	Sponsor	Alto	Alto

Figura20. Matriz de interesados.

Fuente: Elaboración propia.

A continuación, en la Figura21 se presenta la matriz de poder e interés donde se identifica el nivel de involucramiento de los interesados en el proyecto, donde la mayoría se ubica en el cuadrante de “mantenerse informado”.

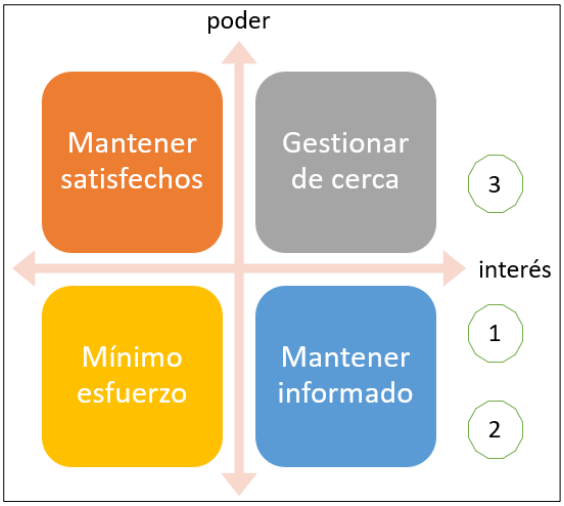


Figura21. Matriz de poder e interés.

Fuente: Elaboración propia.

3.2.8 Gestión de la integración del proyecto

3.2.8.1 Acta de cierre del proyecto

En cuanto al acta de cierre del proyecto de implementación de Gophish en una entidad financiera, se considera el cronograma simplificado, lecciones aprendidas, productos generados, beneficios alcanzados, cierre de adquisiciones, documentación generada en el proyecto y las respectivas firmas tal como se detallan a continuación.

Cronograma simplificado

En relación con la fecha de inicio programada y la fecha de inicio real del proyecto, no hubo variaciones al respecto, esta se mantuvo y se dio inicio el 01/10/19, así mismo respecto a la fecha fin programada y la fecha fin real fue el mismo día 27/12/19, tal como se puede apreciar en la Tabla4.

Tabla4. Cronograma simplificado.

Cronograma			
Fecha inicio programada	01/10/19	**Fecha fin programada**	27/12/19
Fecha inicio real	01/10/19	**Fecha fin real**	27/12/19

Fuente: Elaboración propia.

Lecciones aprendidas

- Con relación al envío del phishing utilizando un framework opensource como Gophish y canalizándose a través de Gmail, se tiene que realizar una configuración adicional en Gmail para habilitar el acceso para aplicaciones menos seguras.

- Por otra parte, para el envío del phishing se pudo identificar que Gmail bloquea los correos salientes cuando se envía consecutivamente sin tener un lapso de espera, ya que lo detecta como phishing.

- En cuanto al landing page, se tiene que realizar una configuración adicional para capturar las contraseñas introducidas por los usuarios y llegue automáticamente al dashboard de Gophish.

Productos generados

Al cierre se generaron todos los productos establecidos en el enunciado del alcance del proyecto, que fueron cubiertos al 100% de implementación, obteniendo los siguientes módulos totalmente operativos: Dashboard, Campañas, Grupos y usuarios, Plantilla de correo, Landing page, Perfil de envío y Configuración.

Beneficios alcanzados

Se pudo determinar que el beneficio alcanzado cumple con lo establecido en el enunciado del alcance del proyecto, el cual fue de mejorar la seguridad de la información ante ciberataques del tipo phishing en un 54.83% para una entidad financiera.

Cierre de adquisiciones

Al cierre del proyecto se verifica que el monto presupuestado conforme a lo establecido en la gestión de adquisiciones es idéntico al monto ejecutado en S/ 5,690.00, donde todas las adquisiciones se concretaron y se encuentran cerradas, tal como se muestra en la Tabla5.

Tabla5. Cierre de adquisiciones.

Cierre de adquisiciones					
Adquisiciones programadas	**Cantidad**	**Presupuesto**	**¿Se realizó la adquisición?**	**Monto devengado**	**¿Se encuentra cerrada la adquisición?**
Laptop	1	S/ 4,500.00	Si	S/ 4,500.00	Si
Licencia Windows	1	S/ 620.00	Si	S/ 620.00	Si
Modem internet	3	S/ 540.00	Si	S/ 540.00	Si
Papel bond	1	S/ 20.00	Si	S/ 20.00	Si
Lapiceros	1	S/ 10.00	Si	S/ 10.00	Si
	Presupuesto total	**S/ 5,690.00**	**Ejecutado total**	**S/ 5,690.00**	

Fuente: Elaboración propia.

Documentación generada en el proyecto

A continuación, se presenta toda la documentación generada a lo largo del proyecto de implementación, el cual consta de 18 documentos en formato digital tal como se presenta en la Tabla6.

Tabla6. Documentación generada en el proyecto.

Documentación generada en el proyecto		
Documento	**Ubicación**	
	Física	**Digital**
Plan de gestión del alcance		X
Enunciado del alcance del proyecto		X
EDT		X
Cronograma de actividades		X
Presupuesto		X
Plan de calidad		X
Matriz de comunicaciones		X
Matriz de riesgo		X
Matriz de adquisiciones		X
Registro de interesados		X
Reunión de seguimiento		X
Registro de valor ganado del proyecto		X
Acta de cierre del proyecto		X
Acta de conformidad		X
Diagrama de actividades		X

Listado de requisitos funcionales		X
Reporte de fallas		X
Documentación de usuario		X

Fuente: Elaboración propia.

Firmas

El cierre del proyecto obtuvo el visto bueno de cada autoridad inmediata superior que participó en la implementación, tal como se muestra en la Tabla7.

Tabla7. Firmas de cierre del proyecto.

Firmas				
Nombre	**Cargo o rol en el proyecto**	**Elaborado / Revisado / Aprobado**	**Fecha**	**Firma**
Jou Jancachagua	Proyect Manager	Elaborado	27/12/19	
Wilfredo Malla	Supervisor	Revisado	27/12/19	
César Lavalle	Sponsor	Aprobado	27/12/19	

Fuente: Elaboración propia.

3.2.8.2 Acta de conformidad

De la conformidad

Por medio de la presente acta se deja constancia de la finalización y aceptación del proyecto de “Implementación de Gophish en una entidad financiera” a cargo de Jou Jancachagua Vera – Project Manager, el cual fue iniciado el 01 de Octubre del 2019 y culminando el 27 de Diciembre del 2019.

Del cierre del proyecto

Se da por concluido el proyecto, por lo que habiendo constatado el Sponsor la finalización, entrega y aceptación, se certifica el cierre del proyecto, el cual culmina de manera exitosa.

El proyecto comprende la entrega de los siguientes entregables:

- **Gestión del proyecto – Planificación**

- Plan de gestión del alcance
- Enunciado del alcance del proyecto
- EDT
- Cronograma de actividades
- Presupuesto
- Plan de calidad
- Matriz de comunicaciones
- Matriz de riesgo
- Matriz de adquisiciones
- Registro de interesados

- **Gestión del proyecto – Monitoreo y control**

- Reunión de seguimiento
- Registro de valor ganado del proyecto

- **Gestión del proyecto – Cierre**

- Acta de cierre del proyecto
- Acta de conformidad

- **Análisis**

- Diagrama de actividades

- **Diseño**

- Listado de requisitos funcionales

- **Pruebas**

- Reporte de fallas

- **Implementación**

- Documentación de usuario

Aprobación y aceptación del requerimiento

Para el cierre del proyecto firman las partes como señal de conformidad, tal como se observa en la Tabla8.

Tabla8. Firmas de acta de conformidad del proyecto.

JEFE DE PROYECTO	SOLICITANTE DEL REQUERIMIENTO
UNIDAD DE SEGURIDAD DE LA INFORMACIÓN **Firma:** **Nombre:** Jou Jancachagua **Cargo:** Analista de Seguridad de la Información	**UNIDAD DE SEGURIDAD DE LA INFORMACIÓN** **Firma:** **Nombre:** César Lavalle **Cargo:** Gerente de Seguridad e Inspectoría

Fuente: Elaboración propia.

3.3 Desarrollo del proyecto

El presente ítem cubre la implementación de la plataforma Gophish y abarca todas las fases para el envío de un phishing exitoso, usando todos los módulos que brinda la herramienta, el cual este punto servirá como documentación del usuario.

3.3.1 Descargar un sistema operativo Linux

Para la implementación de Gophish es necesario la descarga de un sistema operativo del tipo Linux. En el presente estudio se usa Ubuntu 16.04 LTS el cual puede ser descargado de la página oficial según se visualiza en la Figura22 o también la última versión Ubuntu 20.04.2.0 LTS tal como se aprecia en la Figura23, sin embargo, el investigador realizó

pruebas previas con la versión 16.04 que es más estable, por lo que se usará a lo largo del proyecto.

Conviene subrayar que una vez descargados los programas estos se almacenan en la carpeta “Descargas” de Windows.

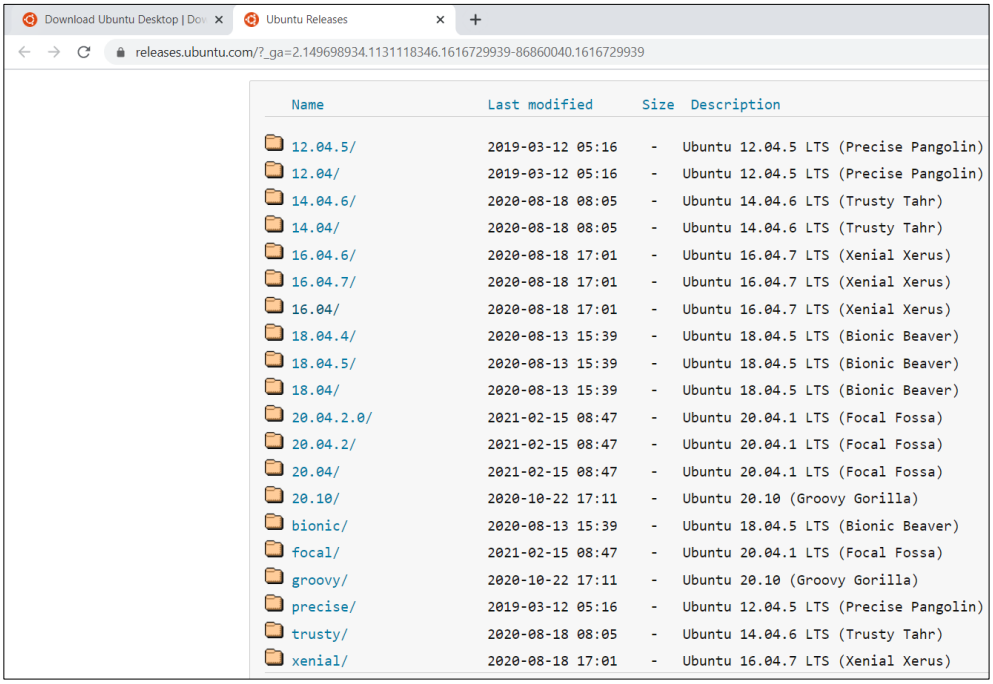


Figura22. Descarga de Ubuntu 16.04 LTS.

Nota: Recuperado de These releases of Ubuntu are available [Imagen], por Ubuntu, 2021. Recuperado de https://releases.ubuntu.com/?_ga=2.149698934.1131118346.1616729939-86860040.1616729939

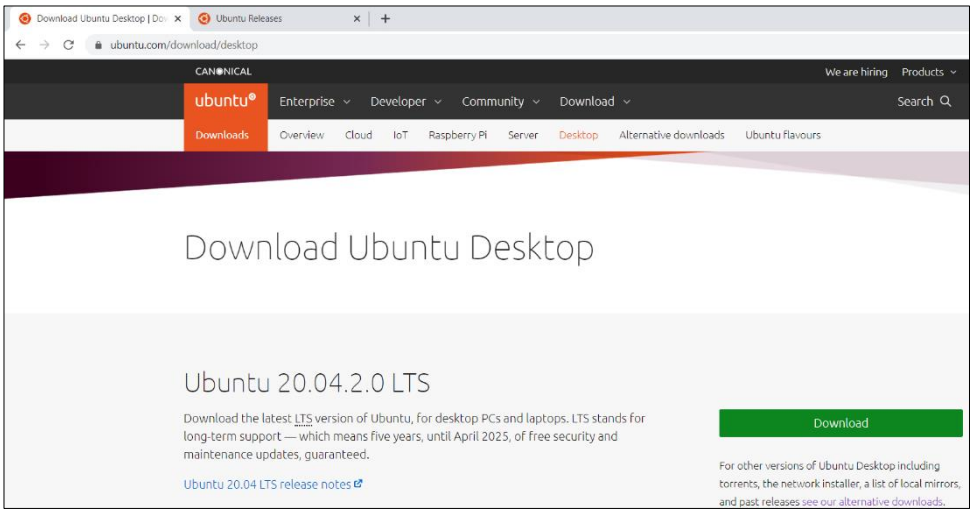


Figura23. Descarga de Ubuntu 20.04.2.0 LTS.

