PLAN PARA CONCIENCIAR A USUARIOS CONECTAMEF EN LA SEGURIDAD DE INGENIERÍA SOCIAL DEL MINISTERIO DE ECONOMIA Y FINANZAS

INVESTIGACION PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS Y SEGURIDAD INFORMÁTICA

AUTOR:

Bach. Valery María Quijano Bravo

PERÚ – 2019

Dedicatoria:

A Dios quien siempre está conmigo aunque yo muchas veces he sido ingrata con él, a mi madre, mi tía y hermana que me vieron en este proceso de superación, y a todos los que se vieron involucrados de alguna manera.

Agradecimiento:

A todos los docentes de la carrera de Ingeniería de Sistemas de la “Universidad Peruana Simón Bolívar” por su valiosa enseñanza y permanente orientación, durante nuestros estudios de Postgrado, a mis amigos que me apoyaron con sus valiosas opiniones; al Mg. Melitón Ricardo Otoya Verástegui, por su asesoría; y a los colaboradores del área de sistemas del MEF; por su valiosa colaboración durante el desarrollo de la presente investigación.

Índice

Índice de tablas

Índice de figuras

Resumen

Vemos como el mundo va creciendo inmensamente a nivel tecnológico ayudando así en diferentes materias como es la medicina, formas de comunicarnos, nuevas formas de realizar nuestras compras, formas de distraernos, y muchas otras, las cuales vemos como poco a poco nos va facilitando el vivir que tenemos actualmente.

Lamentablemente no es tan maravilloso como se podría entender a leer las primeras líneas de este texto, pues así como la tecnología va avanzando a grandes rasgos, las personas con fines maliciosos también están en aumento. Es por eso que a causa de ello se ha visto la necesidad de implementar medidas de seguridad en las redes de comunicación, como los famosos cortafuegos, seguridad en los proxys, y cualquier otra forma de seguridad en las instituciones. Pero de qué sirve implementar la última tecnología en protección si al final el usuario final va aceptar un correo con el último malware de internet y entonces todo lo invertido en protección sería en vano. Ya que con solo el hecho de hacer un clic puede traspasar esas medidas. Es por ello de la importancia de la concienciación a los usuarios finales y es el porqué de este trabajo de investigación. Poder informarles a los usuarios acerca de la seguridad en Ingeniería Social para que no sean vulnerables a los ataques usando esa técnica.

Abstract

We see how the world is growing immensely at a technological level for helping in different areas such as medicine, ways of communication, new ways of doing our shopping, ways to distract us, and any others, which we see as little by little the live we currently have.

Unfortunately it is not as wonderful as we could understand when we read the first lines of this text, because just as technology is advancing in broad strokes, people with malicious purposes are also increasing. As a result, we have seen the importance of implementing security measures in communication networks, such as the famous firewalls, security in the proxies, and any other way of security in the institutions. But what is the purpose of the most recent protection technology implementation, if final user accepts an email with the latest Internet malware, investigation about protection would be in vain. Because with just the fact of making a click can pass these measures. That is the reason the importance of awareness to end users is why this research work. To be able to inform users about security in Social Engineering so they are not vulnerable to attacks using that technique.

Introducción

Así como se mencionó anteriormente a raíz de la aparición de las nuevas tecnologías las organizaciones busquen las medidas de seguridad más adecuadas para su institución para prevenir los robos de información que se podrían presentar en las redes de comunicación. Las instituciones están enfocadas en establecer reglas, bloqueando accesos e infinidad de formas para sentirse seguros ante las amenazas del entorno informático lo cual está muy bien. Pero muchas veces se descuida una de las partes más importantes; que vendría a ser el eslabón más débil, el usuario.

Es por ello que en presente trabajo de investigación se quiere reflejar un plan de concienciación. Siendo en el Capítulo I donde se da una pequeña reseña histórica de la institución, también en este capítulo se verá el espejo del problema que se presentan en el mundo, sin dejar de lado los objetivos generales y específicos, la justificación y delimitación del trabajo. En el capítulo II nos adentramos al marco Teórico-Conceptual refiriéndonos ahí a los antecedentes de la investigación, definiendo algunos términos sobre la Ingeniería Social y amenazas existentes en dicho entorno, usando las variables que serán adecuadas para la investigación. En el capítulo III ya empezamos a trabajar con la metodología de la Gestión del cambio donde vemos algunas definiciones de ello y hablando como va reflejando ello a la institución estudiada y así saber cuáles son las estrategias, actividad operativa, presupuesto, descripción del avance, Limitaciones, análisis de costos y el cronograma de actividades del trabajo. Por último Se verán las conclusiones y recomendaciones obtenidas al fin del trabajo de investigación.

CAPITULO I: EL PROBLEMA

1.1 Reseña de la Empresa del caso de estudio

El Ministerio de Economía y Finanzas fue fundado el 03 de Agosto de 1821 por decreto de Don José de San Martín poniendo inicialmente el nombre de Ministerio de Hacienda, Según la fuente consultada, https://www.mef.gob.pe/es/. El 02 de Marzo de 1969 se aprobó la Ley Orgánica del Ministerio de Hacienda, que determinó su estructura y funciones, Bajo el Decreto Ley N° 17703 del 13 de Junio de 1969, modificó la denominación de Ministerio de Hacienda por Ministerio de Economía y Finanzas.

El Ministerio de Economía y Finanzas con Ruc. 20131370645 es un organismo del Poder Ejecutivo, cuya organización, competencia y funcionamiento está regido por el Decreto Legislativo Nº 183 y sus modificatorias. Está encargado de planear, dirigir y controlar los asuntos relativos a presupuesto, tesorería, endeudamiento, contabilidad, política fiscal, inversión pública y política económica y social. Asimismo diseña, establece, ejecuta y supervisa la política nacional y sectorial de su competencia asumiendo la rectoría de ella.

1.1.1. Vision

Sector que impulsa el crecimiento económico sostenido, que contribuye a una mejor calidad de vida de los peruanos, garantizando una política fiscal responsable y transparente, en el marco de la estabilidad macroeconómica.

1.1.2. Misión

Armonizar la política económica y financiera, a través de la transparencia y responsabilidad fiscal, contribuyendo al crecimiento económico sostenido del país.

1.1.3. Objetivos Estratégicos Institucionales

- Consolidar el equilibrio y sostenibilidad fiscal.
- Mejorar el nivel de estabilidad de los ingresos públicos.
- Lograr una mayor apertura económica y armonización del mercado de bienes y servicios.
- Incrementar la cobertura y eficiencia de los mercados financieros y previsional privado.
- Reactivar la inversión orientada al cierre de brechas de infraestructura social y productiva.
- Mejorar la calidad del gasto público en los diversos niveles de gobierno.
- Optimizar la transparencia y rendición de cuentas en el sector público.
- Modernizar la gestión institucional del Ministerio.

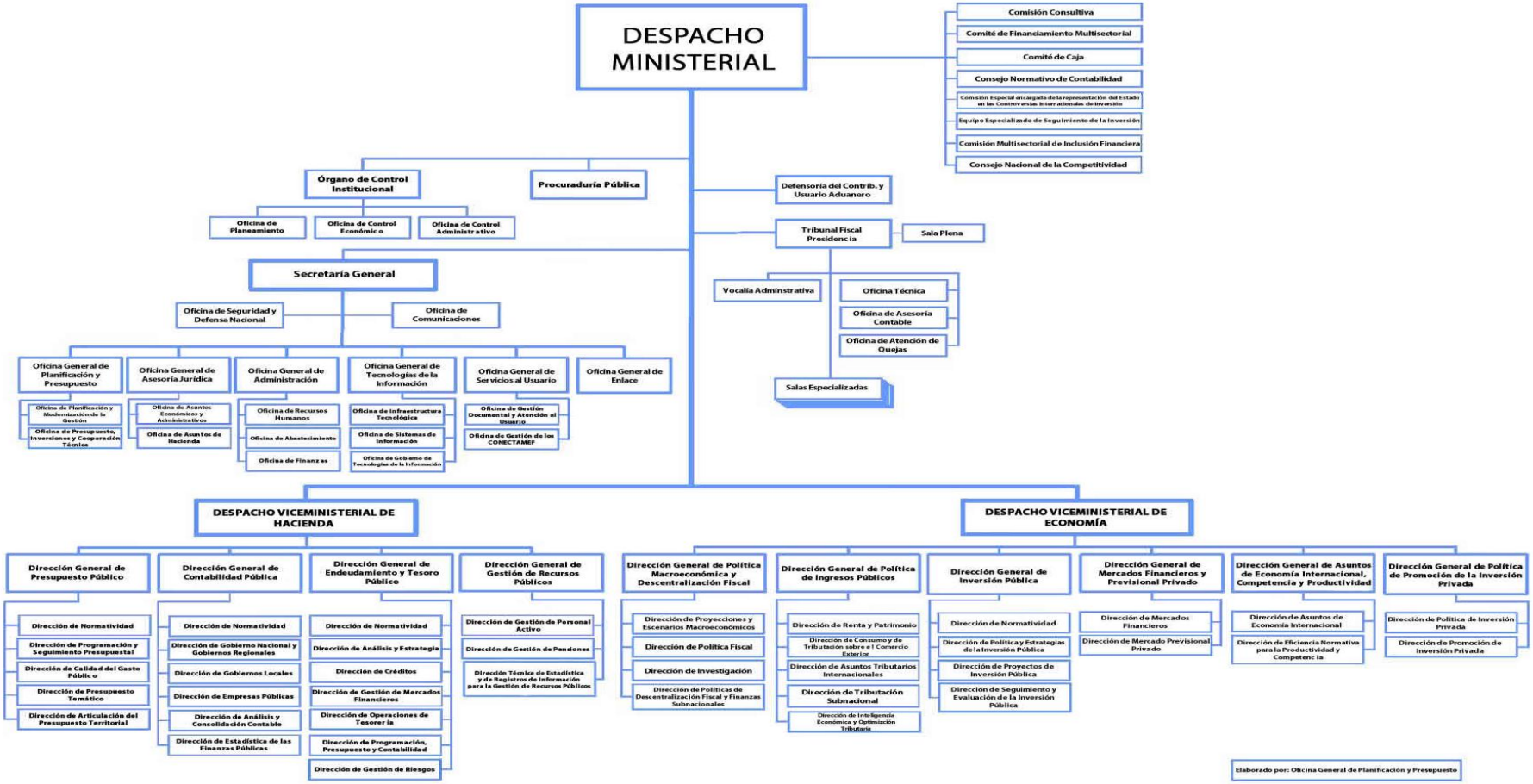


Figura 1. Organigrama Estructural del Ministerio de Economía y Finanzas

Fuente: https://www.mef.gob.pe/images/stories/Organigrama_MEF.jpg

1.2 Descripción del escenario Problema

En los últimos años hemos escuchado sobre estafas que se realizan por tarjetas de crédito, correos de cuentas bancarias, las cuales piden información personal o hasta historiales de las mismas e infinidad de cosas más, ello nos indica que algo anda mal, algo puede pasar, pues ya en muchos medios de comunicación se está informando de dichas estafas las cuales nos mencionan que tienen un impacto significativo para la economía así como lo menciona en su página web (GMO GlobalSing, Inc., 2018) Empresa especializada en transacciones seguras de comercio, comunicaciones y más. Informo que en EE.UU., el FBI al American Banking Journal los costos acumulados de Ingeniería Social desde 2013 han costado a las empresas $1.600 millones.

De acuerdo con el informe de Ponemon Institute Accenture, "Estudio del costo de la delincuencia cibernética de 2017", va en aumento significativo con un 62%. También comenta que las organizaciones están lidiando con un promedio de 130 infracciones de seguridad exitosas cada año y esto va en aumento de 27% año tras año.

GMO GlobalSing, Inc., mencionó también a Tony Reijm quien afirma que los costes de amenazas cibernéticas se proyectan en $2 billones en 2019, y con un gran desastre cibernético es equivalente a uno desastre natural con ($53 mil millones). GMO GlobalSing, Inc., "¿Qué tienen que ver todas estas estadísticas sobre incidentes cibernéticos con la ingeniería social?" pues que más del 90% se deben al elemento humano.

Cifras de verdad muy escalofriantes para que solo haya sido en un sector del mundo y con potencias mejores desarrollas que en otros países, y vemos que al parecer el interés de ataque de Cibernético y sobre todo de ingeniería social es muy grande o está de moda ya que en la investigación Estudio de Metodologías de Ingeniería Social (Marín, 2018) informa que si bien la mayoría de ataques cibernéticos en el año 2016 fueron por malware, tres de las principales amenazas

de ciberataques se relacionaron por el factor humano eso quiere decir que se usó la ingeniería social para realizar dichos ataques.

Sobre este asunto Marín dijo que dichos ataques fueron a través de correos electrónicos con la técnica llamada phishing y otros por los errores del factor humano pero también el uso inadecuado. Mencionando también en su trabajo de investigación que en el año 2015 21.8% de las filtraciones de datos se debieron a ataques de tipo phinshing y spoofing, mientras que en el 2017, los errores humanos tuvieron una cifra del 19% y 36% de todas las violaciones de robos de datos dependiendo del país o región.

Tenemos dos puntos de vista que nos indican sobre las amenazas diciéndonos que las cifras van en aumento con lo que respecta a la participación del ser humano ya sea por la técnica de ataque phissing, spoofing u correos electrónicos, entonces eso quiere decir que las personas somos las que más estamos dando pie a ser víctimas de diversas amenazas y sobre todo de ingeniería social ya que como se mencionó son las de mayor impacto para los ciberataques.

Muchas empresas e instituciones están siendo afectadas por las amenazas que conllevan la ingeniería social. (Roque y Juárez, 2018), hicieron un estudio de investigación en donde pudieron ver en sus resultados que los estudiantes universitarios de la carrera de informática sabían poco acerca del término de phishing y las consecuencias de este ataque.

También en el ámbito universitario (Flórez y Méndez, 2017) concluyeron en su trabajo de investigación titulado Estudio de ingeniería social en el uso de redes sociales que el problema que tenía la universidad del Valle en Cali, Colombia era que un 38% de los encuestados se encontraban vulnerables con lo que respecta el buen manejo de sus cuentas de correo electrónico y que así serian un punto débil para la materialización de una amenaza por ese medio, también mencionaron que un 55% de ellos no tenían las medidas de seguridad pactadas para la creación de contraseñas seguras.

Una de las preguntas sobre ingeniería social fue la siguiente "¿Has sido víctima de ingeniería social?" en la cual dijeron que de 167 encuestados 88 habían dicho que "si" y 79 que "no" el cual no se comparte la opinión pues no es sustento suficiente para saber si han sido víctimas de ingeniería social con una afirmación o negación del estudiante.