Nota: Recuperado de Download Ubuntu Desktop [Imagen], por Ubuntu, 2021. Recuperado de https://ubuntu.com/download/desktop

3.3.2 Descargar Gophish y Ngrok

La descarga de Gophish se realiza de la página oficial, la versión a usar es en la distribución Linux, en la versión 0.11.0 de 64bits, tal como se aprecia en la Figura24.

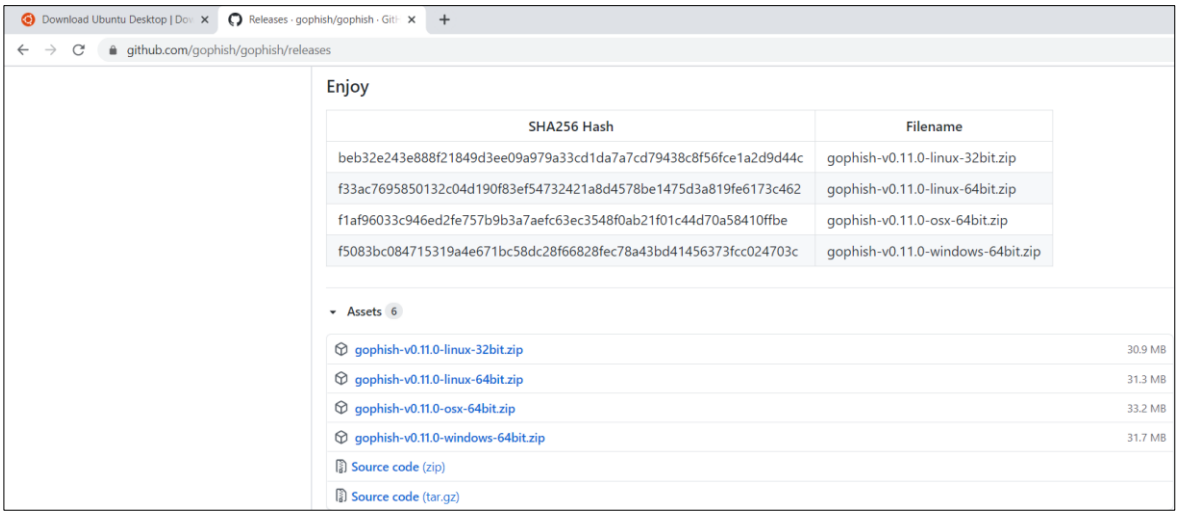


Figura24. Descarga de Gophish 0.11.0 para Linux.

Nota: Recuperado de Gophish v0.11.0 [Imagen], por GitHub, 2020. Recuperado de https://github.com/gophish/gophish/releases

La descarga de ngrok se realiza de la página oficial, la versión a usar es en la distribución Linux de 64bits, según se puede apreciar en la Figura25.

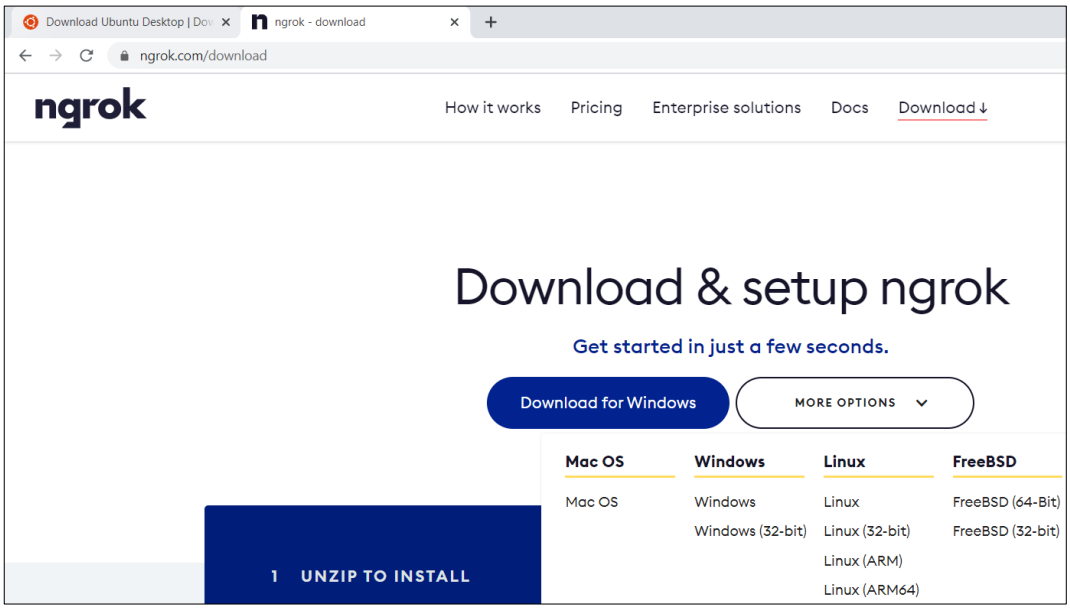


Figura25. Descarga de ngrok para Linux.

Nota: Recuperado de Download & setup ngrok [Imagen], por ngrok, 2021. Recuperado de https://ngrok.com/download

3.3.3 Instalar una máquina virtual con linux

Mediante VMware Workstation 12 Pro se crea una máquina virtual bajo Linux y se escoge de forma recomendada la forma típica, según se puede observar en la Figura26.

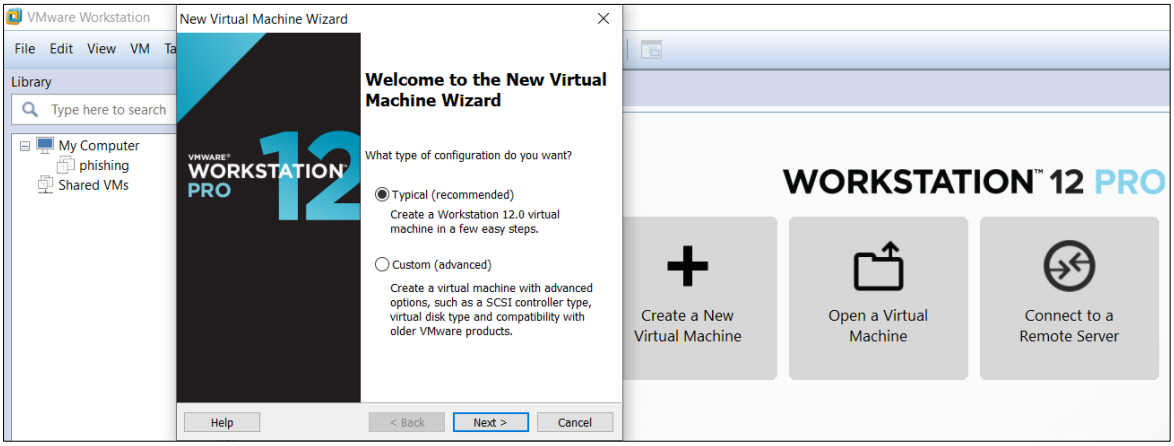


Figura26. Creación de una máquina virtual.

Fuente: Elaboración propia.

Continuando con el proceso de instalación se escoge la imagen descargada de Ubuntu y se procede con el siguiente paso, según se puede observar en la Figura27.

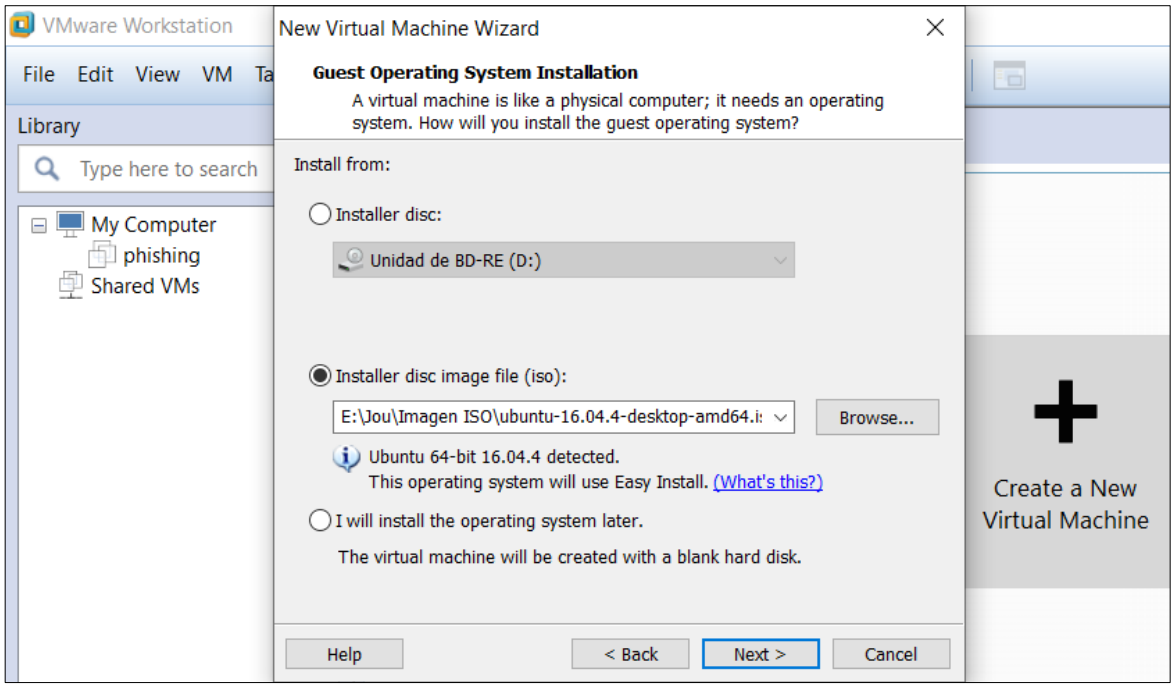


Figura27. Selección del sistema operativo Ubuntu descargado.

Fuente: Elaboración propia.

Por otra parte, se solicita personalizar la máquina virtual con nombre y contraseña, tal como se aprecia en la Figura28.

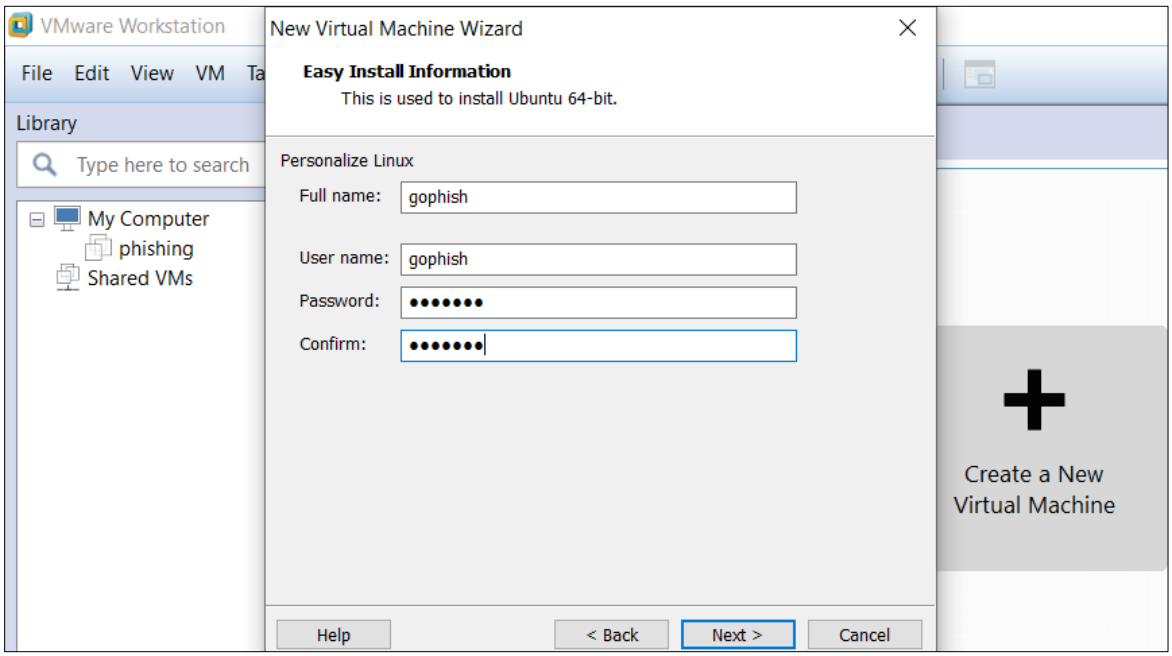


Figura28. Personalización de la máquina virtual.

Fuente: Elaboración propia.

Finalmente, se configura la máquina virtual con un disco de 20GB de capacidad, según se puede visualizar en la Figura29 y después de un par de minutos, el sistema se instala automáticamente tal como se aprecia en la Figura30.

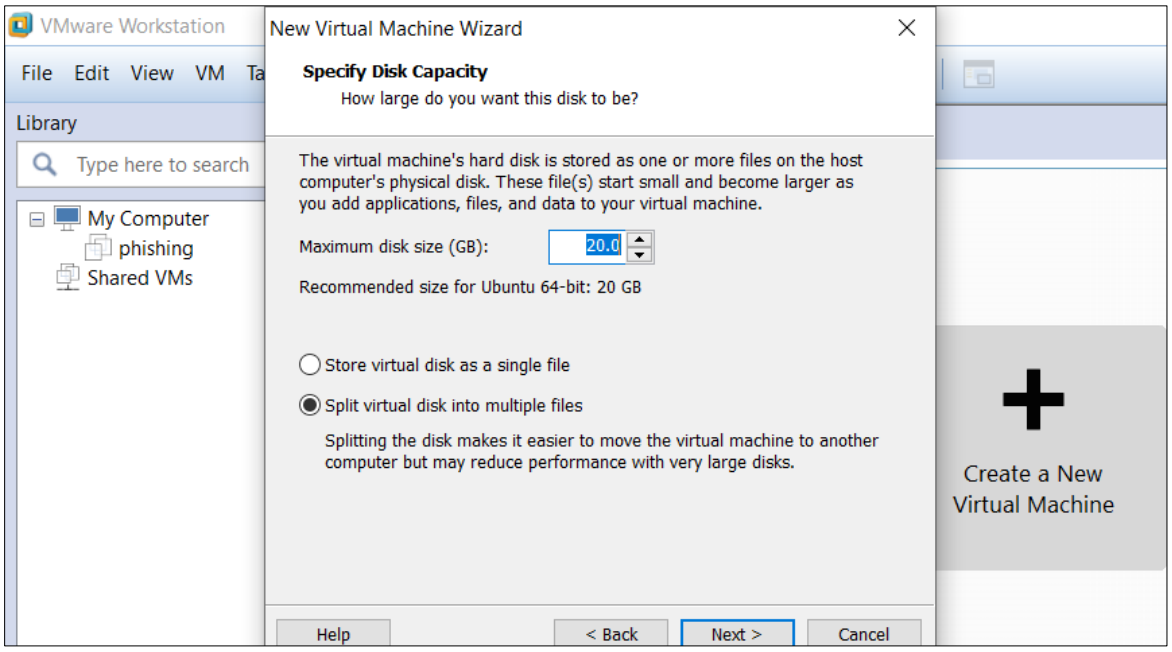


Figura29. Especificación de capacidad del disco de la máquina virtual.

Fuente: Elaboración propia.

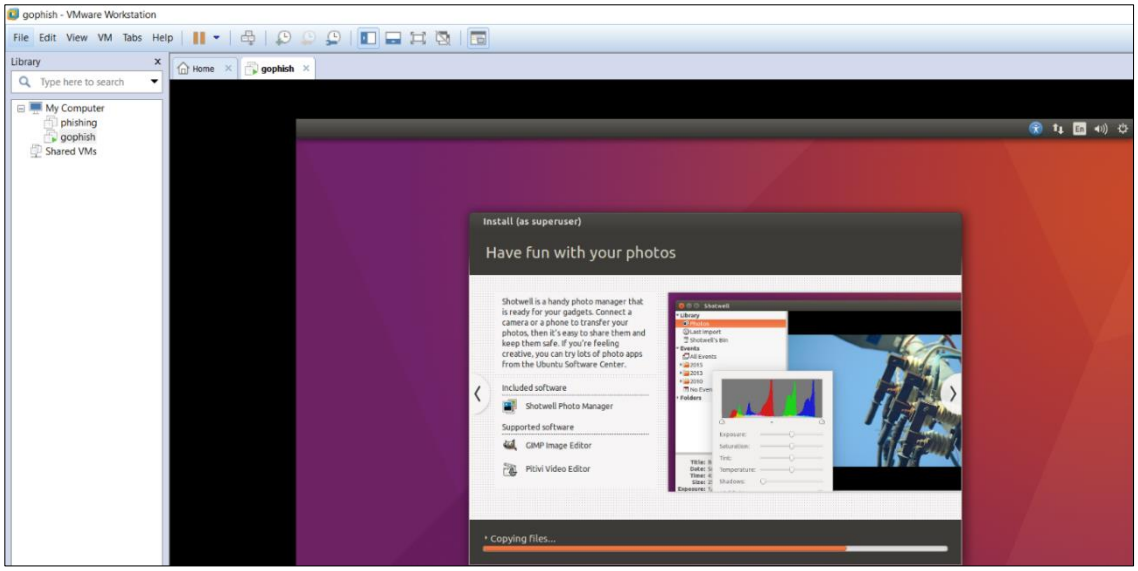


Figura30. Instalación de Ubuntu en la máquina virtual.

Fuente: Elaboración propia.

3.3.4 Instalar Gophish y Ngrok en la máquina virtual con linux

Ciertamente como un paso previo y de forma adicional se configura la máquina virtual para que permita compartir archivos entre el host anfitrión y Ubuntu, tales como los programas descargados inicialmente, según se puede apreciar en la Figura31.

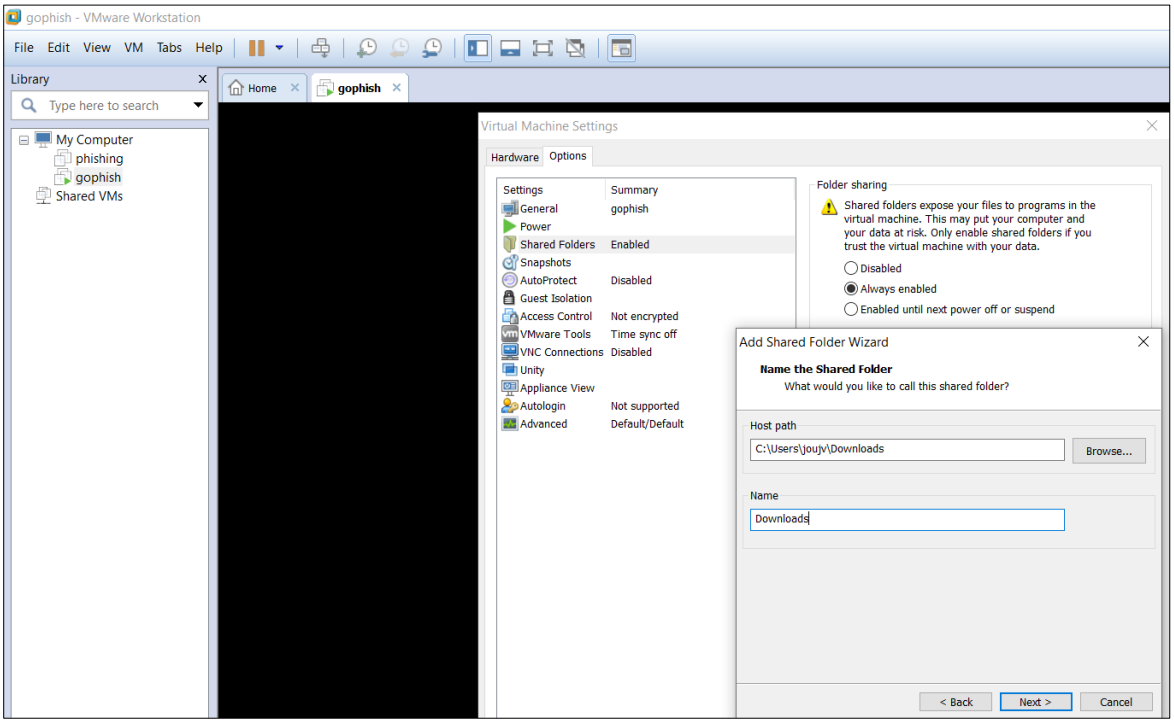


Figura31. Creación de carpeta compartida entre el host anfitrión y Ubuntu.

Fuente: Elaboración propia.

La carpeta compartida con los programas descargados se ubica en la siguiente ruta de Ubuntu /mnt/hgfs/Downloads que luego puede ser copiado al escritorio, tal como se aprecia en la Figura32.

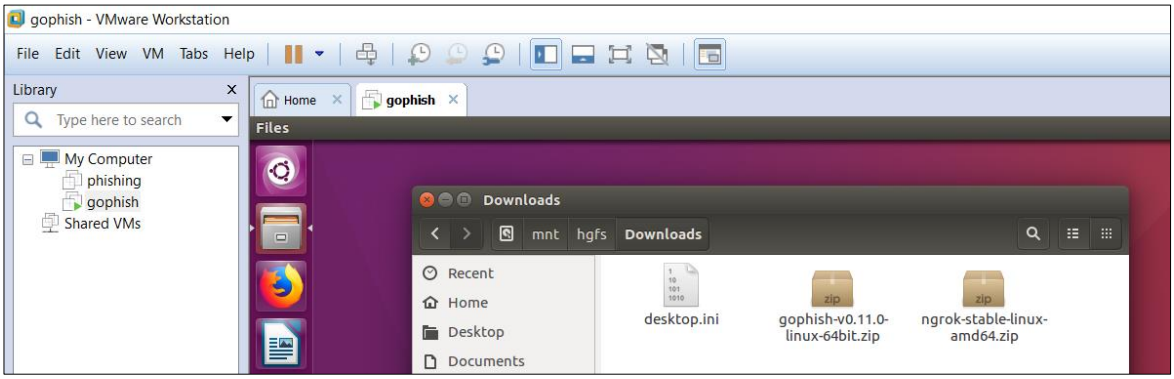


Figura32. Ubicación de la carpeta compartida en Ubuntu.

Fuente: Elaboración propia.

Se usa el comando cd para situarse en el escritorio de Ubuntu, luego el comando mkdir para crear una carpeta denominada phish y ngrok, posterior se usa el comando mv para mover el programa del escritorio a la carpeta creada. Luego se descomprime el .zip con el comando unzip, tal como se aprecia en la Figura33.

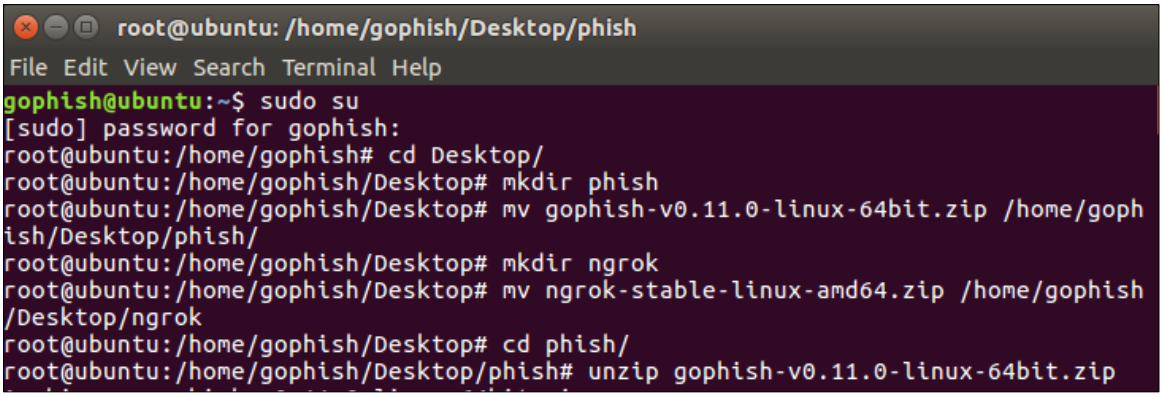


Figura33. Pasos previos para instalar Gophish.

Fuente: Elaboración propia.

Finalmente, se le da permisos con el comando chmod y se instala gophish con un comando adicional, tal como se aprecia en la Figura34.

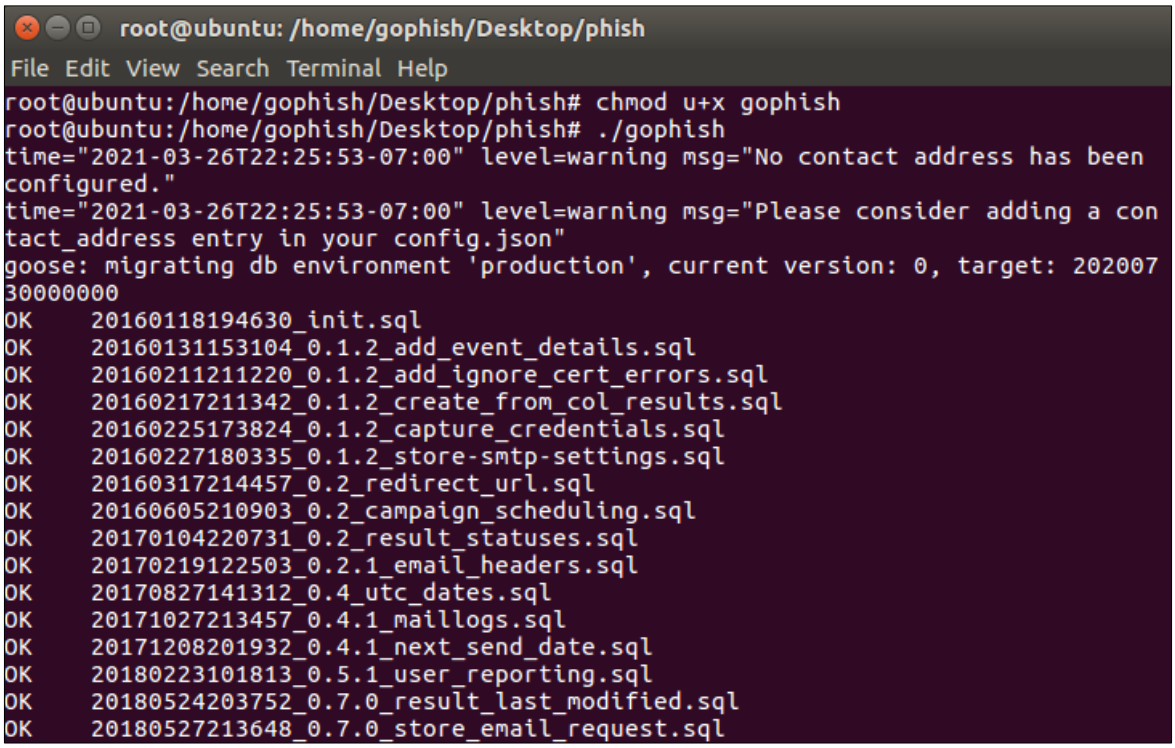


Figura34. Pasos finales para instalar Gophish.