Finalmente dijeron que la universidad no contaba con controles estrictos de seguridad en internet pero si tenían filtros web en especial de contenido sexual videojuegos, etc. Entonces están abiertos a ataques phissing, llegada de spam e infección de malware por tener un bajo índice que personas con contraseñas inseguras haciéndolas una carnada fácil ante los ciberdelincuentes.

Existen problemas de educación en las instituciones y en las empresas de todos los países del mundo. (Mendoza, 2019), redacto en el diario Gestión que en Perú las empresas se estima que un 26% de los ciberataques son originados por empleados maliciosos y el 23% por empleados descuidados. Queriendo decir que por general en el Perú la principal causa de ataques también son causadas por el factor humano.

1.3 Formulación del Problema

Se asume que en el Ministerio de Economía y Finanzas existen posibles amenazas con la Ingeniería Social ya que al parecer se ha visto que posiblemente existan personas afectadas por los correos mal intencionados y también se piensa que el personal no entienden de este tema. También se asume que es posible que algunos usuarios estén recibiendo correos mal intencionados y que no los estén reportando lo que hace más difícil la detección de los correos mal intencionados por el área de sistemas del ministerio.

1.3.1 Problema general

¿De qué manera la concienciación a los usuarios Conectamef influye en la Seguridad de Ingeniería Social en el Ministerio de Economía y Finanzas?

1.4 Pronostico

En caso los usuarios Conectamef del Ministerio de Economía y Finanzas no sean informados sobre las amenazas de Ingeniería Social ellos podrían caer en una trampa, mediante correos mal intencionados que pidan información confidencial pudiendo los usuarios al estar desinformados entregarles dichos datos el cual afecte la infraestructura del Ministerio, robo de información y más.

1.5 Objetivos

1.5.1 Objetivo General

Concienciar a los usuarios conectamef del Ministerio de Economía y Finanzas sobre la Seguridad de Ingeniería Social.

1.5.2 Objetivos específicos

Primer objetivo específico

Realizar plan para concienciar en forma presencial a los usuarios Conectamef del Ministerio de Economía y Finanzas.

Segundo objetivo específico

Realizar plan para concienciar en forma virtual a los usuarios Conectamef del Ministerio de Economía y Finanzas.

Tercer objetivo específico

Implementar kit de concienciación de INCIBE a los usuarios Conectamef del Ministerio de Economía y Finanzas.

Cuarto objetivo específico

Definir tipos de amenazas sobre la Ingeniería Social.

Quinto objetivo específico

Definir tipos de Vulnerabilidades sobre la Ingeniería Social.

1.6 Justificación del Trabajo

La justificación principal según el objetivo del presente trabajo es concienciar a los usuarios conectamef del Ministerio de Economía y Finanzas a cerca de las amenazas y vulnerabilidades que conlleva la Ingeniería Social. Pues el usuario es el eslabón más débil, la pieza más importante que todo hacker malicioso puede vulnerar solo con la psicología.

Teóricamente hablando se sabe que las nuevas tecnologías dan pie a amenazas de nivel informático y de robo de información. Muchos usuarios saben que existe el robo de información gracias a las tecnologías, pero por lo general no hacen mucho caso de ello, puede ser porque si roban la información de la empresa no sería algo tan preocupante para ellos. Es por ello que en las capacitaciones y el ataque dirigido propuesto por INCIBE se realizara una Ingeniería Social para que vean los peligros de divulgar información valiosa que también los podría afectar a ellos y en sus vidas personales es por ello que se plantea poder concienciarlos a cerca de sus acciones al momento que se pueda presentar una amenaza.

Enfocándonos en el ámbito metodológico del presente trabajo de investigación se está utilizando una pre encuesta y una simulación post encuesta para poder medir el impacto de los usuarios Conectamef del Ministerio de Economía y Finanzas a fin de ver que tan concienciados están ellos con temas de seguridad en Ingeniería Social. El plan contiene varias etapas de intervención del usuario, lo cual conlleva a un mejor aprendizaje sobe el tema, dándole mejor retención de la información.

En lo que respecta a la utilidad práctica de la presente investigación se considera la importancia de usar el plan de concienciación para ayudar a los usuarios a no ser vulnerables a causas de amenazas que se podrían presentar al no estar informados sobre la Seguridad en Ingeniería Social, es por ello que se utilizarán ambas variables las cuales favorecerán una con otra para poder

retroalimentar a los usuarios con los temas importantes acerca de la Seguridad informática.

1.7 Delimitación

Actualmente el Ministerio de Economía y Finanzas están compuesto por unos 3500 trabajadores aproximadamente pensando que los usuarios más vulnerables a las amenazas de ingeniería social son los usuarios del Conectamef, los cuales oscilan entre unos 234 colaboradores, se plantea que dichos usuarios necesitan ser capacitados sobre las formas de seguridad de Ingeniería Social, siendo así que se trabajará exclusivamente con ellos ya que en el presente trabajo de investigación se podrá observar que son ellos los más expuestos a ser atacados por las amenazas del factor humano y Web que tienen la Ingeniería Social.

CAPITULO II: MARCO TEÓRICO-CONCEPTUAL

2.1. Antecedentes de la Investigación

Para poder observar diferentes puntos de vista, se ha extraído ideas de otros trabajos de investigación y notas tanto en el ámbito Global como también del Perú, encontrando ideas que realimentaran las fuentes de este trabajo de concienciación a usuarios sobre los ataques de Ingeniería Social aplicados a los Conectamef del Ministerio de Economía y Finanzas.

Un Plan de Concientización nos otorgaría beneficios como la percepción del usuario al saber que ser infectado puede ser tan rápido como hipotéticamente dicho un abrir y cerrar de ojos, aprenderá que realizando acciones inadecuadas podría infectar al Ministerio de Economía y Finanzas y a ellos mismos. Y ese aprendizaje será mediante una técnica de capacitación y técnicas de ataques simulados.

2.1.1. Trabajos Previos Internacionales

Roque, Juárez (2018), Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios, Guadalajara México. Investigación realizada para explorar las deficiencias en seguridad informática que poseen los alumnos universitarios de licenciatura en informática en sus primeros semestres, y para evaluar preliminarmente el efecto que tendría un programa de capacitación y concientización diseñado para ellos. Se realizó un estudio experimental de un solo grupo con pre-test y post-test siendo la encuesta su forma de medición con el software SPSS para analizar los datos obtenidos. En esta investigación fueron seis alumnos de segundo semestre de la Licenciatura en informática (LI) de la Facultad de Comercio, Administración y Ciencias Sociales (FCACS) de la Universidad Autónoma de Tamaulipas (UAT), en Nuevo Laredo. El estudio se realizó en el periodo de clases de primavera del año 2017, donde había 27 alumnos registrados en el segundo semestre de LI en la FCACS. Se realizó en un evento formativo en modalidad de conferencia. Se concluyó en el trabajo de investigación que los estudiantes universitarios de la carrera de informática sabían poco acerca del término de phishing y las consecuencias de

este ataque. También mencionaron que la implementación de un programa permanente con los objetivos de capacitar y concientizar a los estudiantes universitarios acerca de temas de seguridad informática sería benéfica para crear comunidades más seguras con usuarios más protegidos y con mayor conciencia de sus acciones.

Flórez, Méndez (2017) Estudio de Ingeniería Social en el uso de las Redes Sociales Proyecto de Grado en la Universidad Nacional Abierta y a distancia Escuela de Ciencias Básicas, Tecnología e Ingeniería Especialización En Seguridad Informática Bogotá D.C. Colombia en el año 2017. La problemática es ver cuáles son las vulnerabilidades más comunes en la seguridad de la información y que hacen factible un ataque de Ingeniería Social al personal de la Universidad del Valle y también las técnicas más utilizadas para el robo de información de las redes sociales de la universidad referente a la Ingeniería Social. El objetivo es Realizar un estudio sobre ingeniería social, en el uso de las redes sociales, aplicando metodologías, técnicas, para obtener el estado de vulnerabilidad de las personas en la sede de la universidad del valle. Es una investigación de tipo descriptivo y se puede enmarcar, según los criterios de la UNAD, dentro de la línea de investigación de Gestión de Sistemas, y cuya temática es la Auditoria de Sistemas. A través de esta investigación se pretendió determinar cuáles son las vulnerabilidades y en sus áreas de trabajo frente a las metodologías, estrategias o técnicas de las que se valen los ingenieros sociales para obtener acceso a información sensible. Como población y muestra, a la vez, para esta labor investigativa se tomó el 100% de la planta administrativa y estudiantil, incluyendo algunos docentes de tiempo completo que cumplen esta función dentro la sede de la Universidad del Valle de Cali - Colombia, puesto que su ambiente laboral permite un fácil acceso a información sensible o a las computadoras a cargo del personal en mención por parte de 66 agentes externos o no permitidos. Se utilizaron técnicas de recolección de datos como la observación, encuestas y entrevistas. 167 asistentes respondieron al cuestionario Se utilizó una hoja de cálculo, donde utilizaron tablas dinámicas para realizar el análisis de datos recogidos. Los autores concluyeron que personal administrativo, profesores y

personas ajenas de la universidad, se pudo conocer que tienen poco conocimiento o desconocimiento acerca de la Ingeniería Social así que se tiene que concientizar sobre los riesgos que existen al ser víctima de la Ingeniería Social.

Bermúdez (2015), Ingeniería Social, un factor de riesgo informático inminente en la Universidad Cooperativa de Colombia Sede Neiva Investigación para optar al título de Especialista en Seguridad Informática en el año 2015. Cuyo problema fue ver cuáles son las vulnerabilidades más comunes en la seguridad de la información y que hacen factible un ataque de ingeniería social al personal del área administrativa de la Universidad Cooperativa de Colombia sede Neiva. El objetivo de su investigación fue Identificar las vulnerabilidades frente a los ataques de Ingeniería Social de las diferentes zonas, dependencias, plataformas y personal administrativo de la Universidad Cooperativa de Colombia Sede Neiva, ejecutando una serie de pruebas y aplicando métodos de recolección de datos, para disminuir el riesgo y la probabilidad de fallas en la seguridad de la información. Se utilizó un diseño metodológico preliminar con tipo de investigación descriptiva. Los métodos de recolección de información fueron con los procesos de observación, y también a través de la aplicación de cuestionarios con preguntas cerradas y entrevistas no estructuradas. Como población y muestra se tomó 100% de la planta administrativa de la Universidad Cooperativa de Colombia Sede Neiva y 110 asistentes respondieran el cuestionario, incluyendo al personal de servicios generales, manteniendo, auxiliares, jefes y directivos de todas las áreas, y docentes de tiempo completo. Se excluyó a los docentes de medio tiempo y catedráticos porque, aunque hacen parte de la institución, son un sector muy pequeño y no permanecen 100% del tiempo en las instalaciones de la universidad la medición de los datos se realizaron con una Hoja de Cálculo en Excel. El autor concluyo que las vulnerabilidades encontradas, no solo a través de la observación y la experiencia, sino también, con los resultados de la encuesta, son bastantes. Como primera medida no existe un plan o programa de capacitación permanente a los empleados de la universidad respecto a los temas de la seguridad informática y de la información. Y que ello se puede minimizar estableciendo dicho programa de capacitación permanente para todos sus trabajadores de la universidad, en el

que el tema central sea la seguridad informática y de la información. Este deberá estar diseñado por parte del departamento de gestión tecnológica y apoyada por las directivas de la sede.

2.1.2. Trabajos Previos Nacionales

Aguilar, De la Cruz (2015) Implementación de una solución de Hacking Ético para mejorar la seguridad en la infraestructura informática de La Caja Municipal De Sullana - Agencia Chimbote tesis para optar el título profesional de Ingeniero de Sistemas e Informática en la Universidad Nacional del Santa Facultad de Ingeniería Escueta Académico Profesional de Ingeniería de Sistemas e informática en Nuevo Chimbote Perú del año 2015. Cuyo problema es ver de qué manera la Implementación de una Solución de Hacking Ético mejorará la Seguridad en la Infraestructura Informática de la Caja Municipal de Sullana - Agencia Chimbote siendo Su objetivo mejorar la seguridad en la Infraestructura Informática de la Caja Municipal de Sullana - Agencia Chimbote a través de la implementación de una Solución de Hacking Ético. El Diseño de Investigación a utilizar fue de preprueba - postprueba con un solo grupo que corresponde a la muestra. Utiliza el método experimental. La población la constituye la infraestructura informática de la Caja Municipal de Sullana - Agencia Chimbote que está constituida por 20 Computadoras de Escritorio y 02 Servidores y la muestra son 05 computadoras y 02 servidores del área de préstamos. Se utilizó prácticas de laboratorio, observación, revisión bibliográfica, entrevista y encuesta. Concluyeron que la implementación de la Solución de Hacking Ético mejora a seguridad en la Infraestructura Informática de la Caja Municipal de Sullana - Agencia Chimbote, ya que se adelanta a posibles fallas o problemas de seguridad, previniendo desarrollar controles de seguridad con lo cual optimizan los sistemas físicos y lógicos de la entidad.

Dioppe (2015) Seguridad Informática, informe de trabajo práctico de suficiencia para optar el título profesional de ingeniero de sistemas e informática con mención en la facultad de Ingeniería De Sistemas e Informática de la Universidad Nacional de la Amazonía Peruana. Iquitos Perú año 2015. El

problema es el actual comprender acerca de la Seguridad Informática en las organizaciones y las decisiones que la alta gerencia pueda tomar respecto a ello. Realizar una revisión general de los conceptos relacionados a la seguridad informática, mostrando su clasificación, políticas, mecanismos, procedimientos y la aplicación de estándares dentro de las organizaciones. Se concluyó que Debido al constante crecimiento de la tecnología a nivel mundial, el ataque y las amenazas hacia la seguridad informática son cada vez más frecuentes provocando que las organizaciones requieran implantar políticas, normas, procedimientos con el fin de reducir el impacto de las amenazas y ataques. y también que Debido a las constantes amenazas en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

Alcántara (2015) Guía de Implementación de la Seguridad basado en la Norma Iso/Iec 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del Norte P.N.P en la Ciudad De Chiclayo Tesis para optar El Título de Ingeniero de Sistemas y Computación Presentada a la Facultad de Ingeniería de la Universidad Católica Santo Toribio de Mogrovejo, Chiclayo Perú en el año 2015. El problema es sobre la falta de importancia a la auditoria de sistemas que la mayoría de las empresas le dan siendo el objetivo es identificar las causas de los problemas existentes en los sistemas de información y a su vez las áreas de oportunidad que puedan encontrarse, identificando causas y soluciones a problemas específicos de los sistemas de información, que pueden estar afectando a la operación y a las estrategias del negocio; así como las acciones preventivas y correctivas necesarias para mantener a los sistemas de información confiables y disponibles. El tipo de investigación es Tecnológica Aplicada. La población de la presente investigación lo constituirá los 30 trabajadores de la Comisaria del Norte de la PNP de la ciudad de Chiclayo, que además son efectivos policiales. Según Hernández y Fernández 1991: Debido a que la población es muy pequeña (n<=30) se tomarán a los 30 trabajadores de la Entidad mencionada. La selección de la muestra será en base a un muestreo no probabilístico, de tipo intencional o por

conveniencia; que para el caso la muestra será el total de la población. Para la obtención de dicha información y recolección de datos se consideró conveniente el uso de las técnicas de recolección de datos tales como encuestas, entrevistas, así como fichas de observación. Es una Investigación Cuasi-Experimental. Con el Plan de Capacitación y Concienciación puesto en marcha en la Institución, se logró incrementar el conocimiento, y su vez mejorar el nivel de capacitación para el personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la institución, teniendo como resultado personal comprometido con la seguridad en favor de la institución. y también Con la Guía de Implementación, se logró incrementar el nivel de la seguridad en las aplicaciones informáticas de la institución policial, y esto se vio reflejado en el incremento de políticas de seguridad que fueron puestas en marcha que beneficiaron a la institución y ayudaron a incrementar el nivel de seguridad en la misma.