Fuente: Elaboración propia.

En los logs se ubica el usuario y contraseña de inicio de sesión a Gophish así como la URL y puerto donde se encuentra escuchando el servicio, tal como se aprecia en la Figura35.

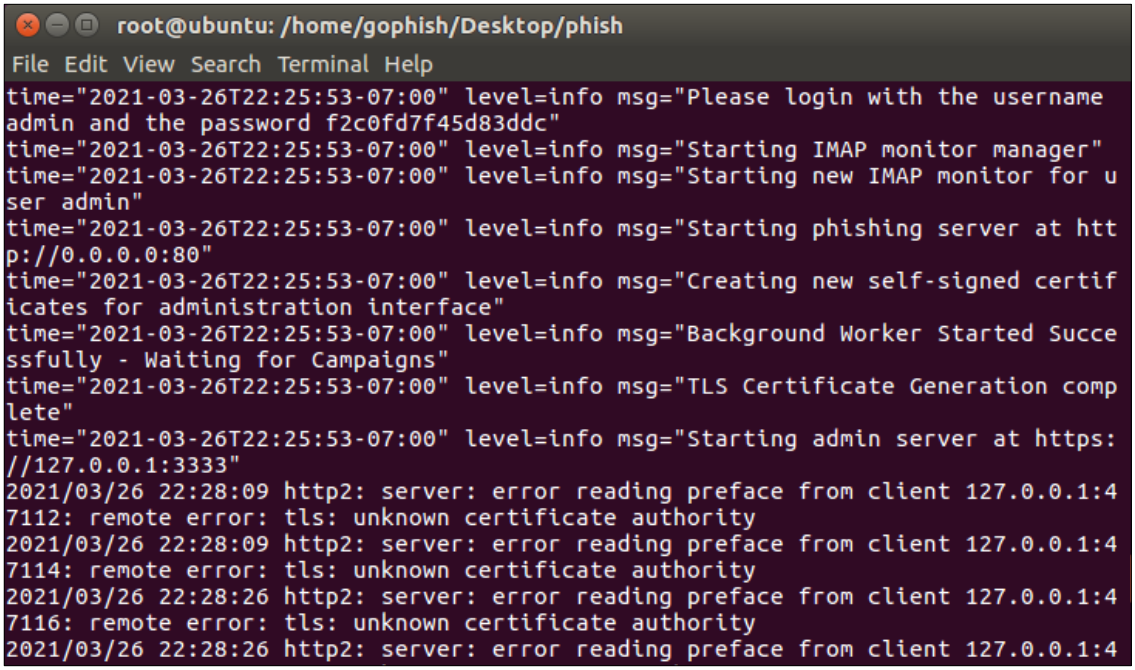


Figura35. Logs de gophish donde se ubica las credenciales y URL.

Fuente: Elaboración propia.

Se ingresa a la URL y cargará una página web tal como se aprecia en la Figura36, así mismo se coloca las credenciales de inicio de sesión y el sistema pedirá cambio de contraseña tal como se muestra en la Figura37.

Figura36. Página de inicio de sesión de Gophish.

Fuente: Elaboración propia.

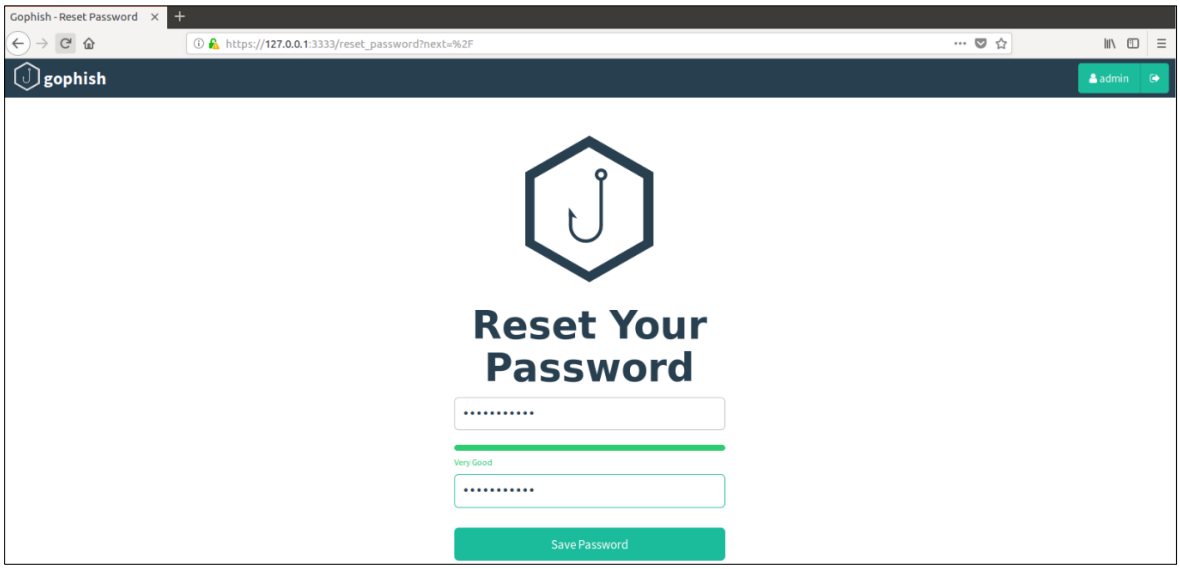


Figura37. Cambio obligatorio de contraseña.

Fuente: Elaboración propia.

Para la instalación de ngrok se usa el comando ls y cd para posicionarnos en la carpeta creada y luego se usa el comando unzip para descomprimir el archivo, tal como se aprecia en la Figura38.

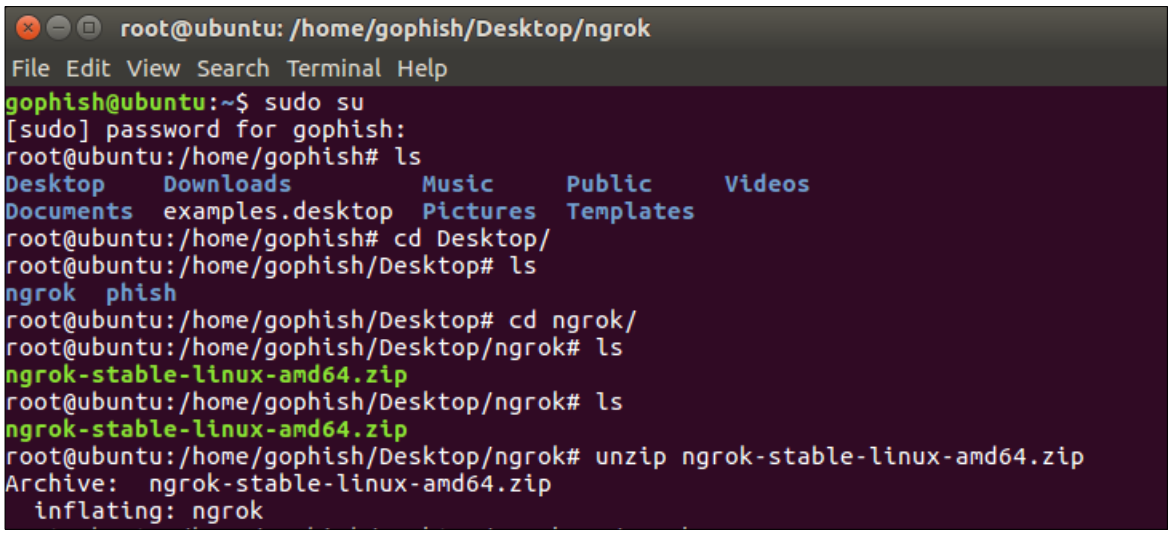


Figura38. Pasos para instalar ngrok.

Fuente: Elaboración propia.

Finalmente se usa el siguiente comando para publicar la URL y crear un túnel desde internet hacia el servidor local y se pueda acceder desde fuera, tal como se aprecia en la Figura39.

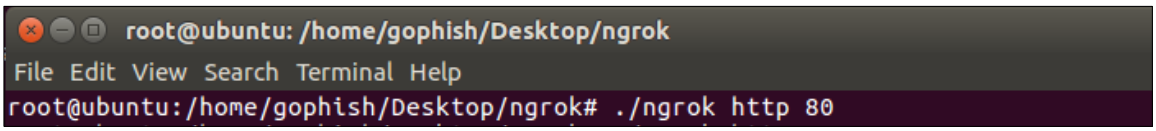


Figura39. Comando para publicar la URL en internet.

Fuente: Elaboración propia.

A continuación, se muestra la URL que será usada en la campaña de phishing y que será accesible desde internet, tal como se aprecia en la Figura40.

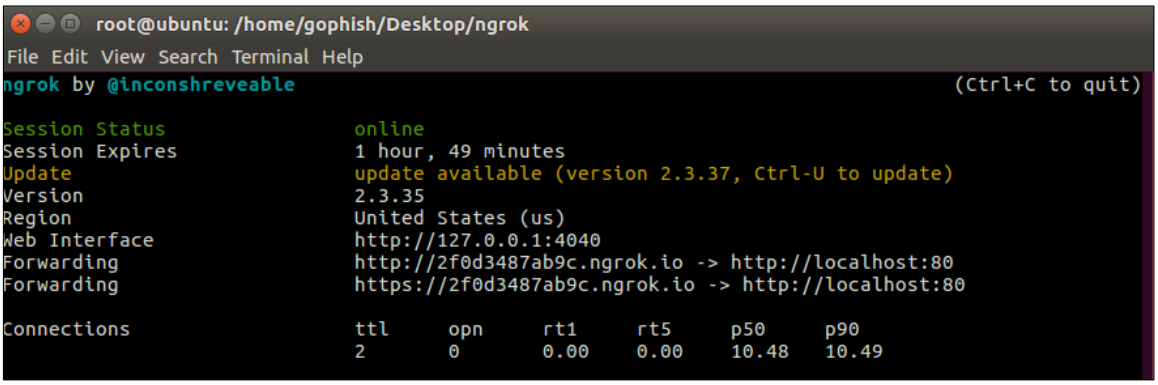


Figura40. Conexión abierta mediante una URL publicada en internet.

Fuente: Elaboración propia.

3.3.5 Cargar una lista de usuarios con email a Gophish

A continuación, una vez logueado en la plataforma, nos ubicamos en la pestaña de Users & Group y se procede a crear un nuevo grupo y se agregan los usuarios manualmente o por bloque en formato .csv tal como se aprecia en la Figura41, que serán usados posteriormente al crear una campaña de phishing,

Tal como se aprecia en la Figura42 se adjunta una muestra de los usuarios a ser cargados a la plataforma, sin embargo, se recorta la imagen en el campo de correo por un tema de privacidad y confidencialidad de la información.

Finalmente se cargan los 450 usuarios a la plataforma tal como se aprecia la Figura43 para continuar con el proceso del envío del phishing.

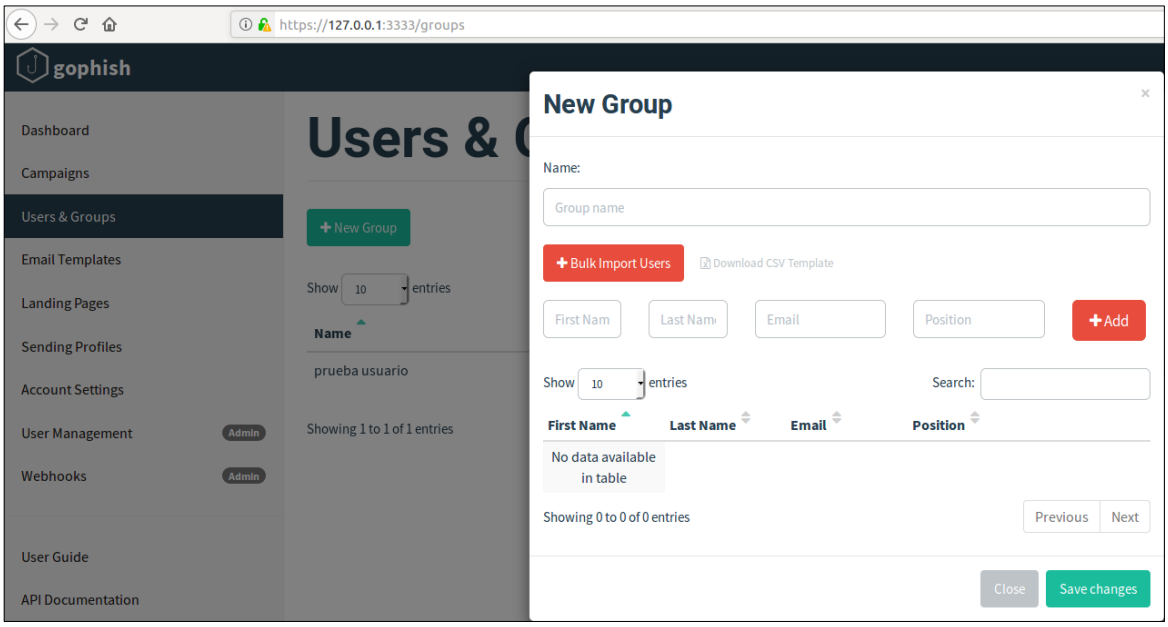


Figura41. Creación de grupos y usuarios en Gophish.