2.2. Bases Teóricas

2.2.1. Importancia de concienciar al usuario en Seguridad de Ingeniería Social

Las personas que trabajamos en tecnología estamos un poco más familiarizadas sobre las posibles amenazas que existen en las redes de comunicación pero otras áreas muchas veces no lo están, lo cual en su mayoría dificulta el proceso de prevención informático que se le pueda asignar a una empresa. Por ello se espera poder plantearle al personal sobre las vulnerabilidades que puedan existir en la actualidad y en un futuro, las técnicas actuales que realizan los hackers sociales en ingeniería informática y como podrían prevenirse de esos ataques cibernéticos.

Una de las personas más reconocidas en el mundo informático es Kevin Mitnick, quien se caracterizó por ser uno de los pioneros en técnicas de Ingeniería Social. Mitnick considera que el factor que determina la seguridad del hardware y el software es el factor humano, es decir, el usuario. Este es quien se encargará de interpretar las políticas de seguridad correctamente y buscará que se respeten.

Considerando que es posible fallar en este aspecto y que un ataque de Ingeniería Social puede tomar desprevenido a cualquier usuario, y teniendo en cuenta también que incluso es posible que sea llevado a cabo solamente con ayuda de un teléfono, Mitnick establece 4 principios comunes que aplican a todas las personas:

- Todos queremos ayudar.
- Siempre, el primer movimiento hacia el otro, es de confianza.
- Evitamos decir NO.
- A todos nos gusta que nos alaben.

Estos métodos de manipulación, basándose en la confianza del usuario, son los que conducen a engaños como phishing, páginas con códigos maliciosos alojados esperando infectar a sus víctimas, o robo de información, y otras técnicas de manipulación donde el usuario es quien sin darse cuenta está cayendo en este tipo de estafas las cuales pueden perjudicar a la empresa pero también al mismo usuario con el robo de su información.

2.2.2. Formas para realizar un Plan de Concientización al usuario

Roque y Juárez (2018), afirman que la concienciación mediante interactivos materiales ayuda a los usuarios a ver los beneficios de aprender las medidas de seguridad y de lo importante de seguir las reglas para lograrlo. Comentan que para lograrlo hay que incluir seminarios, entrenamientos en línea, vídeos, correos electrónicos, posters y juegos. En un proceso continuo y a largo plazo pero sin abrumar al usuario.

INCIBE (Instituto Nacional de Ciberseguridad en España, 2017) comenta que las personas que gestionan la información en las empresas son los empleados, siendo ellos los encargados de gestionar, procesar, almacenar, modificar, transmitir y eliminar la información siendo los principales en el funcionamiento de la empresa. Entonces mencionan que existen riesgos por desconocimiento y

desinformación ante cualquier situación crítica.

2.2.2.1. Concienciar de forma Presencial

Pendergast (como se citó en Marín, 2018), expone mediante un análisis exhaustivo diciendo que se tiene que capacitar a los usuarios para su concienciación sobre las vulnerabilidades de la ingeniería Social. Una forma para poder interactuar con el usuario presencialmente es por medio de las capacitaciones en el cual se pueden exponer la importancia de prevención sobre la ingeniería social pudiendo así dar otro enfoque sobre este tema a los asistentes de estos seminarios.

2.2.2.2. Concienciar de forma Virtual

Belloch (S/F), de la Unidad de Tecnología Educativa de la Universidad de Valencia España indica que un aprendizaje de forma virtual tiene infinidad de ventajas pues cuenta con la flexibilidad a la hora de perfilar enfoques de instrucción y aprendizaje. Pues tiene calidad comunicacional con posibilidades de comunicación sincrónica y asincrónica entre todas las personas involucradas en la acción formativa. Incorporando elementos que faciliten el conocimiento como:

- Correos electrónico y mensajería interna.
- Videos con material formativo.
- Posters.
- Intranet.

2.2.2.3. Concienciar con Ataque dirigido

INCIBE nos dice que “Podemos formar a nuestros empleados por medio de la concienciación en materia de Ciberseguridad”. Ellos nos brindan un Kit de Concienciación el cual se enfoca en etapas para la formación a los empleados y dichas etapas se muestran en la siguiente imagen:

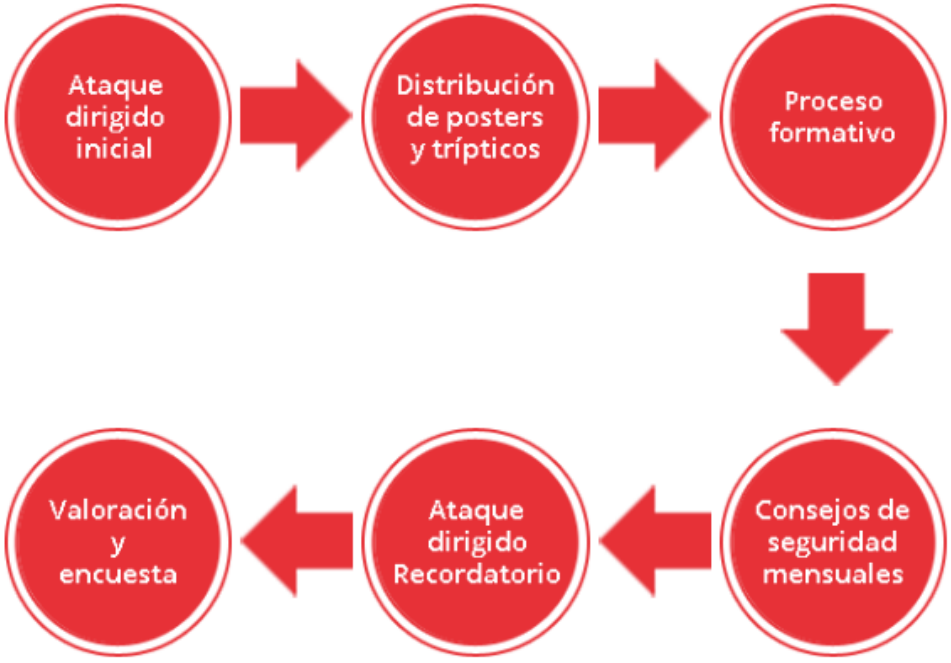


Figura 2. Concienciar al usuario
Tomado de https: //www.incibe.es/protege-tu-empresa/kit-concienciacion, por INCIBE (Instituto de Ciberseguridad en España).

Al ver que un gran número de infecciones a través del malware viene como ficheros adjuntos a los correos electrónicos recibidos por los usuarios el instituto Nacional de Ciberseguridad de España (INCIBE) recomienda realizar un ataque dirigido para poder concienciar al usuario de las consecuencias que se puedan generar a través de abrir dichos correos.

2.2.3. Seguridad en Ingeniería Social

Actualmente hemos crecido inmensamente en cuanto a tecnología y medios de comunicación, lo que ha llevado a personas muy capacitadas con conocimientos altos en informática aprovechen de ello para delinquir y usar sus habilidades para poder realizar actos no autorizados obteniendo lo que deseen. Para poder entender como poder minimizar el impacto negativo provocado por ataques existen procedimientos y mejores prácticas para así poder ver estrategias de seguridad efectivas para mitigar el riesgo que esta pueda tener.

Una de las mejores formas de ver cómo asegurar nuestra organización es pensar como el atacante dijo Mueres (2009), en Evil Fingers portal comunitario sobre seguridad informática mencionando también que para tener la mentalidad del atacante hay que comprender y analizar la forma en que los atacantes llevan a cabo un ataque y estas se dividen en 5 fases expuestas en la siguiente imagen:

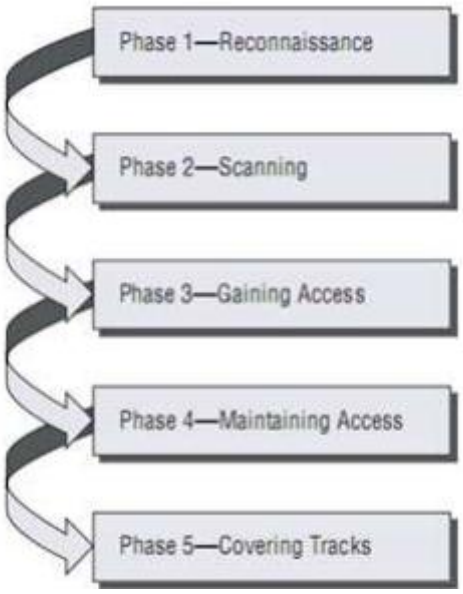


Figura 3. Fases del Ataque Informático
Tomado de
https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Mueres indica que la fase 1 es Reconnaissance (Reconocimiento) el cual es para obtener la información de la víctima, usualmente en este paso se usa la Ingeniería Social, Fase 2: Scanning (Exploración) en el cual se usa la recolección obtenida en el reconocimiento para poder sacar información del sistema de la víctima, Fase 3: Gaining Access (Obtener acceso) es en el cual empieza a usar la información recolectada en las primeras dos fases y aprovechando las vulnerabilidades que encuentre después con ello sigue las fase 4 Maintaining Access (Mantener el acceso) para poder ver la forma de poder acceder a lo que necesite las veces que desee para después poder ver la forma de borrar todas las huellas para que no puedan identificar que hubo algún cambio en el sistema y esa

fase es Covering Track (Borrar huellas).

2.2.3.1. Vulnerabilidad

Mueres también menciona que los atacantes pueden usar los tres elementos fundamentales de la seguridad (confidencialidad, integridad y disponibilidad) para poder explotar las vulnerabilidades del sistema. INCIBE también menciona en su página web que la vulnerabilidad en términos de informática es una debilidad que pone en riesgo la seguridad haciendo que el atacante pueda comprometer los tres elementos de seguridad por ello es importante identificarlas para poder minimizar esos agujeros. Ojeda (2018) menciona en página web (GB advisors es un socio comercial que da soluciones de evaluación del Riesgo, Vulnerabilidad y más) que existen dos tipos de Ingeniería Social por el factor humano y por la Web explicando estas vulnerabilidades a continuación:

2.2.3.1.1. Mediante el Factor Humano

Los ataques de ingeniería social basados en personas para extraer la información que necesiten se ayudan de las emociones humanas para logras su cometido usando teorías psicológicas de motivación, excitación, incentivos y de opciones entre otras para mover sentimientos complejos (compasión; amor; miedo; curiosidad; necesidad de protección o de pertenecer a un grupo) y/o necesidades primarias (sexo; hambre; sueño; sed; etc.) dijo Ojeda pues los seres humanos compartimos por lo general los mismo miedos, debilidades y necesidades entonces toman ventaja sociales de esas premisas para poder suplantar la identidad de alguna persona conocida y obtener la información que necesiten siendo las personas más vulnerables las más propensas en caer en estos engaños.

2.2.3.1.2. Mediante el Factor Web

El ser humano puede ser engañado muy fácilmente por medio de la vista y una

de ellas es por la Web, uno de los métodos más comunes es suplantando la identidad de alguna página web haciéndola muchas veces idéntica y logrando engañar al usuario para que ingrese y llene los datos o infectándose en ella, pues muchas veces se envían correos también de páginas reconocidas para que la carnada en este caso el usuario caiga y de clic a un link malicioso o proporcione información sensible de la institución para los fines que desee el ciberdelincuente.

2.2.3.2. Amenaza

Una amenaza es la forma de aprovechar una vulnerabilidad poniendo en riesgo a la organización por diferentes tipos de ataques y así atentar con la seguridad del sistema aprovechando las brechas vulnerables que tiene dicha institución con el fraude, robo u virus. Estas amenazas pueden ser tanto internas como externas en el ámbito de la seguridad de Ingeniería Social hay algunos tipos de métodos que pueden amenazar a la institución siendo estos el Vishing, Spoofing, USB, Spam, Phising entre otros.

2.2.3.2.1. Phissing

El phishing es tratar de robar información suplantándose por otra persona o entidad. Los casos más conocidos son los clásicos correos de una entidad bancaria pidiendo ingresen la clave en la página web o aceptando algo y el atacante tendrá acceso inmediato a su cuenta del banco y utilizar esa información como mejor le parezca. Por lo general no va enfocado a una persona en particular sino que es un mensaje masivo el cual un porcentaje podría caer en la trampa, es también relacionado como spam.

Algunas de las técnicas que se utilizan en el phishing son:

- Imitar la imagen, logotipo de la entidad o persona a suplantar.
- Engañar al usuario con direcciones de páginas web muy parecidas a las originales puede ser cambiado solo con una letra. Pero al entrar a la página se

puede observar que es tal cual a la original. (Los suplantadores hacen una copia exacta de la original).

- Amenazan al usuario con cancelar sus cuentas o que pasará algo malo sino entregan sus claves de acceso.

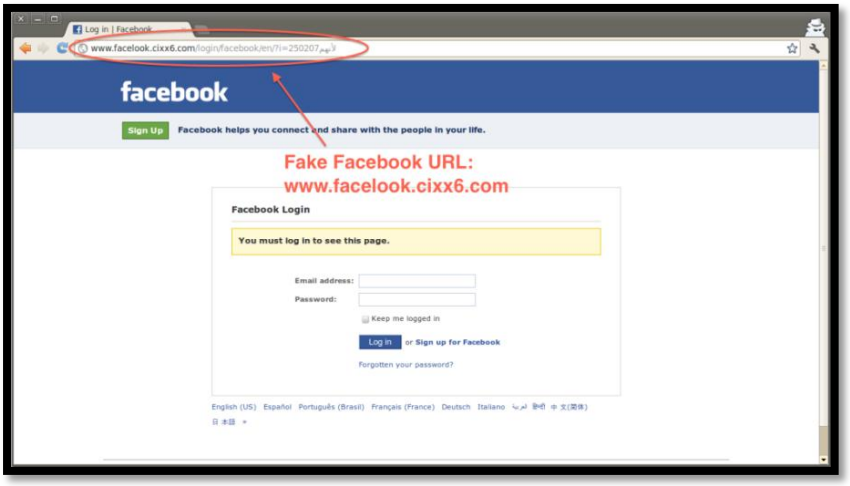


Figura 4. Amenaza Phising
Tomado de http://www.cronicahacker.com/2015/10/4-maneras-conseguir-una-contrasena-facebook.html

2.2.3.2.2. Vhising

Es una variación del phishing pero con voz VoIP realizados principalmente en mensajería que también es llamado smishing o por voz solicitando la clave de sus cuentas haciéndose pasar por otras personas u entidades.

Figura 5. Amenaza Vishing
Tomado de http://www.carmelowalsh.com/2015/07/phishing-and-vishing-attacks-are-up/

2.2.3.2.3. Spoofing

Es como el phising un suplantador de identidad, pero este actúa diferente. Tiene que ir de la mano con otro método para robar información de claves de cuentas. Una vez tenga la información de la cuenta, la usara para enviar documentación infestada u otros datos para dañar a la organización. EL Spoofing tiene variantes las cuales son Spoofing IP el cual suplanta una IP falsa y la usa, Spoofing web suplanta la página web para que la información le pueda llegar ahí, Spoofing mail como el nombre lo dice nos habla de la suplantación de unos correos para poder acceder a algún dato importante para la empresa.

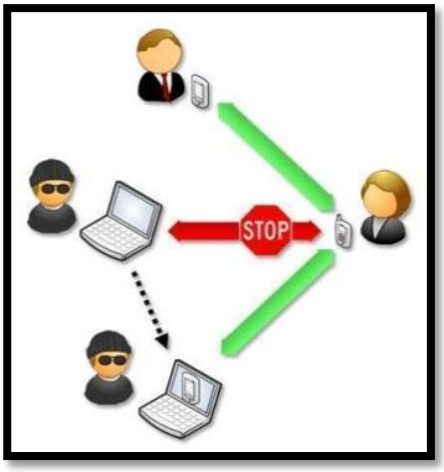


Figura 6. Amenaza Spoofing
Tomado de https://www.ecured.cu/Ataque_de_autenticaci%C3%B3n

Actualmente existen varias herramientas de seguridad que hace difícil que los atacantes puedan acceder a los sistemas y eso es de gran ayuda pero no si el atacante utiliza las debilidades de la persona con Ingeniería Social esta podría poner en riesgo la organización. Por medio del engaño el ser humano podrá caer ante un ataque de ingeniería social siendo esta una amenaza al sistema pues el ser humano es vulnerable.

Figura 7. Riesgo

Tomado de https: //www.incibe.es/sites/default/files/contenidos/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian/riesgo.png, por INCIBE (Instituto de Ciberseguridad en España).

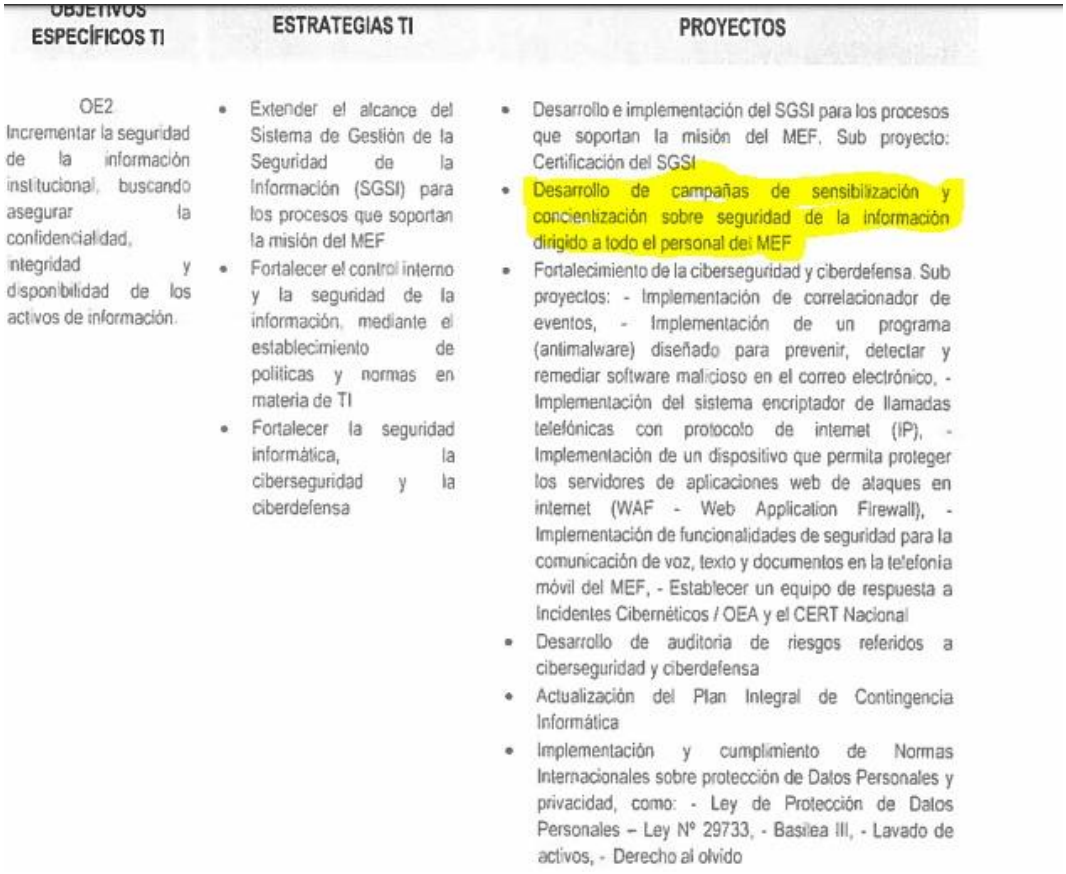
CAPITULO III METODOLOGIA DE LA GESTION DEL CAMBIO

3.1 Tipos de Gestión del Cambio

La gestión de cambio es como su palabra lo dice, un cambio, el cual en este caso se realiza en el ámbito privado y público teniendo un hecho inherente para la mejora de la organización, pues con ello se mejoran aspectos que no están funcionando adecuadamente, se corrigen los errores y se aprende de ellos para su mejoría. En el Perú La Política Nacional de Modernización de la Gestión Pública al 2021 es el principal instrumento orientador de la modernización de la gestión pública del país el cual tiene como objetivo orientar, articular e impulsar a las entidades públicas del proceso de modernización hacia una gestión pública en bienestar del ciudadano teniendo tres ejes transversales y cinco pilares centrales para ello como se muestra en la siguiente imagen:

Figura 8. Proceso de Gestión del cambio en la Gestión Pública (PNMGP 2021, p.35)

Una de las importancias de la gestión del cambio en las entidades del estado se puede ver en la Ley Servir que tiene como objetivo fortalecer la gestión del empleo e incrementar los niveles de eficacia y eficacia del funcionario público para darle un buen servicio al ciudadano aplicando nuevas reglas sobre la capacitación, el mérito, la evaluación del desempeño entre otros. Siendo está política una de los principales en la reforma del servicio civil meritocrático.



OBJETIVOS ESPECÍFICOS TI	ESTRATEGIAS TI	PROYECTOS
OE2 Incrementar la seguridad de la información institucional, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información.	• Extender el alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) para los procesos que soportan la misión del MEF • Fortalecer el control interno y la seguridad de la información, mediante el establecimiento de políticas y normas en materia de TI • Fortalecer la seguridad informática, la ciberseguridad y la ciberdefensa	• Desarrollo e implementación del SGSI para los procesos que soportan la misión del MEF. Sub proyecto: Certificación del SGSI • Desarrollo de campañas de sensibilización y concientización sobre seguridad de la información dirigido a todo el personal del MEF • Fortalecimiento de la ciberseguridad y ciberdefensa. Sub proyectos: - Implementación de correlacionador de eventos, - Implementación de un programa (antimalware) diseñado para prevenir, detectar y remediar software malicioso en el correo electrónico, - Implementación del sistema encriptador de llamadas telefónicas con protocolo de internet (IP), - Implementación de un dispositivo que permita proteger los servidores de aplicaciones web de ataques en internet (WAF - Web Application Firewall), - Implementación de funcionalidades de seguridad para la comunicación de voz, texto y documentos en la telefonía móvil del MEF, - Establecer un equipo de respuesta a Incidentes Cibernéticos / OEA y el CERT Nacional • Desarrollo de auditoria de riesgos referidos a ciberseguridad y ciberdefensa • Actualización del Plan Integral de Contingencia Informática • Implementación y cumplimiento de Normas Internacionales sobre protección de Datos Personales y privacidad, como: - Ley de Protección de Datos Personales – Ley N° 29733, - Basilea III, - Lavado de activos, - Derecho al olvido

Figura 9. Plan Estratégico de Tecnologías de la Información 2017 - 2019 (RM469_2017EF44, p.16)

En el Peti también podemos observar que el porcentaje del personal capacitado en Seguridad de la Información para incrementar la seguridad institucional, buscando la confidencialidad, integridad y disponibilidad de los activos de información estuvo en un 55% en el 2017, en el 2018 65% y 75 % en el 2019 siendo ello porcentajes semestrales que realizan para poder ver el avance de los objetivos planteados así como se observa en la siguiente imagen:

Tabla N° 8: Indicadores

OBJETIVO ESPECÍFICO TI	INDICADOR	META 2017	META 2018	META 2019
OE1. Consolidar la gobernanza de tecnologías de la información, estableciendo procesos que aseguren el cumplimiento de objetivos y metas institucionales	Porcentaje de clientes afirman estar satisfechos	-	95%	97%
	Índice de atenciones realizadas	-	97%	98%
	Porcentaje de cumplimiento de los SLA	-	97%	98%
	Porcentaje de servicios de TI con estándares internacionales de calidad	-	85%	90%
	Eficacia en el cumplimiento de los proyectos de TI	95%	96%	97%
	Porcentaje de brechas cubiertas de capacitación	-	85%	90%
	Eficiencia en el uso de los recursos	95%	96%	97%
	Lineamientos de TI aprobados	2	3	3
	Herramientas de gestión de TI implementadas	-	2	2
OE2. Incrementar la seguridad de la información institucional, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información	Porcentaje de controles implementados	-	97%	98%
	Eventos de seguridad de la información realizados	1	2	2
	Porcentaje del personal capacitado en seguridad de la información	55%	65%	75%
OE3.	Tiempo máximo de recuperación de la continuidad operativa[4] de los servicios críticos	30'	29'	28'

Figura 10. Plan Estratégico de Tecnologías de la Información 2017 - 2019 (RM469_2017EF44, p.33)

3.2 Planificación Operativa para instrumentar el cambio

3.2.1 Diagnóstico Inicial

3.2.1.1. PROBLEMÁTICA ACTUAL

La realidad problemática de la actividad de informática de la Oficina General de la Información - OGTI del Ministerio de Economía y Finanzas – MEF, se describen bajo el contexto de FODA (Fortalezas, Oportunidades, Debilidades y Amenazas), que son las siguientes:

3.2.1.1.1. FORTALEZAS

1. La OGTI brinda servicios a través de un catálogo de servicios aprobado.
2. Las áreas de negocio están sensibilizadas en el uso de buenas prácticas de seguridad de la información.
3. Existencia de un marco normativo que regula la administración y uso de las TI en el Ministerio de Economía y Finanzas aprobado.
4. La OGTI cuenta con procesos definidos de nivel 1 y 2.
5. Se cuenta con sistemas de alcance nacional (Sistemas Transversales).

3.2.1.1.2. DEBILIDADES

1. Incipiente adopción de estándares internacionales y buenas prácticas de tecnologías de la información.
2. La gran variedad de herramientas y plataformas desde donde se desarrolla y entrega servicios de TI originan un alto consumo de recursos.
3. Escaso registro de requerimientos que permita medir la capacidad operativa de la OGTI en relación a la demanda de servicios de TI.
4. Falta de mecanismos de validación o medición de la calidad de los servicios brindados de TI.
5. Existencia de áreas de TI paralelas a la OGTI.

3.2.1.1.3. OPORTUNIDADES

1. Existen una gran oferta de proveedores de tecnología en el mercado que resultaría en beneficio al fortalecimiento de la OGTI.
2. Interés y apoyo de la Alta Dirección y de los organismos internacionales para el desarrollo tecnológico del Ministerio de Economía y Finanzas.
3. La OGTI integra el Comité de Coordinación de la Administración Financiera del Sector Público.
4. Interconexión de las distintas entidades del Estado con el Ministerio de Economía y Finanzas.
5. Las regulaciones a nivel de Estado en materia de TI exigen a las entidades la adopción de buenas prácticas, por lo tanto contribuyen a brindar un mejor servicio al ciudadano.
6. La OGTI ha logrado consolidarse como principal soporte de las entidades públicas, sobre los sistemas transversales que apoyan los procesos económico y financiero.

3.2.1.1.4. AMENAZAS

1. Existencia de riesgos asociados en los procesos de contrataciones que impactan negativamente en el logro de los objetivos.
2. La falla de acceso a internet o su baja calidad, en algunas zonas al interior del país dificulta la transmisión de la información y por ende desmedra la calidad del servicio a las entidades.
3. Riesgo de actos indebidos de funcionarios.
4. Existencia de hackers que constantemente intentan vulnerar los sistemas informáticos de las entidades del Estado por lo que, de produciré un ataque a los sistemas transversales podría afectar las operaciones en el sector público.
5. La edificación en donde se encuentra el Centro de Cómputo principal del Ministerio de Economía y Finanzas presenta vulnerabilidades en su estructura, que pondrían en riesgo inminente la salud y vida del personal ante un sismo de gran intensidad.

Con lo antes descrito podemos ver que tenemos algunas deficiencias en cuestión a seguridad informática en el Ministerio de Economía y Finanzas siendo uno de los principales la cantidad de amenazas que asechan en el Ministerio de Economía y Finanzas como se puede ver en la siguiente imagen vemos la cantidad de ataques que el Ministerio recibió en el año 2018 siendo en su gran mayoría bloqueadas por las herramientas de seguridad del área de Sistemas, lo cual es una buena forma de contrarrestar la amenazas que tienen actualmente el área de TI.