Fuente: Elaboración propia.

	A	B	C
1	dmontoya	Diana Vanessa Montoya Briceño	Funcionario de Negocio IV
2	jalejo	Jimmy Guido Alejo Mamani	Funcionario de Negocios I
3	spascaja	Sonia Ayde Pascaja Llallacachi	Funcionario de Negocios I
4	ttoctom	Tania Margaret Tocto Morocho	Funcionario de Negocios I
5	jcalderony	Juan Carlos Calderon Yamunaque	Funcionario de Negocios II
6	jtoro	Jose Roifer Toro Alejandria	Funcionario de Negocios III
7	jpachecoc	Juan Francisco Pacheco Crisostomo	Funcionario de Negocios II
8	lauqui	Lisbeth Auqui Gomez	Funcionario de Negocios Empresa
9	jromeroh	Jorge Joel Romero Herrera	Funcionario de Negocios II
10	cdurand	Carlos Eduardo Durand Marcelo	Funcionario de Negocios III
11	jcastilloc	Julio Humberto Castillo Chavez	Funcionario de Negocios II
12	mmore	Miguel Angel More Anton	Funcionario de Negocios II
13	mmoreno	Mario Luis Moreno Ramos	Funcionario de Negocios II
14	gsilva	Gustavo Adolfo Silva Zavaleta	Funcionario de Negocios I
15	cnima	Cristhiam Manuel Nima Ramirez	Funcionario de Negocios I
16	gcardozo	Gloria Judith Cardozo Zumaeta	Funcionario de Negocios III
17	hmolocho	Henry Smith Molocho Quiroz	Funcionario de Negocios II
18	caedo	Cristian Raul Aedo Nonajulca	Funcionario de Negocios I
19	jcarlin	Jorge Fernando Carlin Navarro	Funcionario de Negocios II
20	cccama	Cyntia Chanel CCama Tacca	Funcionario de Negocios III
21	cticona	Clemencia Ticona Zuñiga	Funcionario de Negocios I
22	zhuaraca	Zoraida Iris Huaraca Alfonso	Funcionario de Negocios II
23	gferrer	Gladis Monica Ferrer Melgarejo	Funcionario de Negocios Empresa
24	mjimenez	Magali Jimenez Saavedra	Funcionario de Negocios I

Figura42. Lista de usuarios a ser cargados a Gophish.

Fuente: Elaboración propia.

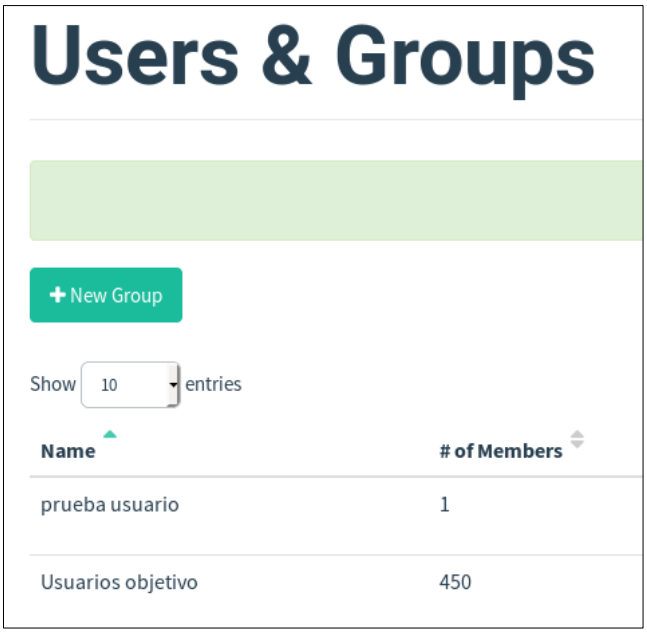


Figura43. Grupos y usuarios creados en Gophish.

Fuente: Elaboración propia.

3.3.6 Generar el landing mediante clonación de una página web

Una vez logueado en la plataforma, nos ubicamos en la pestaña de Landing Pages y al hacer click en Import Site podemos colocar la página que será clonada, o bien se puede programar en formato html tal como se aprecia en la Figura44.

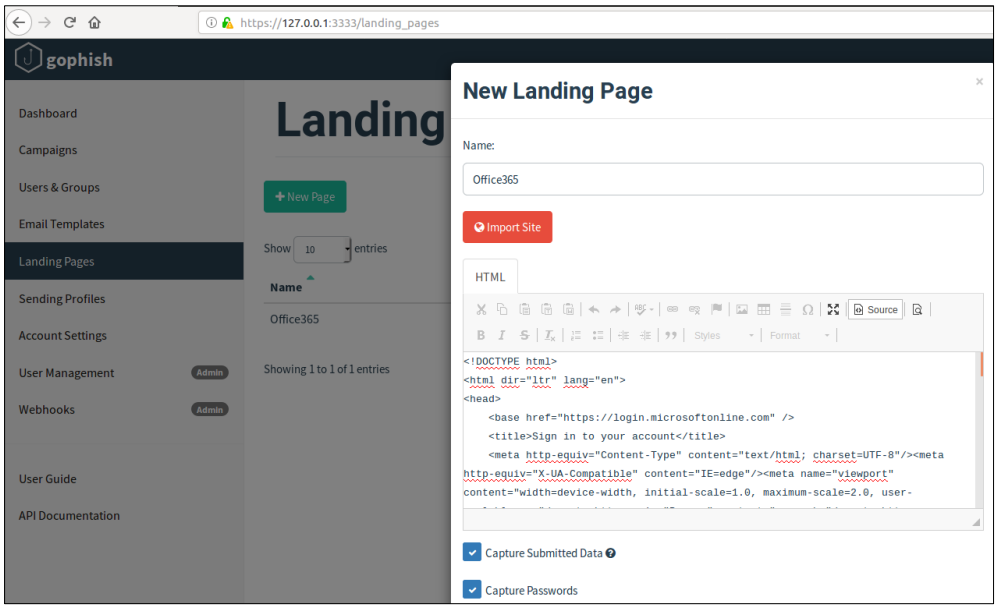


Figura44. Creación de Landing Page.

Fuente: Elaboración propia.

A continuación, en la Figura45, se visualiza la página web clonada que se presentará al usuario y será cargado cuando este haga click en el enlace del correo phishing, por ello se le denomina Landing Page ya que es la página que carga cuando el usuario cae en la trampa.

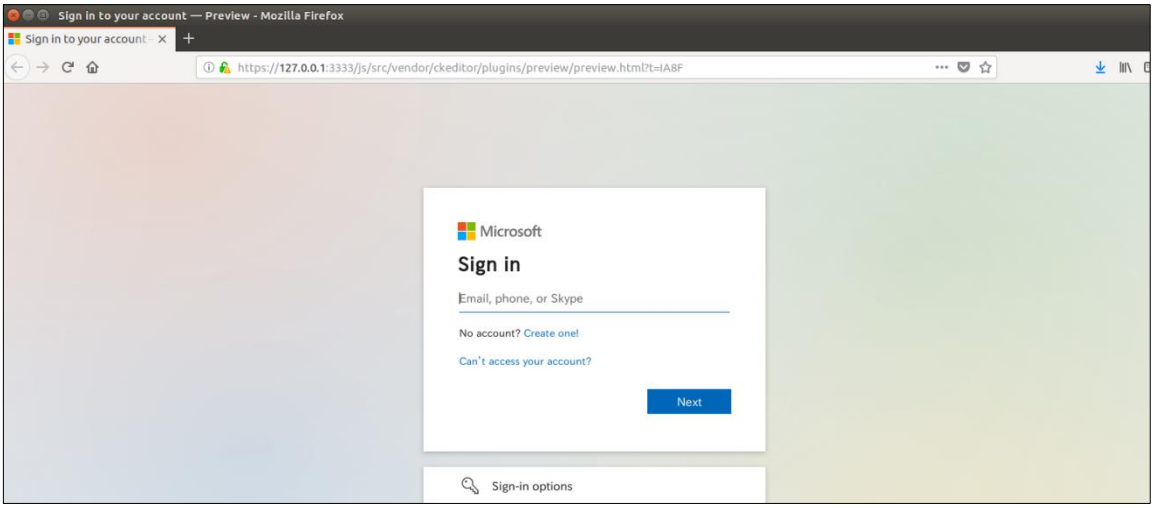


Figura45. Página web clonada de Office365.

Fuente: Elaboración propia.

Se presenta un extracto del código html de la página web clonada de Office365 que puede modificarse respecto al color, tamaño de letra, espacios, logo, entre otros, según se puede observar en la Figura46.

```
TYPE html><html dir="ltr" lang="en"><head>
   <base href="https://login.microsoftonline.com"/>
   <title>Sign in to your account</title>
   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/><meta http-equiv="X-UA-
tible" content="IE=edge"/><meta name="viewport" content="width=device-width, initial-
=1.0, maximum-scale=2.0, user-scalable=yes"/><meta http-equiv="Pragma" content="no-cache"/
a http-equiv="Expires" content="-1"/>
   <link crossorigin="" href="https://aadcdn.msauth.net" rel="preconnect"/><meta http-
="x-dns-prefetch-control" content="on"/>
   <link href="//aadcdn.msauth.net" rel="dns-prefetch"/>
   <link href="//aadcdn.msftauth.net" rel="dns-prefetch"/><meta name="PageID"
nt="ConvergedSignIn"/><meta name="SiteID" content=""/><meta name="ReqLC" content="1033"/
a name="LocLC" content="en-US"/><meta name="referrer" content="origin"/><noscript>
   <meta http-equiv="Refresh" content="0; URL=https://login.microsoftonline.com/jsdisabled" />
/noscript><meta name="robots" content="none"/><script type="text/javascript">//<![CDATA[
ig={"fShowPersistentCookiesWarning":false,"urlMsaSignUp":"https://login.live.com/
20_authorize.srf?response_type=code\u0026client_id=51483342-085c-4d86-bf88-cf50c7252078
6scope=openid+profile+email+offline_access\u0026response_mode=form_post
6redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2
6state=rQIIAYWSu4-TcADHS--u513i-YiDk7nBwZjQAj-
Ckdf0NJCOYgJ4YDScjz6gCs0rj5GE43DxcnJ6KbL6eTicos3m7gbJ-NgHM7o6T_g8l0-3-
uk8VKESkiN1fQIlq9jgOcMMt7FEyZJIBxCkVgE8dIGBCABBiC2gQCZpc3LzKv3q79enOPu__h9MnvB0blENow_PGBU7Si4CV0bRT
TGA4BigSEGW0XKkQRZ3dR0RZIXRei7UlnWoZgogsh7dlF9NlLRY9iRBVDQiem4rsYL8ju4jmnW2wM8Yr4F9f5bK27Hva0op1zwWC
Uin1KM1uOMpsUxsAzT7VErXWK7Y5Tpu7BpGYzDJt3BThRKSA10086o73CEJ3mGK9YnjZ2en1Rqc7GhpJo1oycSpap4q5VkowMGFQ
Fc1dz27kbV36uQs_Xzmz59vnH0enGM_7F3VuP73zcyh2vleaJaKaSXan3qG62h9jzhuJ1PLxXGkY9h6tpaXxA7gdZmibubbyKPip
6estsfed=1\u0026uaid=05b9ab42b3fd458586c5fc94ff875f38\u0026signup=1\u0026lw=1\u0026fl=easi2
6fci=4345a7b9-9a63-4910-a426-35363201d503\u0026mkt=en-US","urlMsaLogout":"https://
.live.com/logout.srf?iframed_by=https%3a%2f%
in.microsoftonline.com","urlOtherIdpForget":"https://login.live.com/forgetme.srf?
ed_by=https%3a%2f%
```

Figura46. Página web clonada de Office365 en formato html.

Fuente: Elaboración propia.

3.3.7 Redactar la plantilla de email

Una vez logueado en la plataforma, nos ubicamos en la pestaña de Email Templates y se completa los datos del asunto con que se remitirá el correo, así como el cuerpo del correo en formato texto o html. Esta parte de la plantilla de correo es personalizable, con incrustación de imágenes, cambio de color, etc, según se puede observar en la Figura47. Así mismo se presenta la plantilla de correo creada, que solicita el cambio de contraseña, supuestamente proveniente de una fuente confiable como Microsoft, tal como se aprecia en la Figura48.

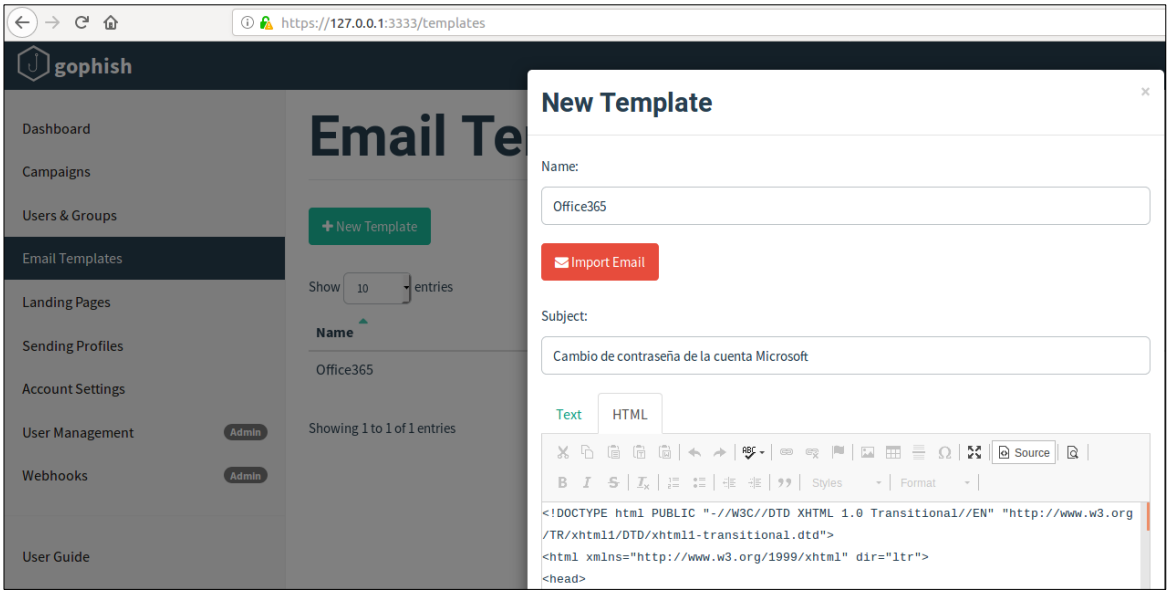


Figura47. Creación de la plantilla de correo.

Fuente: Elaboración propia.

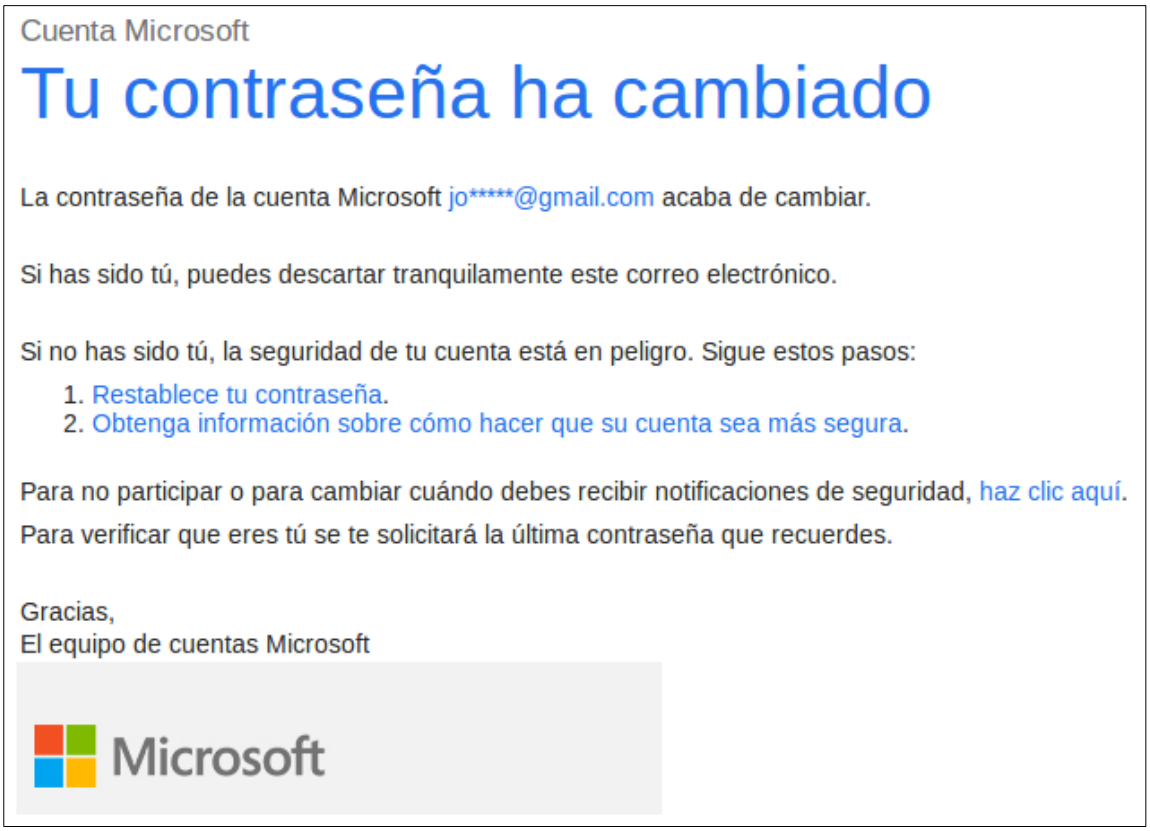


Figura48. Plantilla de correo phishing solicitando el cambio de contraseña.

Fuente: Elaboración propia.

A continuación, en la Figura49, se presenta el código completo de html que se usó para elaborar la plantilla de correo bajo la temática de Microsoft de recuperación de contraseña. Cabe mencionar que en el código html se incrusta los links que se expusieron cuando se instaló ngrok. Entonces cuando llega este correo y el usuario hace click en cualquier enlace se abrirá el landing page donde ingresarán sus credenciales.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr">
<head>
<style type="text/css">
 .link:link, .link:active, .link:visited {
       color:#2672ec !important;
       text-decoration:none !important;
 }