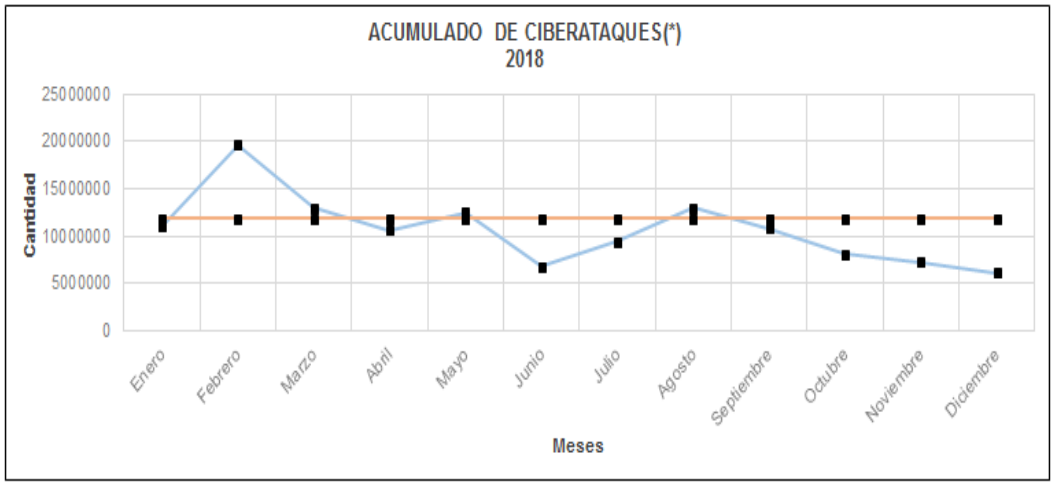


Figura 11. Ciberataques Ministerio de Economía y Finanzas año 2018
(Elaboración propia)

Con un promedio aproximado de millones de ataques al mes podemos ver que las herramientas de seguridad realizan el trabajo esperado al momento de bloquear dichos ataques pero que los usuarios aun así han sido víctimas de correos phishing y Spam y en su mayoría del Conectamef del Ministerio pues ellos actualmente no han recibido alguna capacitación. Entonces qué pasa si tenemos los mejores equipos de seguridad pero sin capacitar al usuario más vulnerable en estos momentos del Ministerio de Economía y Finanzas, los usuarios Conectamef, ellos podrían ser víctimas de fraude, por ello el problema de este trabajo de investigación: ¿De qué manera la concienciación a los usuarios Conectamef influye en la Seguridad de Ingeniería Social en el Ministerio de Economía y Finanzas? Siendo respondida con el siguiente gráfico.

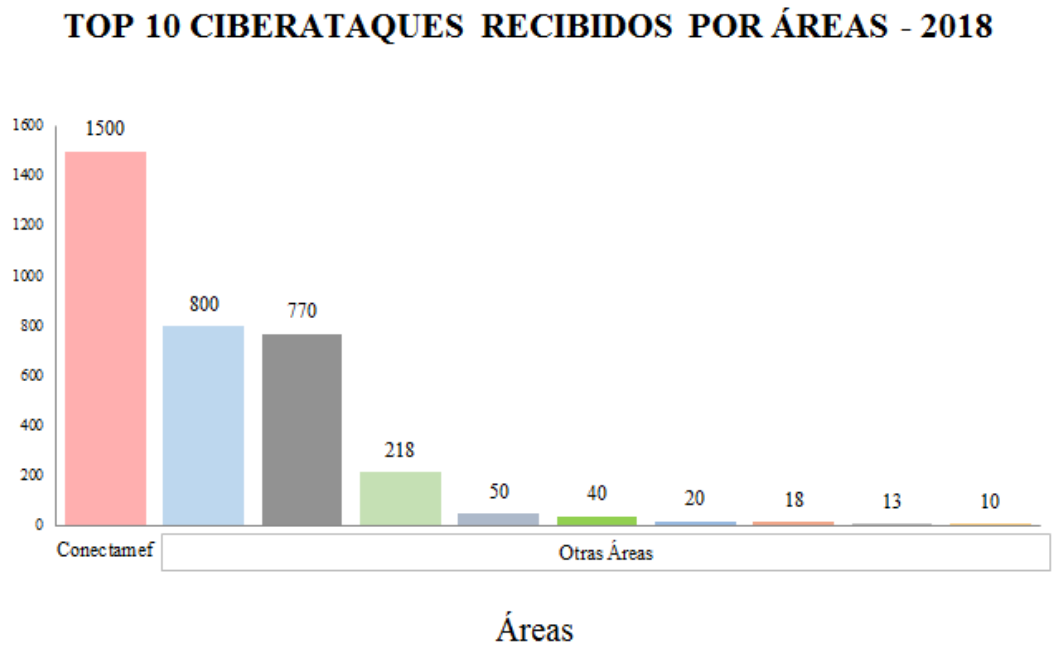


Figura 12. Ciberataques Ministerio de Economía y Finanzas por áreas año 2018
(Elaboración propia)

Los usuarios de los Conectamef son los más vulnerables ya que en el 2018 fueron los que tuvieron la mayor cantidad de ciberataques en el Ministerio de

Economía y Finanzas por ello al tener un plan de concienciación se estima esa cantidad disminuya.

3.2.2. Alcance

El objetivo principal del proyecto es realizar un plan para informar a los usuarios Conectamef del Ministerio de Economía y Finanzas para concienciarlos sobre la Seguridad de Ingeniería Social en la institución y en su vida cotidiana, en el cual se les explicará a los usuarios el porqué de la importancia de ciertos programas y restricciones en el ámbito laboral. Dicha concienciación se realizará en tres formas como se detalla en la siguiente imagen:

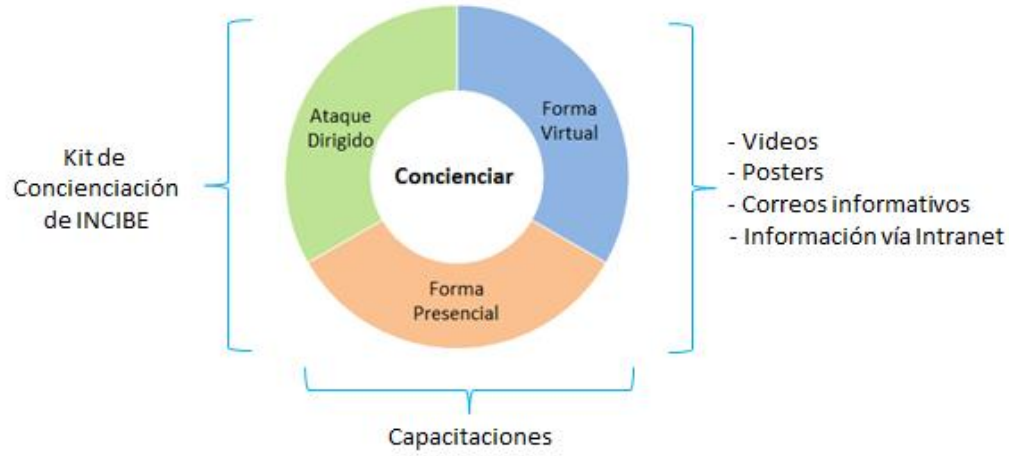


Figura 13. Formas para Concienciar a Usuarios (Elaboración propia)

Los beneficios que se alcanzarán con dicho plan de concienciación es que los usuarios sabrán que podrían ser infectados en cualquier momento por realizar acciones inadecuadas no solo afectando a las empresas sino que también a ellos mismos, así que por medio del miedo ellos trataran de tomar en práctica los consejos que se les dé. Así los usuarios Conectamef tendrían menos porcentaje de ataques cibernéticos por la Ingeniería Social.

3.2.3. Plan Operativo

1. Meta: Realizar plan para concienciar a usuarios Conectamef en la Seguridad

de Ingeniería Social del Ministerio de Economía y Finanzas.

2. Resultados Específicos: Lograr Concienciar a los usuarios Conectamef del Ministerio de Economía y Finanzas sobre la Seguridad de Ingeniería Social.

3.2.3.1. Alineamiento con el Plan Estratégico

Tabla 1

Factores que Inciden en la Gestión Estratégica de Tecnologías de la Información del Ministerio de Economía y Finanzas

FACTORES EXTERNOS	Incidencia del Factor en la Gestión Estratégica de Tecnologías de la Información del Ministerio de Economía y Finanzas
Gobierno Electrónico	"Las iniciativas de Gobierno Electrónico, en el ámbito de las Políticas Públicas, se ejecutan a través de: desarrollo de programas centrados en el ciudadano, promoción de la participación ciudadana, mejora en la prestación de los servicios mediante herramientas con alto valor tecnológico, comparación y análisis del desempeño del Gobierno Electrónico". (fuente: ONGEI - Conceptos e-Gob.) La política Nacional de Gobierno Electrónico (2013 – 2017), es la guía principal para el desarrollo dentro del campo de las Tecnologías de Información y Comunicaciones en las organizaciones del Estado.
Regulación Gubernamental	Es relevante considerar la correspondiente implantación y uso de las TIC según la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y el Instituto Nacional de Estadística e Informática (INEI).
Modernización de la Gestión Pública	El objetivo general de la Política de Modernización es orientar, articular e impulsar en todas las entidades públicas, el proceso de modernización hacia una gestión pública para resultados que impacte positivamente en el bienestar del ciudadano y el desarrollo del país. Es Importante considerar lo establecido en el Plan de Implementación de la Política Nacional de Modernización de la Gestión Pública (2013-2017)

Aplicación de “Mejores Prácticas” y Estándares.	Es importante considerar la aplicación de las denominadas “mejores prácticas” y estándares tecnológicos, en el ámbito de la gestión y operación de los servicios TIC.
Tendencias Tecnológicas	Tomar en cuenta las tendencias de Tecnologías ya que establecen el camino tecnológico a seguir y afrontar.
FACTORES INTERNOS	**I**ncidencia del Factor en la Gestión Estratégica de Tecnologías de la Información del Ministerio de Economía y Finanzas
Recursos Humanos	El éxito de un p**l**an estratégico, no termina con el proceso de redacción del documento PETI, este termina con la Implementación del mismo en el Ministerio de Economía y Finanzas, por ello, es importante considerar las capacidades del factor humano con el que se cuenta.
Cultura Organizacional	Para el éxito en la implementación del PETI en el Ministerio de Economía y Finanzas, es importante tomar en cuenta la Cultura Organizacional, a fin de atenuar las posibles resistencias a cambios.
Situación Tecnológica Actual	Las soluciones o recomendaciones a implantar como parte de este plan, tienen que considerar la herencia tecnológica que actualmente cuenta el Ministerio de Economía y Finanzas.

Fuente: Elaboración propia.

3.2.3.2. Factores Clave de Éxito – FCE

Tabla 2

Factores Clave de Éxito

Factores Clave de Éxito – FCE		Descripción del FCE	Objetivo Estratégico General del Proyecto
FCE 1	Realizar plan para concienciar en forma presencial a los usuarios Conectamef del Ministerio de Economía y Finanzas.	Se realizará en forma de capacitaciones un mecanismo de concienciación hacia los usuarios Conectamef del Ministerio de Economía y Finanzas.	Incrementar la Seguridad en Ingeniería Social mediante la concienciación a los Usuarios Conectamef del Ministerio de Economía y Finanzas
FCE 2	Realizar plan para concienciar en forma virtual a los usuarios Conectamef del Ministerio de Economía y Finanzas.	Se realizará una variedad de elementos visuales y audiovisuales para la concienciación hacia los usuarios Conectamef del Ministerio de Economía y Finanzas.	
FCE 3	Implementar kit de concienciación de INCIBE a los usuarios Conectamef del Ministerio de Economía y Finanzas.	Se realizará una serie de simulaciones de ataques dirigidos de prueba para la concienciación de los usuarios Conectamef del Ministerio de Economía y Finanzas.	

Leyenda:

- FCE más sensibles a las TIC
- FCE medianamente sensibles a las TIC
- FCE menos sensibles a las TI

Fuente: Elaboración propia

3.2.3.2.1. Potencial Contribución del Proyecto al FCE.

Es importante detallar la contribución que tendrá el proyecto en cada uno de los FCE en el Ministerio de Economía y Finanzas.

FCE 1. Realizar plan para concienciar en forma presencial a los usuarios Conectamef del Ministerio de Economía y Finanzas.

- Se realizará en forma de capacitaciones un mecanismo de concienciación hacia los usuarios Conectamef del Ministerio de Economía y Finanzas.

Apoyo en el fortalecimiento de los conocimientos acerca de la Seguridad en Ingeniería social para que así los usuarios Conectamef del Ministerio de Economía y Finanzas tengan la capacidad de poder tener una mejor respuesta ante un verdadero ataque cibernético y mitigar la vulnerabilidad del usuario que generan las amenazas de ingeniería social.

FCE 2. Realizar plan para concienciar en forma virtual a los usuarios Conectamef del Ministerio de Economía y Finanzas.

- Se realizará una variedad de elementos visuales y audiovisuales para la concienciación hacia los usuarios Conectamef del Ministerio de Economía y Finanzas.

Apoyo al fortalecimiento y capacidades de aprendizaje que se dictaron en las capacitaciones presenciales, con posters y videos que recalquen los puntos relevantes y complementen el conocimiento adquirido fomentando la curiosidad y motivación de los usuarios, para así poder consolidar los temas mencionados y no ser olvidados con el tiempo.

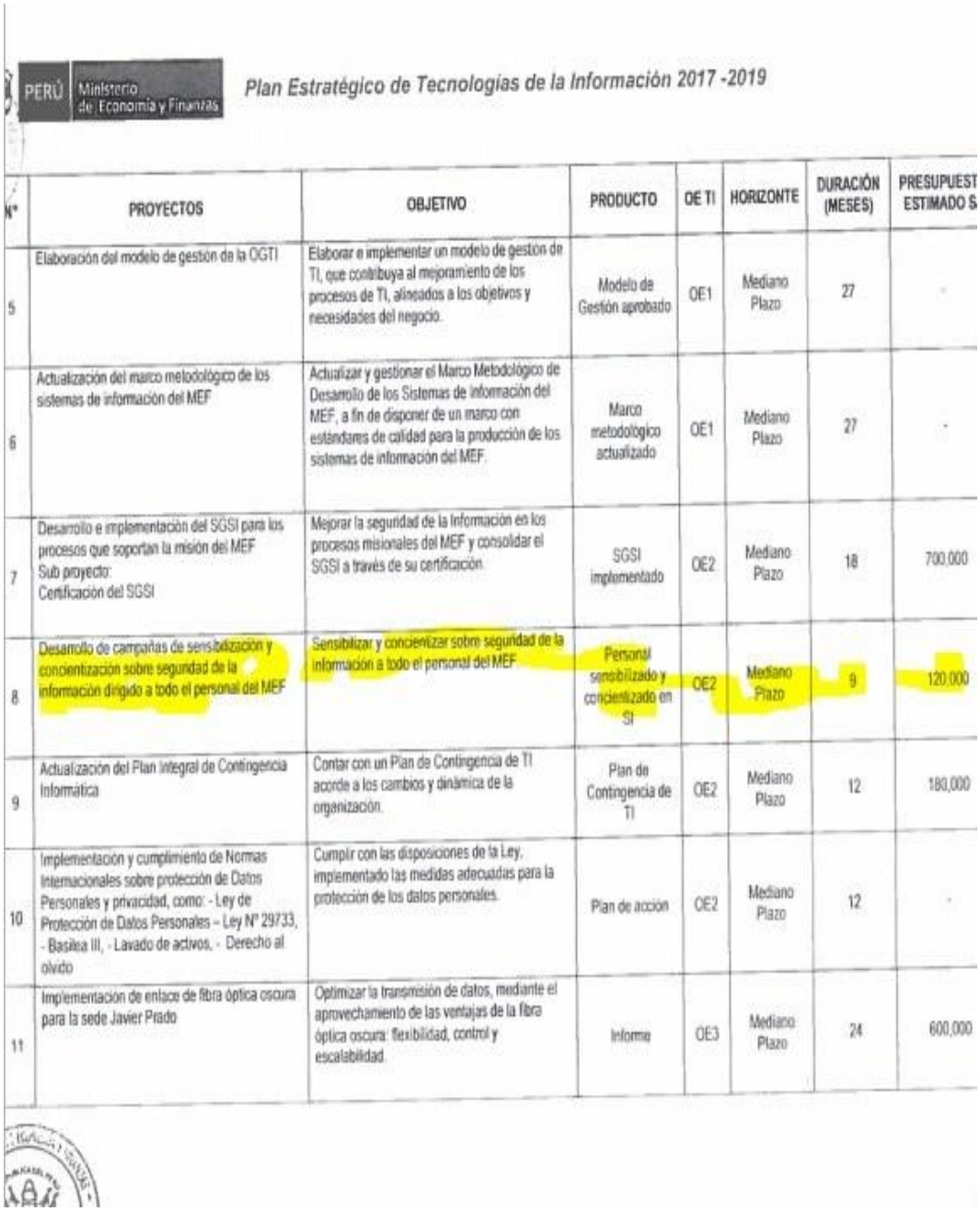
FCE 3. Implementar kit de concienciación de INCIBE a los usuarios Conectamef del Ministerio de Economía y Finanzas.

- Se realizará una serie de simulaciones de ataques dirigidos de prueba para la concienciación de los usuarios Conectamef del Ministerio de Economía y Finanzas.

Utilización de softwares y Planificación de ataques de prueba, no dañinos hacia el sistema del Ministerio de Economía y Finanzas, que se realizará paulatinamente para poder ver y/o medir la acción de los usuarios y poder comprobar si recuerdan los pasos a seguir ante un posible ataque real. Se hará llegar a los usuarios un comunicado personalizado mencionando si fueron buenas las acciones que realizaron en los ataques.

3.2.3.3. Presupuesto

Así como se presentó en su plan estratégico de tecnologías de la información el presupuesto estimado para la concienciación y sensibilización a los usuarios del Ministerio se destinó un total de S/. 120.000 de soles el cual se muestra en la siguiente imagen:



PERÚ | Ministerio de Economía y Finanzas — *Plan Estratégico de Tecnologías de la Información 2017 -2019*

N°	PROYECTOS	OBJETIVO	PRODUCTO	OE TI	HORIZONTE	DURACIÓN (MESES)	PRESUPUEST ESTIMADO S
5	Elaboración del modelo de gestión de la OGTI	Elaborar e implementar un modelo de gestión de TI, que contribuya al mejoramiento de los procesos de TI, alineados a los objetivos y necesidades del negocio.	Modelo de Gestión aprobado	OE1	Mediano Plazo	27	-
6	Actualización del marco metodológico de los sistemas de información del MEF	Actualizar y gestionar el Marco Metodológico de Desarrollo de los Sistemas de información del MEF, a fin de disponer de un marco con estándares de calidad para la producción de los sistemas de información del MEF.	Marco metodológico actualizado	OE1	Mediano Plazo	27	-
7	Desarrollo e implementación del SGSI para los procesos que soportan la misión del MEF Sub proyecto: Certificación del SGSI	Mejorar la seguridad de la información en los procesos misionales del MEF y consolidar el SGSI a través de su certificación	SGSI implementado	OE2	Mediano Plazo	18	700,000
8	Desarrollo de campañas de sensibilización y concientización sobre seguridad de la información dirigido a todo el personal del MEF	Sensibilizar y concientizar sobre seguridad de la información a todo el personal del MEF	Personal sensibilizado y concientizado en SI	OE2	Mediano Plazo	9	120,000
9	Actualización del Plan Integral de Contingencia Informática	Contar con un Plan de Contingencia de TI acorde a los cambios y dinámica de la organización.	Plan de Contingencia de TI	OE2	Mediano Plazo	12	180,000
10	Implementación y cumplimiento de Normas Internacionales sobre protección de Datos Personales y privacidad, como: - Ley de Protección de Datos Personales – Ley N° 29733, - Basilea III, - Lavado de activos, - Derecho al olvido	Cumplir con las disposiciones de la Ley, implementado las medidas adecuadas para la protección de los datos personales.	Plan de acción	OE2	Mediano Plazo	12	-
11	Implementación de enlace de fibra óptica oscura para la sede Javier Prado	Optimizar la transmisión de datos, mediante el aprovechamiento de las ventajas de la fibra óptica oscura: flexibilidad, control y escalabilidad.	Informe	OE3	Mediano Plazo	24	600,000

Figura 14. Plan Estratégico de Tecnologías de la Información 2017 - 2019 (RM469_2017EF44, p.31)

Del plan estratégico propuesto por el Ministerio de Economía y Finanzas Se ha estimado utilizar en el proyecto de Concienciación la cantidad de S/. 50.000 Soles para los usuarios del área de los Conectamef, el cual se detallará en las siguientes tablas.

Tabla 3

Recursos a utilizar en el Plan de Concienciación

1	Forma Presencial (Capacitaciones)	Pasajes	S/. 50,000
		Expositores	
		Catering	
		Auditorio	
		Servicios	
		Otros	
2	Forma Virtual	Herramientas audiovisuales	
		Documentación	
		Personal CAS	
3	Ataque Dirigido (Kit de Concienciación INCIBE)	USB's	
		Software infectado prueba	
TOTAL			S/. 50,000

Fuente: Elaboración propia

Tabla 4

Forma Presencial (Capacitaciones)

1	**Servicio del personal capacitador**	Pasajes	S/. 300
		Viaticos	S/. 200
		SUB TOTAL	S/. 27,000
2	**Elementos requeridos para capacitación**	Auditorio	S/. 1,000
		Catering	S/. 10,800
		Servicios (Agua, Luz)	S/. 0
		SUB TOTAL	**S/. 11,800**
		TOTAL	S/. 38,800

Fuente: Elaboración propia

Tabla 5

Forma Virtual

1	**Herramientas Audiovisuales**	GoAnimate	S/. 175
		SUB TOTAL	**S/. 175**
2	**Otros**	Personal CAS (Capacitador)	S/. 3,500
		Documentación	S/. 1,000
		SUB TOTAL	**S/. 4,500**
		TOTAL	S/. 4,675

Fuente: Elaboración propia

Tabla 6

Ataque Dirigido (Kit de Concienciación INCIBE)

1	**Herramientas Audiovisuales**	USB's	S/. 3,200
		SUB TOTAL	**S/. 3,200**
2	**Otros**	Software infectado prueba	S/. 0
		SUB TOTAL	**S/. 0**
		TOTAL	S/. 3,200
		TOTAL GENERAL	**S/. 46,675**

Fuente: Elaboración propia

De los S/. 50.000 soles estimados para el área del Conectamef se calculó la cantidad de S/. 46.675 soles dejando como presupuesto de reserva S/. 3.325 soles para gastos imprevistos y/o adiciones que puedan presentarse durante los 9 meses de la ejecución del Plan de Concienciación que fue destinado en el presente trabajo de investigación.

Tabla 7

Ficha Técnica para la Programación de Actividades y Proyectos

<table>
<tr><td colspan="2">F-001</td><td colspan="11">FICHA TÉCNICA PARA LA PROGRAMACION DE ACTIVIDADES Y PROYECTOS</td></tr>
<tr><td rowspan="6">I.</td><td colspan="9">DENOMINACIÓN DE LA ACTIVIDAD O PROYECTO</td><td colspan="3">Orden 01</td></tr>
<tr><td colspan="12">Plan para Concienciar usuarios Conectamef en la Seguridad de Ingeniería Social del Ministerio de Economía y Finanzas.</td></tr>
<tr><td colspan="12">Descripción del proyecto:</td></tr>
<tr><td colspan="12">Elaboración de Plan para la concienciación a los usuarios conectamef del Ministerio de Economía y Finanzas.</td></tr>
<tr><td colspan="3">TIPO:</td><td colspan="9">Actividad ( ) Proyecto (x)</td></tr>
<tr><td colspan="3">TIPO DE ORIENTACIÓN:</td><td colspan="9">Orientado a la Gestión: Interna (x) Externa ( )</td></tr>
<tr><td rowspan="2"></td><td colspan="3">PRIORIDAD:</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr>
<tr><td colspan="3"></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td></td><td></td></tr>
<tr><td rowspan="4">II.</td><td colspan="12">DATOS GENERALES</td></tr>
<tr><td>2.1</td><td colspan="2">UNIDAD EJECUTORA:</td><td colspan="10">Oficina General de Tecnología de la Información</td></tr>
<tr><td>2.2</td><td colspan="2">DURACIÓN:</td><td colspan="2">Fecha Inicio</td><td colspan="3">12/02/2019</td><td colspan="2">Fecha Fin</td><td colspan="2">15/04/2019</td></tr>
<tr><td>2.3</td><td colspan="2">COSTO TOTAL:</td><td colspan="10">S/. 50,000</td></tr>
<tr><td rowspan="5">III.</td><td colspan="12">DEL PROYECTO</td></tr>
<tr><td>3.1</td><td colspan="11">Descripción de la Actividad / Proyecto:</td></tr>
<tr><td colspan="12">Elaboración de Plan para la concienciación a los usuarios conectamef del Ministerio de Economía y Finanzas.</td></tr>
<tr><td>3.2</td><td colspan="11">Objetivos de la Actividad / Proyecto:</td></tr>
<tr><td colspan="12">Elaboración de Plan para la concienciación a los usuarios conectamef del Ministerio de Economía y Finanzas.</td></tr>
<tr><td rowspan="2">IV.</td><td colspan="12">META ANUAL: SISTEMAS ( ) MANTENIMIENTOS () MÓDULOS ( )</td></tr>
<tr><td colspan="12">MESES</td></tr>
</table>

	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SET	OCT	NOV	DIC
		X	**X**	**X**								
V.	**COBERTURA DE ACCIÓN:** Nacional (X) Regional ( ) Local ( ) Institucional ( ) Global ( )											
	Conectamef del Ministerio de Economía y Finanzas.											
VI.	**INSTITUCIONES INVOLUCRADAS:**											
	Conectamef del Ministerio de Economía y Finanzas.											
VII.	**PRODUCTOS FINALES:**											
	Concienciación del Usuario Conectamef del Ministerio de Economía y Finanzas.											
VIII	**USUARIOS DE PRODUCTOS FINALES:**											
	Unidad: Conectamef. Número de Usuarios Beneficiados: 234 Número de Usuarios que Demandan: 234 Cantidad de Presupuesto de Reserva: S/. 3.325											

Fuente: Elaboración propia

3.2.3.4. Descripción del Avance.

En el plan de concienciación hacia los usuarios Conectamef del Ministerio se realizaran los planes propuestos en la matriz de variables las cuales indican los objetivos específicos para poder concienciar y sensibilizar a los usuarios, los planes propuestos son: realizar plan de concienciación en forma presencial, plan de concienciación de forma virtual y la implementación de un plan de ataque dirigido desarrollado por el Instituto Nacional de Ciberseguridad de España (INCIBE). Los cuales se desarrollaran de la siguiente manera:

3.2.3.4.1. Plan de Concienciación de Forma Presencial

Así como se manifiesta en el primer objetivo del presente proyecto se propone realizar un plan de concienciación de forma presencial a los usuarios Conectamef del Ministerio de Economía y Finanzas el cual será mediante capacitaciones presenciales indicando las vulnerabilidades y amenazas que existen en Ingeniería Social. Se desea Concienciar al usuario sobre temas como:

- En primer lugar, dar a conocer cómo usar soluciones de seguridad como antivirus, que prevendrán infecciones mediantes exploits o códigos maliciosos, entre otros.
- No aceptar en redes sociales a gente desconocida. La variedad que ofrece la tecnología permite, por ejemplo, preguntarle a un contacto mediante Whatsapp si nos agregó realmente para saber si es quien dice ser.
- Ser cuidadosos con los correos electrónicos recibidos de remitentes desconocidos: pueden robar información y estar infectado con archivos maliciosos adjuntos.
- Descargar aplicaciones de su fuente original. Esto evitará las infecciones en el equipo.
- En conexiones libres como en bares, cafés y lugares públicos, es bueno tener en cuenta no usar servicios que requieran información sensible como usuario y contraseña. Algo que podría ayudarte si necesitaras estos servicios, es el uso de VPN, que enviará todas las comunicaciones cifradas. Explicándole esto a los usuarios.
- La siempre mencionada política de crear contraseñas robustas y fuertes, va a prevenir ataques. Puede resultar un poco tedioso tener diferentes contraseñas para los servicios utilizados, pero se pueden usar aplicaciones gestoras de usuarios y contraseñas; información que es almacenada en un archivo cifrado.
- En sitios web que requieran información de usuario y contraseña, chequear que utilizan https en lugar de http.

3.2.3.4.2. Plan de Concienciación de Forma Virtual

Se realizarán una serie de lanzamientos virtualmente a los usuarios Conectamef del Ministerio de Economía y Finanzas los cuales tendrán como finalizar informar

sobre las formas de protección ante amenazas. Para ello se realizó o se piensa realizar una serie de Videos, posters, correos informativos e información vía Intranet.