 .link:hover {
       color:#4284ee !important;
       text-decoration:none !important;
 }
</style>
<title></title>
</head>
<body>
<table dir="ltr">
      <tr><td id="i1" style="padding:0; font-family:'Segoe UI Semibold', 'Segoe UI Bold', 'Segoe UI', 'Helvetica Neue Medium', Arial, sans-serif; font-size:17px;
color:#707070;">Cuenta Microsoft</td></tr>
      <tr><td id="i2" style="padding:0; font-family:'Segoe UI Light', 'Segoe UI', 'Helvetica Neue Medium', Arial, sans-serif; font-size:41px; color:#2672ec;">Tu contraseña ha
cambiado</td></tr>
      <tr><td id="i3" style="padding:0; padding-top:25px; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size:14px; color:#2a2a2a;">La contraseña de la
cuenta Microsoft <a dir="ltr" id="iAccount" class="link" style="color:#2672ec; text-decoration:none" href="mailto:jo*****@gmail.com">jo*****@gmail.com</a> acaba de cambiar.</
td></tr>
      <tr><td id="i4" style="padding:0; padding-top:25px; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size:14px; color:#2a2a2a;">Si has sido tú, puedes
descartar tranquilamente este correo electrónico.</td></tr>
      <tr><td id="i5" style="padding:0; padding-top:25px; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size:14px; color:#2a2a2a;">Si no has sido tú, la
seguridad de tu cuenta está en peligro. Sigue estos pasos:</td></tr>
      <tr><td id="i6" style="padding:0; padding-top:6px; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size:14px; color:#2a2a2a;">
         <ol>
          <li><a id="iLink1" class="link" style="color:#2672ec; text-decoration:none" href="https://996e03a7d595.ngrok.io">Restablece tu contraseña</a>.</li>
          <li><a id="iLink2" class="link" style="color:#2672ec; text-decoration:none" href="https://996e03a7d595.ngrok.io">Obtenga información sobre cómo hacer que su cuenta
sea más segura</a>.</li>
         </ol>
      </td></tr>
      <tr><td id="i7" style="padding:0; padding-top:6px; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size:14px; color:#2a2a2a;">Para no participar o para
cambiar cuándo debes recibir notificaciones de seguridad, <a id="iLink3" class="link" style="color:#2672ec; text-decoration:none" href="https://996e03a7d595.ngrok.io">haz
clic aquí</a>.</td></tr>
 </td></tr>
<tr><td id="i7" style="padding:0; padding-top:6px; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size:14px; color:#2a2a2a;">Para verificar que eres tú se
te solicitará la última contraseña que recuerdes.</td></tr>
      <tr><td id="i8" style="padding:0; padding-top:25px; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size:14px; color:#2a2a2a;">Gracias,</td></tr>
      <tr><td id="i9" style="padding:0; font-family:'Segoe UI', Tahoma, Verdana, Arial, sans-serif; font-size:14px; color:#2a2a2a;">El equipo de cuentas Microsoft</td></tr>
</table>
</body>
<img border="0" src="https://msstoreintlemail.blob.core.windows.net/14880-fy18-international-template-update/INTL_es_ES_Promo_Transactional_01.jpg" width="360" height="85"
alt="Microsoft" style="display: block; border: none; color: #000000; background-color: #f2f2f2; font-size: 12px; font-family: Arial;">
</html>
```

Figura49. Plantilla de correo de recuperación de contraseña en formato html.

Fuente: Elaboración propia.

3.3.8 Ejecutar el envío del phishing

Se debe configurar el perfil de envío del phishing, donde se completan los campos de: correo origen, configuración SMTP, usuario y contraseña, tal como se aprecia en la Figura50.

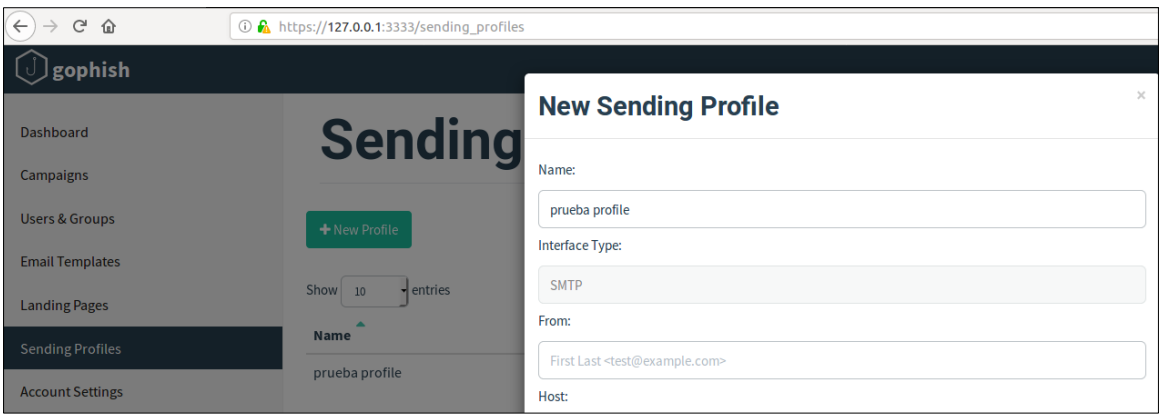


Figura50. Configuración del perfil de envío del phishing.

Fuente: Elaboración propia.

Al remitir un correo de prueba, la plataforma Gophish establece una conexión con Gmail, validando que tanto el usuario, contraseña, servidor SMTP de Gmail y puerto estén sincronizados, tal como se aprecia en la Figura51. Este punto es importante, ya que, si la conexión falla, no se puede continuar con el envío de phishing. Así mismo se debe considerar que se puede usar un servidor de correo instalado de forma local en Ubuntu como alternativa.

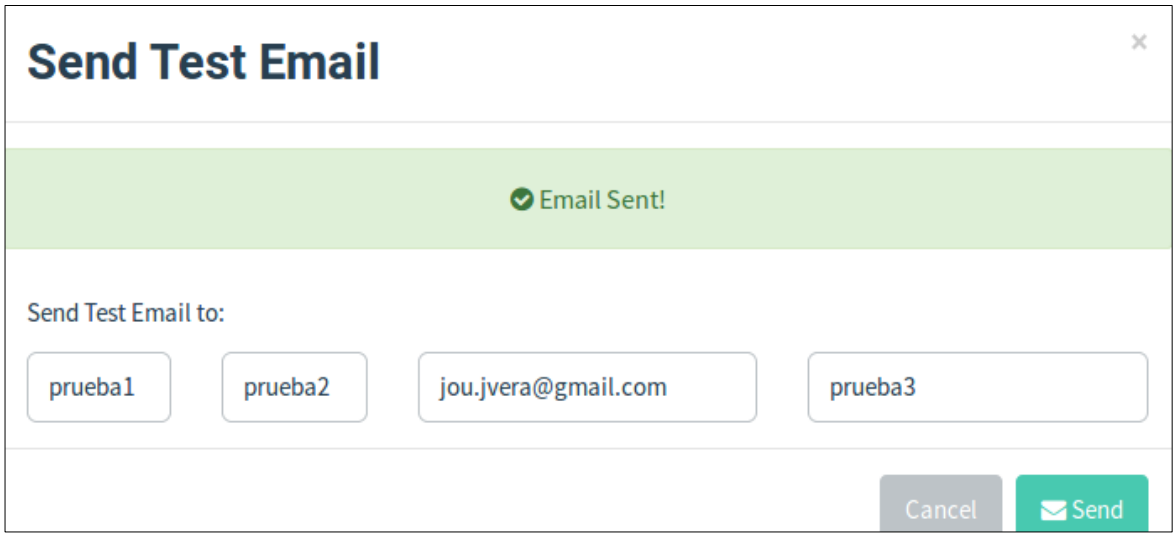


Figura51. Envío de correo de prueba.

Fuente: Elaboración propia.

A continuación, en la Figura 52, se presenta la recepción del correo de prueba.

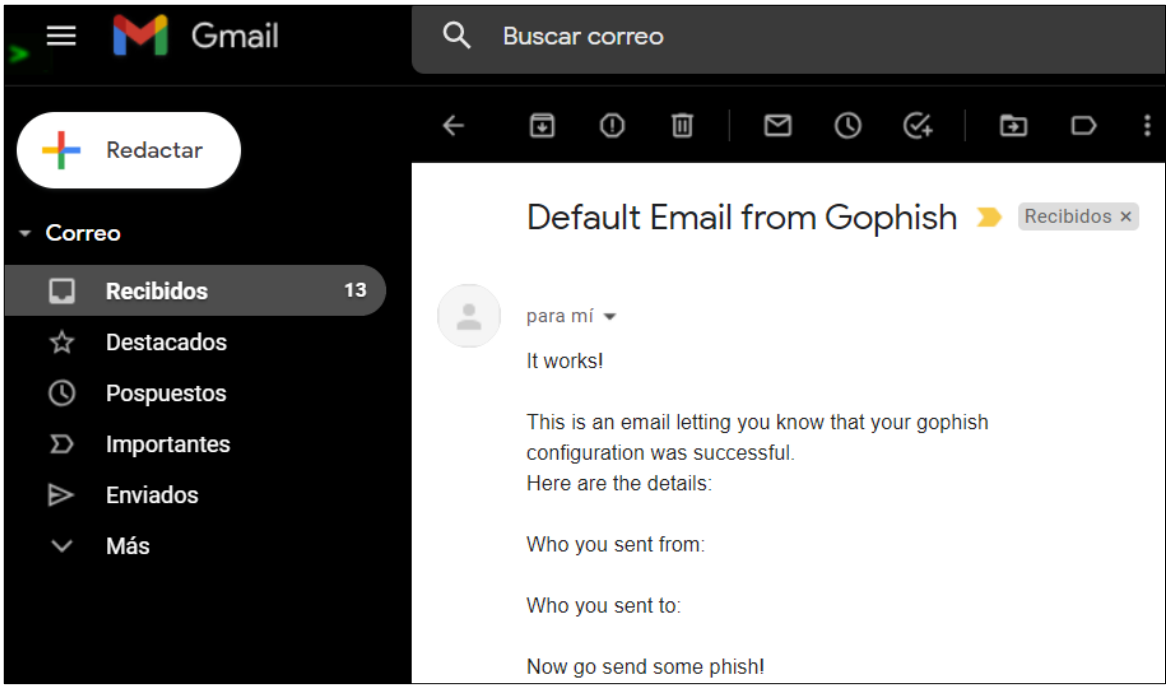


Figura52. Recepción de correo de prueba.

Fuente: Elaboración propia.

Dentro de Gophish se puede programar el envío del phishing en el momento o en una fecha determinada y también se usa para reforzar a los usuarios que cayeron en la trampa del phishing, programándolos en una nueva fecha para mejorar la métrica y reforzando la concientización de los usuarios hasta que no representen un riesgo para la seguridad de la información. Dicho esto, en Gophish se crea una campaña tal como se aprecia en la Figura53, donde se autocompleta los campos con información previa de los anteriores módulos, tales como: plantilla de correo, landing page, perfil de envío y grupos de usuarios.

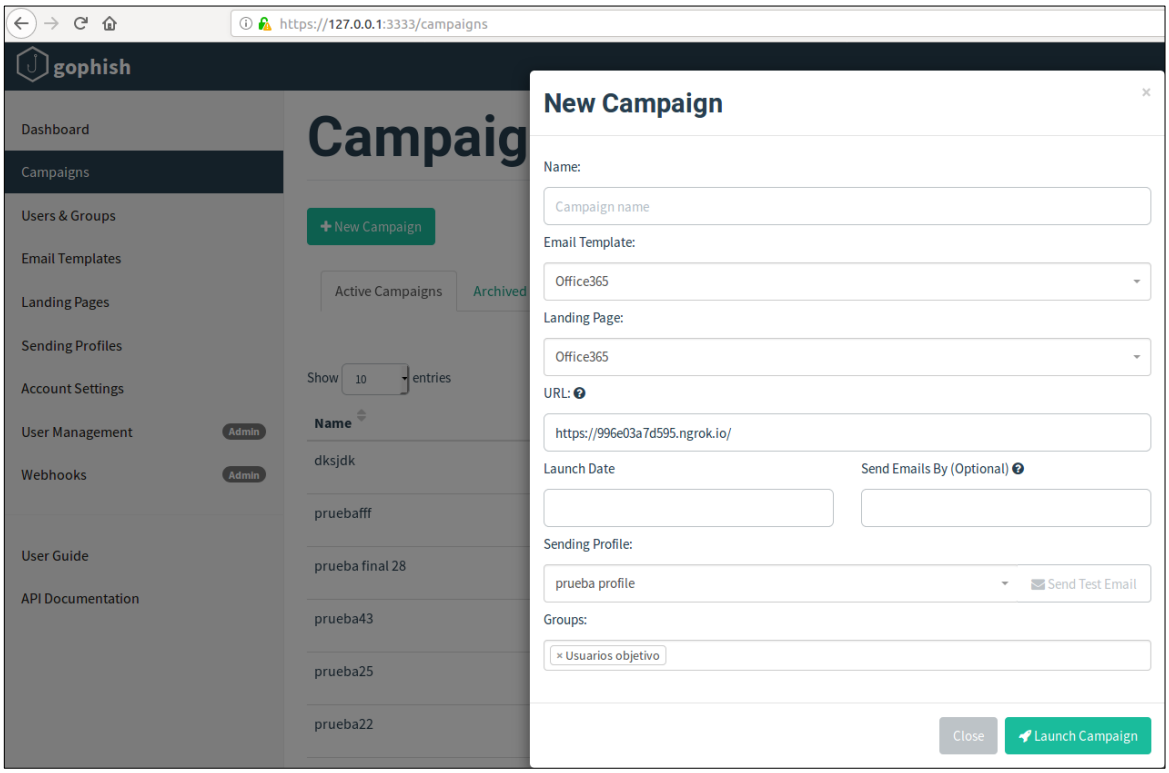


Figura53. Creación de una campaña de phishing.

Fuente: Elaboración propia.

CAPITULO 4

RESULTADOS Y PRESUPUESTO

4.1 Resultados

Se implementó la plataforma Gophish para mejorar la seguridad de la información a fin de reducir los ciberataques del tipo phishing en una entidad financiera; para ello, para que se pueda medir correctamente la mejora, se tiene un antes y un después de ejecutar una campaña de phishing. Según se puede apreciar en la Figura54, de forma previa al inicio del proyecto de investigación, se remitió un total de 450 correos a los colaboradores, donde 242 abrieron el correo y 190 le hicieron click al link adjunto, así mismo 95 colocaron sus datos personales y 7 reportaron, lo que resulta en un número abultado y negativo frente a los indicadores que se maneja en el área.

Figura54. Indicadores previos de una campaña de phishing.

Fuente: Elaboración propia.

4.1.1 Resultados de los objetivos específicos

Objetivo Nº1: Reducir el porcentaje de los usuarios que hacen click al link de un correo phishing.

Según la Figura55, se redujo la cantidad de usuarios que hacen click al link de un correo phishing en un 40%, el cual es válido, ya que se busca llegar lo más cercano a 100%.

Inicialmente 190 usuarios hicieron click al link de un correo phishing, luego bajó a 114.

Objetivo Nº2: Reducir el porcentaje de los usuarios que brindan información al completar un formulario falso de un correo phishing.

Según la Figura55, se redujo la cantidad de usuarios que brindan información al completar un formulario falso de un correo phishing en un 67.36%, el cual es válido, ya que se busca que ningún usuario que cae en el phishing brinde sus datos tales como: usuario y contraseña.

Inicialmente 95 usuarios brindaron información al completar un formulario falso de un correo phishing, luego bajó a 31.

Objetivo Nº3: Aumentar el porcentaje de los usuarios que reportan un correo phishing.

Según la Figura55, se aumentó la cantidad de usuarios que reportan un correo phishing en un 57.14%, el cual es válido, ya que se busca que más usuarios reporten estos casos con el sólo hecho de abrir el correo phishing.

Inicialmente 7 usuarios reportaron el correo phishing, luego aumentó a 11.

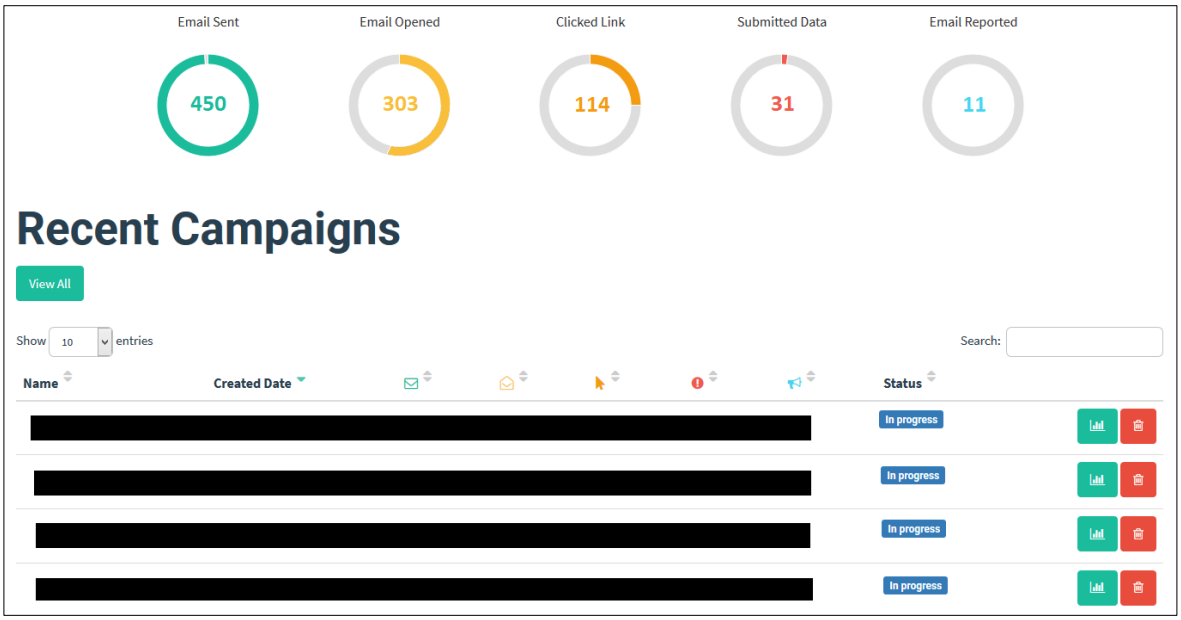


Figura55. Indicadores posteriores a la campaña de phishing.

Fuente: Elaboración propia.

4.2 Presupuesto

Para el desarrollo del proyecto dentro del presupuesto se consideró el recurso humano, equipamientos utilizados y recursos materiales con un monto total de S/ 24,728.00 para el lapso de 03 meses que dura el proyecto, tal como se detalla en la Tabla9.

Tabla9. Presupuesto del proyecto.

Recursos humanos	Dedicación	N° horas	Costo por hora	Sub-total
Analista de seguridad de la información	Completa	768	S/ 23.50	S/ 18,048.00
Jefe de seguridad de la información	Parcial	10	S/ 36.50	S/ 365.00
Gerente de seguridad e inspectoría	Parcial	10	S/ 62.50	S/ 625.00
Equipamiento utilizado	**Tipo de Equipo**	**Cantidad**	**Costo**	**Sub-total**
Laptop	Core i7	1	S/ 4,500.00	S/ 4,500.00
Licencia Windows	Windows 10 Home	1	S/ 620.00	S/ 620.00
Modem internet	Plan ilimitado	3	S/ 180.00	S/ 540.00
Recursos materiales	**Unidad**	**Cantidad**	**Costo**	**Sub-total**
Papel bond	Paquete	1	S/ 20.00	S/ 20.00
Lapiceros	Caja	1	S/ 10.00	S/ 10.00
Total				S/ 24,728.00

Fuente: Elaboración propia.

4.2.1 Desempeño del proyecto y valor ganado

Asimismo, para controlar los costos en el desarrollo del proyecto, se presenta el valor ganado que combina medidas del alcance, cronograma y recursos para evaluar el desempeño y el avance del presente proyecto de implementación. A continuación, en la Figura56 se presenta la línea base del alcance con la línea base de costos, junto con la línea base del cronograma, las cuales forman parte de la línea base para la medición del desempeño.

- Valor Planificado (VP): Es el presupuesto autorizado que se ha asignado al trabajo programado.

- Valor Ganado (EV): Es la medida del trabajo realizado en términos de presupuesto autorizado para dicho trabajo.

- Costo Real (AC): Es el costo incurrido por el trabajo llevado a cabo en una actividad durante un periodo de tiempo específico.

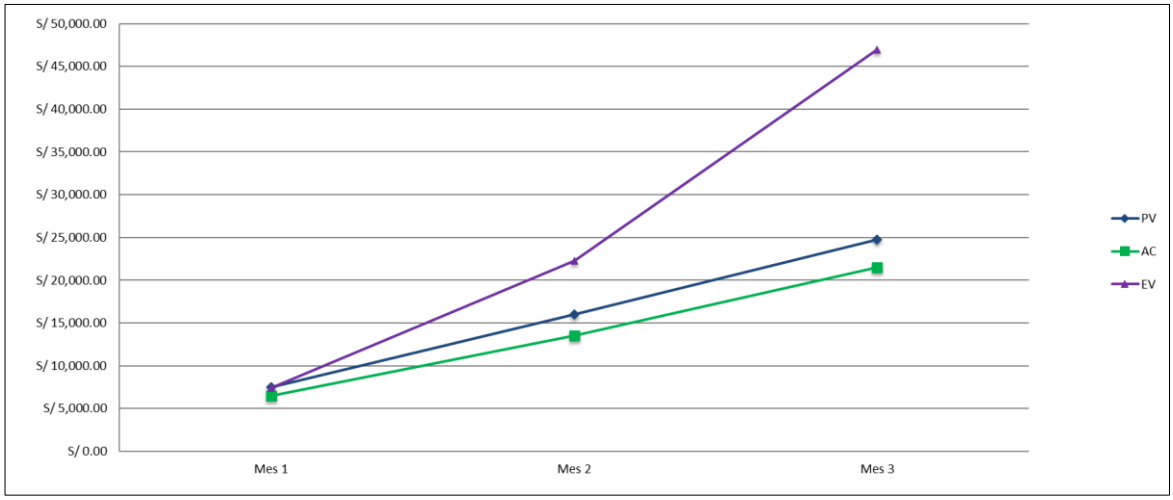


Figura56. Medición del desempeño del proyecto.

Fuente: Elaboración propia.

En cuanto al cierre del proyecto en el Mes 3, se tienen los siguientes valores: Valor Planificado (PV) en S/ 24,728.00, Valor Ganado (EV) en S/ 24,728.00 y Costo Real (AC) en S/ 21,500.00, según se puede apreciar en la Figura57.

Valor Ganado				
Proyecto:	Implementación de Gophish en una entidad financiera			
ID:	IGEF-2019			
		Mes 1	**Mes 2**	**Mes 3**
Valor Planificado		S/ 7,500.00	S/ 8,500.00	S/ 8,728.00
Valor Planificado Acumulado	**PV**	S/ 7,500.00	S/ 16,000.00	S/ 24,728.00
Costo Real		S/ 6,500.00	S/ 7,000.00	S/ 8,000.00
Costo Real Acumulado	**AC**	S/ 6,500.00	S/ 13,500.00	S/ 21,500.00
Porcentaje de avance completado del mes	**%comp**	30.0%	60.0%	100.0%
Valor ganado del trabajo realizado	**[EV= % comp x BAC]**	S/ 7,418.40	S/ 14,836.80	S/ 24,728.00
Valor ganado del trabajo realizado acumulado	**EV**	S/ 7,418.40	S/ 22,255.20	S/ 46,983.20
Costo total prespuestado (BAC)	S/ 24,728.00			

Figura57. Matriz de valor ganado.

Fuente: Elaboración propia.

Conviene subrayar que la variación del costo (CV) tiene un valor positivo el cual indica que el proyecto ha gastado menos de lo presupuestado. Así mismo, la variación del cronograma (SV) tiene un valor positivo el cual indica que el proyecto está adelantado acorde a la revisión de cada mes, según se puede observar en la Figura58.

Indices y variaciones	Valor
Variación del costo (CV/Cost Variance) [**CV=EV-AC**]	25,483
Variación del cronograma (SV/Schedule Variance) [**SV=EV-PV**]	22,255
Índice de desempeño del costo (CPI/Cost Performance Index) [**CPI = EV/AC**]	2.19
Índice de desempeño del cronograma del proyecto (SPI/Schedule Performance Index) [**SPI = EV/PV**]	1.39
Estimación a la conclusión (EAC/Estimate at Completion) [**EAC = BAC/CPI**]	11,316

Figura58. Matriz de índices y variaciones.

Fuente: Elaboración propia.

4.2.2 Flujo de caja

En cuanto al flujo de caja se determina la posición del efectivo al final de cada mes de lo que dura el proyecto, de Octubre a Diciembre del 2019, obteniendo al cierre del proyecto en el mes de Diciembre un saldo positivo de S/ 3,228.00 según se puede observar en la Figura59.

Flujo de caja

	Inicio	OCT 2019	NOV 2019	DIC 2019
Efectivo en la mano (al principio del mes)	S/ 24,728.00	S/ 24,728.00	S/ 18,228.00	S/ 11,228.00
Ingresos				
Ingreso real		S/ 0.00	S/ 0.00	S/ 0.00
Efectivo total disponible	S/ 24,728.00	S/ 24,728.00	S/ 18,228.00	S/ 11,228.00
Gastos				
Gasto real		S/ 6,500.00	S/ 7,000.00	S/ 8,000.00
Efectivo total pagado	S/ 0.00	S/ 6,500.00	S/ 7,000.00	S/ 8,000.00
Posición del efectivo (al final del mes)	S/ 24,728.00	S/ 18,228.00	S/ 11,228.00	S/ 3,228.00

Figura59. Flujo de caja.

Fuente: Elaboración propia.

CONCLUSIONES

Luego de haber desarrollado la presente investigación se logró solucionar el problema planteado y cumplir con los objetivos propuestos, obteniendo resultados satisfactorios, los cuales se detallan a continuación:

- Se cumple plenamente el objetivo general de “mejorar la seguridad de la información para reducir los ciberataques del tipo phishing en una entidad financiera” en un 54.83%. De acuerdo con el resultado se concluye que los trabajadores están más concientizados en temas relacionados a ciberseguridad, el cual fortalece los demás controles de seguridad que se tienen implementados en la organización y reduce la brecha frente a un ciberataque de phishing.

- Se cumple plenamente el objetivo específico de “reducir el porcentaje de los usuarios que hacen click al link de un correo phishing” en un 40%. De acuerdo con el resultado se concluye que los trabajadores hacen menos click en algún link de un correo phishing, esto va de 190 a 114 para la muestra analizada según los datos proporcionados luego de la implementación de Gophish.

- Se cumple plenamente el objetivo específico de “reducir el porcentaje de los usuarios que brindan información al completar un formulario falso de un correo phishing” en un 67.36%. De acuerdo con el resultado se concluye que los trabajadores brindan menos información en los formularios falsos de un correo phishing, esto va de 95 a 31 para la muestra analizada según los datos proporcionados luego de la implementación de Gophish.

- Se cumple plenamente el objetivo específico de “aumentar el porcentaje de los usuarios que reportan un correo phishing” en un 57.14%. De acuerdo con el resultado se concluye que los trabajadores reportan más un correo phishing, esto va de 7 a 11 para la muestra analizada según los datos proporcionados luego de la implementación de Gophish.

BIBLIOGRAFÍAS

World Economic Forum (2021). *The Global Risk Report 2021.* Recuperado de http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Microsoft (2020). *Microsoft Digital Defense Report*. Recuperado de https://www.microsoft.com/en-us/download/confirmation.aspx?id=101738

Aquije J. y Jave L. (2012). *Metodología de gestión de seguridad de la información para el sector financiero peruano* (tesis de pregrado). Universidad Nacional de Ingeniería, Lima, Perú.

MITRE CORPORATION (2021). ATT&CK Matrix for Enterprise [Imagen]. Recuperado de https://attack.mitre.org/matrices/enterprise/

Welivesecurity (2015). 5 tipos de phishing en los que no debes caer [Imagen]. Recuperado de https://www.welivesecurity.com/la-es/2015/05/08/5-tipos-de-phishing/

AntiPhishing Latinoamérica (2020). Cuidado: Correo “Consultas Clientes” es phishing [Imagen]. Recuperado de https://twitter.com/AntiPhishing_La/status/1213209089104330757/photo/1

Malwarebytes (2020). Spear Phishing 101: lo que necesitas saber [Imagen]. Recuperado de https://malwarebytes.antimalwares.es/890-2

Protegerse (2019). Una campaña de phishing que suplanta al banco Santander se propaga por correo y SMS [Imagen]. Recuperado de https://blogs.protegerse.com/2019/06/04/una-campana-de-phishing-que-suplanta-al-banco-santander-se-propaga-por-correo-y-sms/

Castillo, C. (25 de abril, 2019). 'Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas?. *BBVA.* Recuperado de https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

Reciprocity (18 de noviembre, 2019). ¿Qué son los controles de seguridad de la información?. Recuperado de https://reciprocitylabs.com/resources/what-are-information-security-controls/

Avila S. (11 de diciembre de 2020). Fraude informático: 1771 personas han sido víctimas de los ciberdelincuentes según estadísticas de la DIVINDAT. *Perú21*. Recuperado de https://peru21.pe/lima/fraude-informatico-1771-personas-han-sido-victimas-de-los-ciberdelincuentes-segun-estadisticas-de-la-divindat-nczp-noticia/

Bermúdez R., y Moreira K. (2020). *Análisis de las incidencias e impactos de ataques de ingeniería social o ciberdelitos en la carrera de ingeniería civil de la facultad de ciencias matemáticas y físicas* (tesis de pregrado). Universidad de Guayaquil, Guayaquil, Ecuador.

Montenegro L. (2017). *Propuesta metodológica para la evaluación de seguridad de usuarios de redes sociales con relación a ataques de ingeniería social* (tesis de maestría). Universidad de Cuenca, Cuenca, Ecuador.

Quispe R. (2020). *Implementación de Wombat Security Awareness para reducir ciberataques de phishing al personal de la entidad financiera* (tesis de pregrado). Universidad Tecnológica del Perú, Lima, Perú.

ISO (2014). *Information technology - Security techniques - Information security management systems - Overview and vocabulary* (3ª ed.) [PDF], Suiza: publicado independientemente.

ISO (2015). *Tecnología de la Información – Técnicas de Seguridad – Código de prácticas para los controles de seguridad de la información* (1ª ed.) [PDF], España: AENOR.

Prowse D. (2018). *CompTIA Security+ SY0-501 Cert Guide* (4ª ed.) [PDF], USA: Pearson.

Gómez L. y Fernández P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad* (1ª ed.) [PDF], España: AENOR.

SBS (2009). *Gestión de la seguridad de la información* (Circular Nº G-140-2009). Recuperado de https://www.sbs.gob.pe/Portals/0/jer/Auto_Nuevas_Empresas/Normas_Comunes/9.%20Gesti%C3%B3n%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n_Circ.%20SBS%20G-140-2009.pdf

Vallejos F. (2020). *Desarrollo de un simulador web aplicando la norma ISO/IEC 27002 enfocado a ingeniería social* (tesis de pregrado). Universidad Técnica del Norte, Ibarra, Ecuador.

Reuters (17 de agosto de 2018). Bancos en Perú repelen una serie de ciberataques y suspenden temporalmente sus servicios. *Reuters*. Recuperado de https://www.reuters.com/article/peru-bancos-ciberataque-idLTAKBN1L300D-OUSLB

ONGEI (2010). *VIII Encuesta Nacional de Recursos Informáticos y Tecnológicos de la Administración Pública.* Recuperado de https://docplayer.es/4367362-Viii-enriap-enriap-viii-encuesta-nacional-de-recursos-informaticos-y-tecnologicos-de-la-administracion-publica-ing-carlo-angeles-otarola.html

Kwak Y., Lee S., Damiano A. y Vishwanath A. (2020). Why do users not report spear phishing emails?. *Telematics and Informatics, 48* (1). doi: 10.1016/j.tele.2020.101343

Sahingoz O., Buber E., Demir O. y Diri B. (2018). Machine learning based phishing detection from URLs. *Expert Systems With Applications, 117* (1). doi: 10.1016/j.eswa.2018.09.029

Pirocca S., Allodi L. y Zannone N. (2020) A Toolkit for Security Awareness Training Against Targeted Phishing. *Information Systems Security, 12553* (1). doi: 10.1007/978-3-030-65610-2_9

Hornetsecurity (s.f.). *¿Qué es un ataque de phishing? ¿Y cómo las empresas pueden protegerse de ello?.* Recuperado de https://www.hornetsecurity.com/es/knowledge-base/phishing/