Videos

Se usará una herramienta para la elaboración de videos llamada Goanimate el cual servirá para la realización de concienciación sobre las contraseñas y el uso debido de ellas y poder ver el impacto que se podría lograr en caso no se esté informado adecuadamente, para ello se realizó un proyecto demo el cual se presenta en la siguiente imagen:

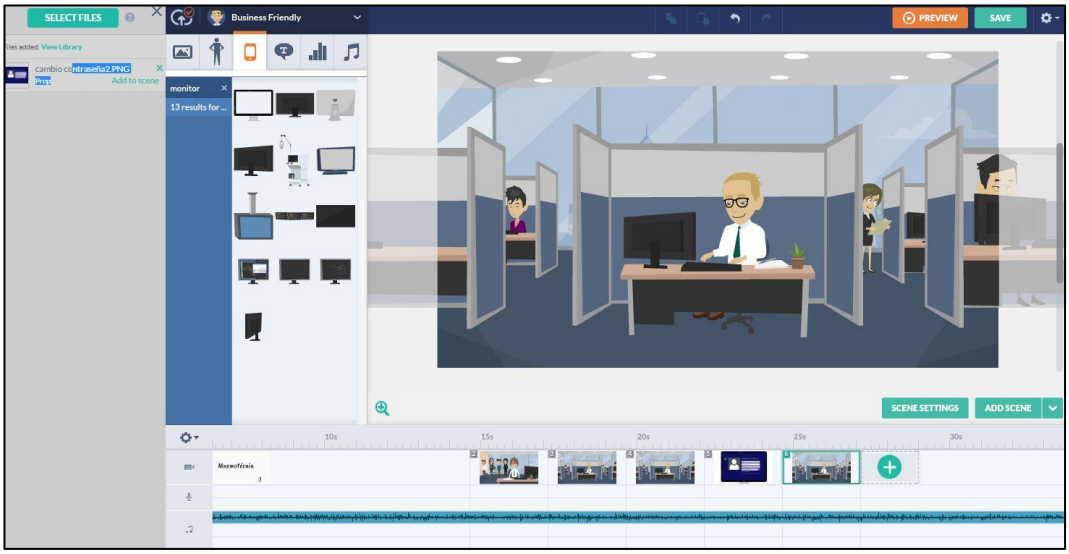


Figura 15. Elaboración de Videos de Concienciación (Elaboración propia)

Posters, correos informativos e Intranet

Una de las formas de concienciación también será mediante la realización de comunicado informativo mediante posters donde se indicarán los conceptos de amenazas que existen, dicha información será colgada en la página de intranet del Ministerio, mediante correos regulares y en propaganda pegadas en lugares estratégicos como ascensores y lobbys. Se realizó un posters modelo así como se muestra en la siguiente imagen:

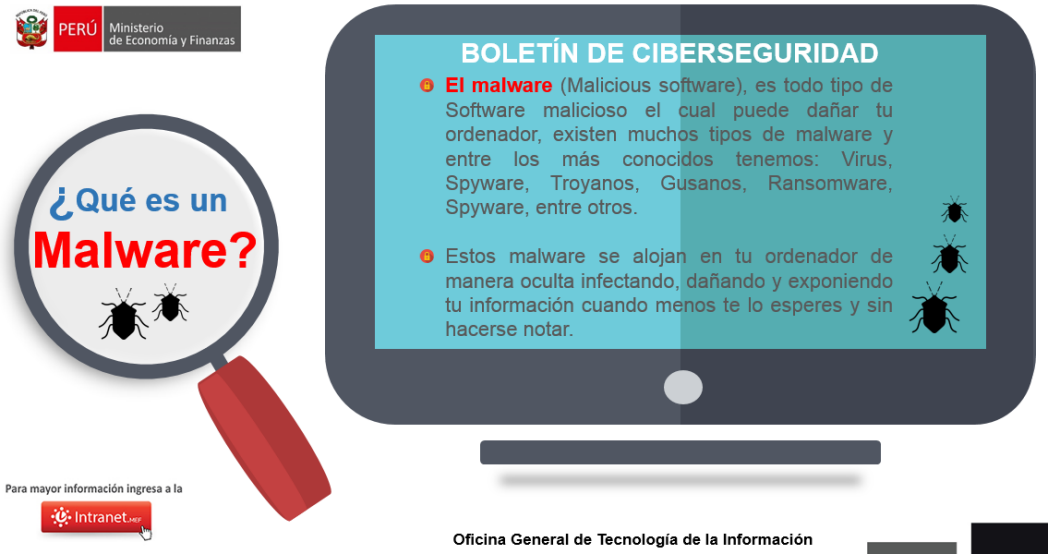


Figura 16. Elaboración de Posters de Concienciación (Elaboración propia)

3.2.3.4.3. Plan de Concienciación Ataque Dirigido Incibe

El plan de concienciación de Incibe viene con una lista de actividades las cuales están conformadas por píldoras según a un plan propuesto de información a los usuarios en este caso irá dirigido a los Conectamef del Ministerio. Se usaran pendrive infectados escondidos en USB, envío de correos electrónicos re direccionados a una página propuesta infectada. El plan propuesto irá de la mano con las formas de concienciación presencial y Virtual.

Pendrive Infectado:

El ataque está basado en la presencia de un fichero infectado en varias memorias USB “extraviadas”, los cuales al ser ejecutados, muestran al usuario un portal web advirtiéndole del peligro que supone lo que acaba de hacer. Para ello, deben seguirse los siguientes pasos:

1. Es recomendable que el fichero “infectado” vaya acompañado de otro tipo de contenido totalmente inofensivo como un directorio llamado “Fotos” y otro “Documentación” donde en cada uno de ellos haya ciertos ficheros

genéricos como imágenes descargadas de internet, documentos PDF y/o documentos Excel o Word. Junto a ellos, se ubicará el fichero infectado, pudiendo ser renombrado con algún nombre atrayente para cualquier persona como “confidencial.exe” o “material_privado.exe”.

2. El objetivo es que el usuario encuentre y utilice el USB o memoria localizada. Para ello, se deberá “abandonar” el dispositivo en una ubicación en la que sea muy probable que un usuario pueda encontrarlo. Algunos de estos lugares pueden ser:

    - ascensor
    - entrada principal
    - sala de café o comida
    - los servicios
    - pasillo transitado

    Es importante que el encargado de desplegar las memorias USB no sea detectado durante el proceso. En el caso de que el usuario la devuelva al área de Sistemas del Ministerio de Economía y Finanzas o cualquier otro responsable, se le explicará la prueba y su finalidad, se le solicitará que no comente nada al resto de compañeros y se iniciará de nuevo el proceso, desplegando el USB en otra ubicación. Es importante indicar al usuario lo correcto de su decisión de devolver el USB sin haberlo usado. Además, para ambos casos se recomienda explicar los motivos de la prueba a los usuarios implicados en la misma una vez haya finalizado esta fase.

Además, para ambos casos se recomienda explicar los motivos de la prueba a los usuarios implicados en la misma una vez haya finalizado esta fase.

Archivo malicioso:

El archivo que se emplea en ambos ataques es un programa cuya única misión

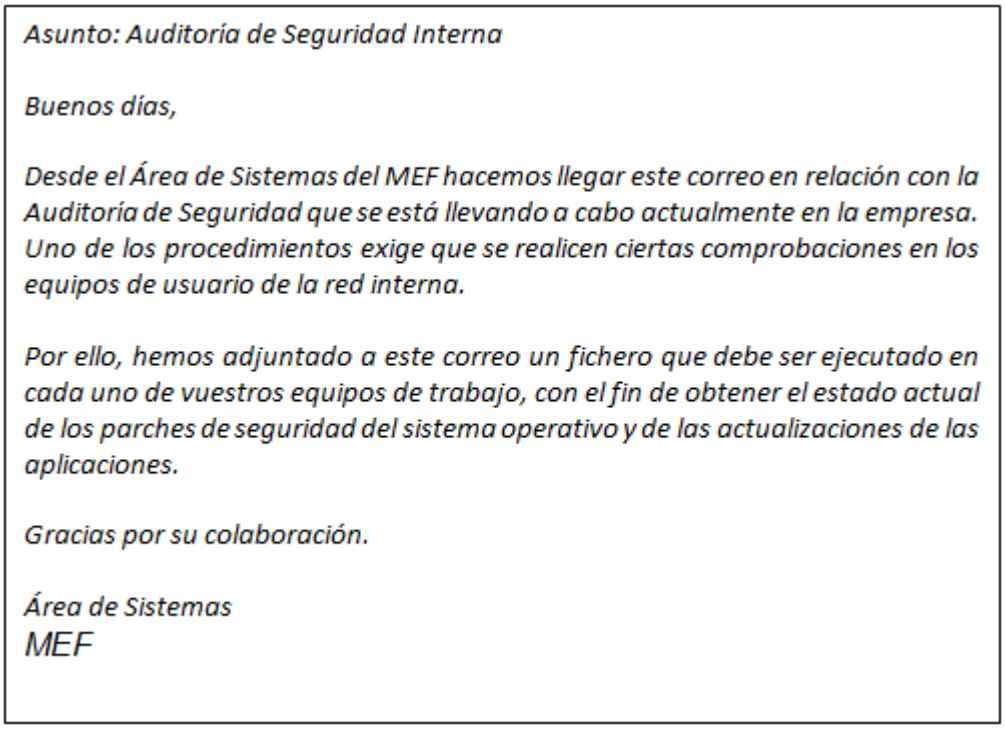
de este fichero es abrir el navegador de usuario o, en el caso de que ya esté abierto, abrirle una pestaña, directamente a una página web de INCIBE o alguna otra que se plantee, donde se expongan los peligros de las acciones que acaba de realizar, así como las medidas que debe tomar para no provocar una posible infección de malware en la red de la empresa.

Es fundamental que el fichero sea renombrado con un nombre "atractivo para el usuario", a ser posible relacionado con la propia empresa. Este fichero NO es identificado por los antivirus como una amenaza. Sin embargo, al tratarse de un fichero ejecutable, es probable que el sistema operativo solicite confirmación de que se desea ejecutar. Una de las razones de esta prueba es observar que decide hacer el usuario en este punto. Una vez finalizada la prueba, se solicitará a los usuarios involucrados que devuelvan el dispositivo pendrive y que eliminen el fichero en el caso de que haya sido copiado a su equipo. Dentro de la información de descarga de los ataques dirigidos podrá encontrar más información sobre el mismo.

Correo electrónico con archivo malicioso adjunto: El primer tipo de ataque está basado en el envío de un correo electrónico con un fichero infectado, el cual al ser ejecutado, muestra al usuario un portal Web advirtiéndole del peligro que supone lo que acaba de hacer. Para ello, deben seguirse los siguientes pasos:

Se utilizará una cuenta de correo electrónico ficticia pero cuyas características sean similares (nombre y apellidos de un empleado "nuevo" o cuenta tipo de un departamento) a las cuentas de correo del Ministerio. Ejemplos: sistemas@empresa.pe, auditoria@empresa.pe o nombre.apellido@empresa.pe. Empleando esta cuenta de correo, se enviará un correo electrónico en el que mediante un pretexto previamente pactado, se pide a las víctimas en este caso usuarios Conectamef del Ministerio que ejecuten el archivo que se incluye en el correo electrónico. Este correo electrónico, puede enviarse a todos los empleados o a un número determinado de destinatarios que "participarán" en el experimento sin su previo conocimiento.

Es recomendable, para dar credibilidad al correo, que éste lleve incluido en copia (campo CC) a algún cargo importante de la empresa. Antes debe obtenerse el permiso explícito de esta persona para incluirlo en la prueba. El asunto o subject debe ser el título con el que queremos que lleguen los correos, por lo que debe ser lo más claro y creíble posible. A continuación, se muestra un ejemplo de correo electrónico a utilizar para desplegar el ataque:



Asunto: Auditoría de Seguridad Interna

Buenos días,

Desde el Área de Sistemas del MEF hacemos llegar este correo en relación con la Auditoría de Seguridad que se está llevando a cabo actualmente en la empresa. Uno de los procedimientos exige que se realicen ciertas comprobaciones en los equipos de usuario de la red interna.

Por ello, hemos adjuntado a este correo un fichero que debe ser ejecutado en cada uno de vuestros equipos de trabajo, con el fin de obtener el estado actual de los parches de seguridad del sistema operativo y de las actualizaciones de las aplicaciones.

Gracias por su colaboración.

Área de Sistemas
MEF

Figura 17. Correo Engañoso
Tomado de https: //www.incibe.es/sites/default/files/contenidos/kit-concienciacion/incibe_kit_de_concienciacion_manual_de_implantacion.pdf, por INCIBE (Instituto de Ciberseguridad en España).

El objetivo del mismo es que el usuario se crea que el correo es legítimo, aunque no lo sea. Se adjuntará al correo a enviar el fichero infectado. Este archivo debe tendrá un nombre como auditoria_interna.exe o audit2015.exe, u otro nombre que se elija según el pretexto que se quiera utilizar. Una vez finalizada la prueba, se eliminará la cuenta de correo ficticia creada.

Según lo anteriormente expuesto en los planes se platea realizar estas formas de concienciación según el tiempo establecido por el PETI planteado en el Ministerio de Economía y Finanzas 2016-2019. Que dice que se ha propuesto un tiempo de 9 meses. En ese tiempo se planteará sea realizado en 7 fases como se muestra en la siguiente imagen:

	NOMBRE DE FASE	DURACIÓN
FASE 1	Plantear el plan de concienciación	Mes 1
FASE 2	Ataques dirigidos	Mes 2
FASE 3	Distribución de posters e información vía Intranet	Mes 2
FASE 4	Proceso Formativo	Mes 3
		Mes 4
		Mes 5
FASE 5	Distribución de Consejos de Seguridad	Mes 6
		Mes 7
		Mes 8
FASE 6	Recordatorio - Ataques Dirigidos	Mes 9
FASE 7	Valoración - Encuesta de Satisfacción	Mes 9

Figura 18. Cronograma de Concienciación (Elaboración propia)

El tiempo de Duración de cada fase es un tiempo aproximado y tentativo para la realización del plan de concienciación.

Fase 1:

Plantear el plan de concienciación: Esta fase servirá para realizar el plan y poder definir fechas con el encargado del área para se pueda llegar a un acuerdo para la empezar con el proyecto.

Fase 2:

Ataques Dirigidos: En esta fase se plantea usar los archivos maliciosos y los Pendrive Infectados mediante correos, USB's según como se plantee en el

planteamiento del plan de concienciación.

Fase 3:

Distribución de posters e información vía Intranet: Dicha Fase es para poder enviar material con el cual se informará sobre los conceptos de amenazas que podrían existir en la institución.

Fase 4:

Proceso Formativo: En esta fase se realizan las capacitaciones a los usuarios de los 27 diferentes Conectamef del Perú las cuales serán definidas en la fase 1.

Fase 5:

Distribución de Consejos de Seguridad: En esta fase se irá distribuyendo paulatinamente material en cual se dan consejos de seguridad y tips para poder actuar de una mejor forma para poder prevenir y actuar ante un posible ataque.

Fase 6:

Recordatorio - Ataques Dirigidos: En Dicha fase se enviará otro ataque dirigido por correo o el uso de los USB's infectados según se coordine en la primera fase para poder ver que usuarios volvieron a ser víctimas de estos ataques de prueba.

Fase 7:

Valoración - Encuesta de Satisfacción: Es está fase se podrá medir el nivel de aprendizaje obtenido por todo el proceso de concienciación, viendo si se lograron las expectativas propuestas con dicho plan.

3.2.3.5. Matriz Encuesta

En la encuesta se realizó una simulación para la obtención de los datos ya que

al no tener el tiempo propuesto por el plan se tuvieron que usar datos supuestos con probabilidades de mejora en un pre entrevista y post-entravista, se muestra a continuación las imágenes de la simulación.

3.2.3.5.1. Pre-Valoración

NIVELES	RANGOS			
BAJA	[13-31>	55	55%	55
MODERADA	[31-48>	32	32%	32
ALTA	[48-65>	13	13%	13
		100	100%	100

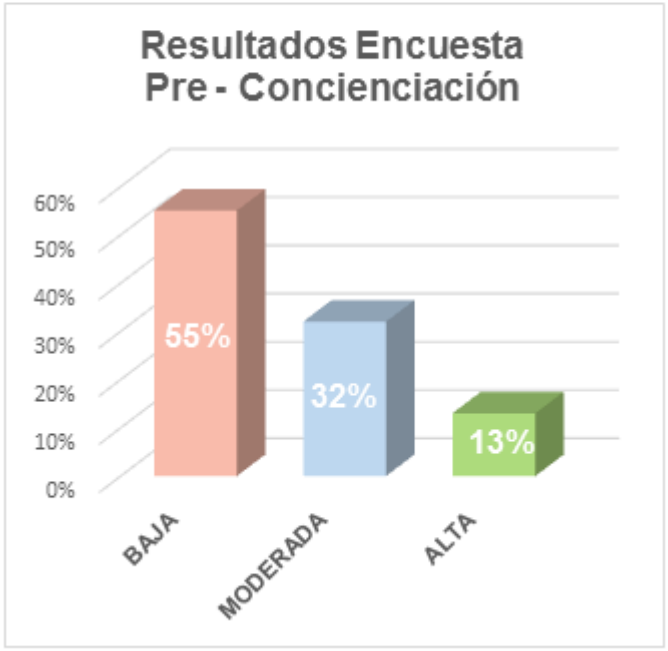


Figura 19. Resultados Encuesta Pre- Concienciación (Elaboración propia)

	V1							V2								
	V1P1	V1P2	V1P3	V1P4	V1P5	V1P6	V1P7	V2P8	V2P9	V2P10	V2P11	V2P12	V2P13	V1	V2	Total
1	1	1	2	1	2	3	2	1	1	2	2	2	2	12	10	22
2	1	2	4	1	4	3	1	1	4	1	2	4	3	16	15	31
3	3	5	3	5	2	4	5	5	2	5	2	4	3	27	21	48
4	3	1	1	3	2	2	1	4	1	3	3	4	1	13	16	29
5	5	1	2	2	1	2	2	1	3	1	2	1	3	15	11	26
6	2	5	2	5	1	2	5	2	1	1	1	1	4	22	10	32
7	5	4	1	1	1	1	1	2	4	1	1	3	3	14	14	28
8	4	2	2	5	5	1	1	1	1	1	2	1	1	20	7	27
9	3	3	2	2	4	2	3	2	5	5	5	5	5	19	27	46
10	4	3	1	4	2	2	2	5	2	1	4	2	2	18	16	34
11	2	2	3	3	1	1	1	3	1	2	2	2	2	13	12	25
12	1	4	5	3	3	4	3	5	4	3	5	5	5	23	27	50
13	3	2	3	2	3	2	1	4	1	1	4	1	4	16	15	31
14	5	3	5	3	3	2	5	3	4	5	4	5	2	26	23	49
15	5	1	1	1	1	1	2	1	1	1	2	1	3	12	9	21
16	3	4	1	1	2	3	1	1	2	2	5	1	4	15	15	30
17	1	1	1	2	1	1	1	2	1	3	2	2	1	8	11	19
18	1	2	3	1	1	2	2	5	1	4	1	1	1	12	13	25
19	2	5	4	5	5	3	3	4	3	5	5	4	5	27	26	53
20	3	1	2	3	3	2	2	1	2	1	2	2	1	16	9	25
21	1	2	1	1	1	3	1	3	3	2	2	3	1	10	14	24
22	2	5	2	1	2	2	1	1	3	1	3	2	2	15	12	27
23	3	2	3	5	4	5	3	4	4	4	5	4	3	25	24	49

Figura 20. Datos Encuesta Pre- Concienciación (Elaboración propia)

3.2.3.5.2. Post Valoración

NIVELES	RANGOS			
DEFICIENTE	[13-31>	9	9%	9
REGULAR	[31-48>	36	36%	36
EFICIENTE	[48-65>	55	55%	55
		100	100%	100

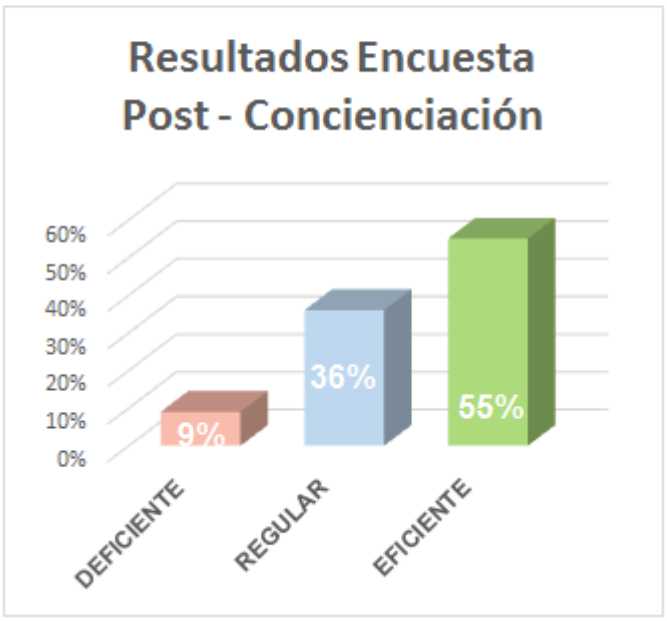


Figura 21. Resultados Encuesta Post- Concienciación Simulación (Elaboración propia)

	V1							V2								
	V1P1	V1P2	V1P3	V1P4	V1P5	V1P6	V1P7	V2P8	V2P9	V2P10	V2P11	V2P12	V2P13	V1	V2	Total
1	4	4	1	5	2	2	5	5	5	5	5	4	3	16	12	50
2	5	5	5	5	4	4	3	5	4	3	3	4	4	24	12	54
3	4	4	1	5	3	3	5	5	5	5	3	4	3	17	13	50
4	4	4	1	5	3	3	5	5	5	5	4	4	3	17	13	51
5	3	3	3	5	5	3	2	1	5	4	2	2	1	19	6	39
6	3	1	3	5	2	3	3	3	3	4	3	1	4	14	9	38
7	4	4	5	5	2	2	5	5	5	5	2	4	3	20	12	51
8	4	3	5	1	3	5	3	4	5	3	2	5	5	16	12	48
9	4	4	5	5	2	2	5	5	5	5	2	4	3	20	12	51
10	3	3	3	1	5	5	5	3	3	5	5	5	4	15	13	50
11	3	5	3	1	2	3	3	5	5	5	4	5	5	14	11	49
12	5	3	3	5	4	3	3	5	5	5	4	4	3	20	11	52
13	1	5	5	5	2	2	1	4	5	4	3	4	4	18	7	45
14	4	4	5	5	2	2	5	5	5	5	3	4	3	20	12	52
15	4	4	5	5	2	2	5	5	5	5	5	4	3	20	12	54
16	4	4	5	5	2	2	5	5	5	5	4	4	3	20	12	53
17	2	2	5	1	4	1	4	2	3	3	4	4	1	14	7	36
18	2	5	5	1	3	3	5	1	3	2	3	4	3	16	9	40
19	1	5	3	5	1	1	3	4	2	3	3	2	1	15	8	34
20	3	2	5	5	5	1	1	2	1	5	2	1	3	20	4	36
21	2	1	3	5	2	1	1	3	1	2	5	5	3	13	5	34
22	1	3	5	5	2	1	2	4	5	1	2	3	1	16	7	35
23	4	1	3	1	2	2	2	3	3	2	3	2	1	11	7	29

Figura 22. Datos Encuesta Post- Concienciación Simulación (Elaboración propia)

3.2.4. Limitaciones

Las presentes limitaciones restringirán la investigación:

i) Disposición por parte de los empleados en brindar información.

Dentro de la población usuaria de la institución no se puede disponer de la información completa para realizar el trabajo de investigación adecuada ya que dicha información es de nivel crítico exponer y por ello se está trabajando con aproximaciones de cantidades.

ii) Disposición de tiempo por parte de los empleados por sus ocupaciones laborales.

Personal de la institución no cuenta con el tiempo adecuado para poder

conversar sobre el tema a realizar en el trabajo de investigación, ya que en el día a día de sus labores el tiempo es limitado y crítico al ser interrumpidos.

iii) Tiempo corto estimado para la realización de pruebas del trabajo.

Al ser un trabajo de investigación de un tiempo predeterminado de aproximadamente 3 meses no se puedo concluir con la totalidad del plan de concienciación planteado de 9 meses lo cual lleva a una conclusión simulada con los datos que se pudo recolectar teniendo una mejora significativa en el objetivo del plan.

3.2.5. Cronograma de Actividades

Figura 23. Cronograma de Actividades (Elaboración propia)

I. Conclusiones

Primera Conclusión:

A raíz de los datos recogidos de los ataques hacia el Ministerio, se pudo comprobar que el área de los Conectamef son los usuarios más vulnerables ante una amenaza en la actualidad.

Segunda Conclusión:

Al termino de las encuestas se pudo obtener el resultado que más del 50% de usuarios encuestados tenía un bajo nivel de concienciación sobre temas referentes a la seguridad en Ingeniería Social.

Tercera Conclusión:

Al hacer un comparativo antes y después de la concienciación a los usuarios se refleja un cambio referentes a los temas expuestos en las capacitaciones.

II. Recomendaciones

Primera recomendación:

Se recomienda realizar cada mes una retroalimentación sobre los temas tratados en el plan de concienciación a los nuevos usuarios que se incorporen a la institución siendo los usuarios antiguos los encargados de informar sobre estos temas.

Segunda recomendación:

Se recomienda actualizar al usuario después del plan de 9 meses sobre los nuevos temas de seguridad acerca de la Ingeniería Social.

Tercera recomendación:

Se recomienda realizar test comparativos cada cierto tiempo para medir el grado de impacto sobre los temas de seguridad en Ingeniería Social a los usuarios Conectamef.

III. Referencias Bibliográficas

MEF (2019). Oficina General de Tecnologías de la Información. Ministerio de Economía y Finanzas. Perú. Recuperado de: https://www.mef.gob.pe/es/quienes-somos/vision-mision-objetivo

GMO GlobalSing, Inc., 2018). Empresa especializada en transacciones seguras de comercio, comunicaciones y más. Recuperado de: https://www.globalsign.com/en/blog/what-is-social-engineering-the-human-confidence-game/

(Marín, 2018). Estudio de Metodologías de Ingeniería Social. Recuperado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81271/6/rmarinjTFM0618memoria.pdf

(Roque y Juárez, 2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072018000200005

(Flórez y Méndez, 2017). Estudio de Ingeniería Social en el uso de las redes sociales. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14505/1/17659358.pdf

(Mendoza, 2019). La mitad de ejecutivos cree que ciberataques a firmas son originados por los empleados, Diario Gestión Perú. Recuperado de: https://gestion.pe/peru/mitad-ejecutivos-cree-ciberataques-firmas-son-originados-empleados-259496

Bermúdez (2015). Ingeniería Social, un factor de riesgo informático inminente en la Universidad Cooperativa de Colombia Sede Neiva. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3629/1/1075210015.pdf

Aguilar, De la Cruz (2015). Implementación de una solución de Hacking Ético para mejorar la seguridad en la infraestructura informática de La Caja Municipal De Sullana - Agencia Chimbote. Recuperado de: http://repositorio.uns.edu.pe/bitstream/handle/UNS/1964/30710.pdf?sequence=1&

isAllowed=y

Dioppe (2015). Seguridad Informática. Recuperado de: http://repositorio.unapiquitos.edu.pe/bitstream/handle/UNAP/4898/Norman_Tesis_Titulo_2015.pdf?sequence=4&isAllowed=y

Alcántara (2015). Guía de Implementación de la Seguridad basado en la Norma Iso/Iec 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del Norte P.N.P en la Ciudad De Chiclayo. Recuperado de: http://tesis.usat.edu.pe/bitstream/usat/539/1/TL_Alcantara_Flores_JulioCesar.pdf

INCIBE (Instituto Nacional de Ciberseguridad en España, 2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Belloch (S/F). Entornos Virtuales de Aprendizaje. Recuperado de: https://www.uv.es/bellochc/pedagogia/EVA3.pdf

Mueres (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas. En Evil Fingers portal comunitario sobre seguridad informática. Recuperado de: https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Ojeda (2018). Página web (GB advisors es un socio comercial que da soluciones de evaluación del Riesgo, Vulnerabilidad y más. Conoce los riesgos y amenazas de la ingeniería social sobre tus activos y datos sensibles. Recuperado de: https://www.gb-advisors.com/es/riesgos-y-amenazas-de-la-ingenieria-social/

MEF (2019). Oficina General de Tecnologías de la Información. Ministerio de Economía y Finanzas. Perú. Recuperado de: https://www.mef.gob.pe/es/por-instrumento/resolucion-ministerial/16777-resolucion-ministerial-n-469-2017-ef-44/file

IV. Anexos

Tabla 8

Matriz de Variables disgregadas en Concientizar al usuario y Ataques de Ingeniería Social Informático

Nombre de la Variable	Concepto de la Variable	Operacionalización de la Variable	Dimensiones	Indicadores
Concienciar al usuario	Es cambiar comportamientos, hábitos y actitudes de los usuarios a través de un proceso continuo. Ramírez (2007, p. 43)	Encuesta que muestre una comparación de un antes y un después de realizar el plan.	Concienciar de forma presencial	- Capacitaciones
			Concienciar de forma virtual	- Videos - Posters - Correos Informativos - Intranet
			Concienciar con ataque dirigido	Kit de concienciación INCIBE
Seguridad en Ingeniería Social	Es el principio a los pasos irreversibles en términos de amenazas que llevan a riesgos asumidos al nivel de protección de la información buscada asegurando ello con el estudio, preparación y la explotación.	Cuadros estadísticos que muestren el porcentaje de un antes y un después de los ataques informáticos detectados.	- Amenazas	- Vishing - Spoofing - USB - Spam - Phishing
			- Vulnerabilidades	- Factor Humano - Factor Web

Fuente: Elaboración propia