REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa

Volumen 8 – Número 1
enero-junio 2025
pp. 65-72

Implementación de un plan de concienciación en ciberseguridad en un centro de investigación de universidades en Panamá

Implementation of a cybersecurity awareness plan in a university research center in Panama

Iván Ho
Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, Panamá
Correo: ivanhog@gmail.com https://orcid.org/0000-0001-8634-0863
Giselle Ulloa
Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, Panamá
Correo : giselle.ulloawork@gmail.com https://orcid.org/0000-0003-4830-9157
Katherine Moreno
Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, Panamá
Correo: profekatherinework@gmail.com https://orcid.org/0009-0003-1988-1733

Recibido: 30-08-2024 Aprobado: 21-10-2024

DOI: https://doi.org/10.48204/j.faeco.v8n1.a6433

RESUMEN

En la actualidad, las universidades estatales carecen una cultura de ciberseguridad para alcanzar la excelencia educativa al integrar sistemas informáticos y herramientas tecnológicas para brindar una mejor educación al país, entregando profesionales con mejores competencias en ciencia y tecnología. La seguridad informática de una institución no es solo tener los últimos software, políticas, lineamientos y equipos tecnológicos contra ciber amenazas , sino tener usuarios concienciados debido a que ellos son el eslabón débil de la seguridad de cualquiera institución u empresa, generalmente es la primera persona a la cual los ciber atacantes acuden para obtener la información necesaria mediante la ingeniería social porque es la manera más fácil y efectiva de obtener la información de la empresa sin necesidad de utilizar softwares sofisticados y así saltar la seguridad que brindan los sistemas informáticos de la institución.

Palabras claves: ciberseguridad, concienciación, correos fraudulentos, seguridad informática, phishing, malware.

ABSTRACT

Currently, state universities lack a cybersecurity culture to achieve educational excellence by integrating computer systems and technological tools to provide better education to the country, delivering professionals with better skills in science and technology. The computer security of an institution is not only having the latest software, policies, guidelines and technological equipment against cyber threats, but also having users who are aware because they are the weak link in the security of any institution or company, generally it is the first person. to which cyber attackers go to obtain the necessary information through social engineering because it is the easiest and most effective way to obtain the company's information without having to use sophisticated software and thus bypass the security provided by the institution's computer systems.

Keywords: cybersecurity, awareness, fraudulent emails, computer security, phishing, malware.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 8 – Número 1
enero-junio 2025
pp. 65-72

INTRODUCCIÓN

Mediante el paso del tiempo la seguridad informática como tal no es primordial dentro del sector empresarial y universitario, el cual es un procedimiento de mayor importancia, ya que con la debilidad del mismo se presenta el riesgo de pérdida de información sensitiva, provocando así el cierre de la empresa y en la universidad con el hecho de perder estudiantes o futuros profesionales que ayudaran al país; cabe mencionar que en Panamá; el presupuesto brindado a las principales universidades por parte del gobierno fue reducido en millones de dólares (O.A. Jaramillo, 2019, p.1), aumentando drásticamente una debilidad como es la seguridad, quedando sin fondos para mejorarse, pero a pesar de todo se tiene una solución parcial a este predicamento y es el plan de concienciación para los administrativos, docentes e inclusive a los estudiantes, brindándoles así una pequeña capa de seguridad ante todos estos ataques que aparecen diariamente, como los son el robo de identidad, phishing, los correos fraudulentos y otros.

Esta problemática se origina por el hecho de que las universidades se han convertido en uno de los puntos de ataques más atractivo por los ciber delincuentes debido a que los estudiantes y el personal que la conforman utilizan el internet de la institución para conectar sus propios dispositivos para acceder a sus cuentas bancarias y los sistemas de la institución, es decir, tenemos usuarios que no aplican medidas de seguridad para proteger su información personal y confidencial (Rodolfo Pilipiak, 2019, p.1).

Según el artículo web del sitio el economista, “Las Universidades son las terceras instituciones más atacadas” (Noelia Garcia, 2019, p.1). Además, un estudio de la empresa Deloitte, revela que el 80% de las universidades consideran que están expuestas a ataques de ciberseguridad (Deloitte, 2018, p.1).

El panorama ante estos ataques puede cambiar implementando un plan de concienciación en donde nos explica el cómo identificar estos ataques y como prevenir ser una víctima más de los mismo. Con esto se pretende hacer un llamado de atención e incentivar a la concienciación en ciberseguridad a la comunidad académica y administrativa de las universidades en Panamá.

Así los colaboradores que la conforman tengan el conocimiento de identificar los posibles ataques y tomar medidas con el que reducirán los riesgos de ataques de ciberseguridad, como la ejecución de archivos maliciosos adjuntados en correos fraudulentos que podrían dejar inutilizado los sistemas informáticos de la institución.

Para entender más sobre el tema se explicará sobre conceptos de ciberseguridad y las fases del plan de concienciación en ciberseguridad.

CONTENIDO

Antes de explicar el plan de concienciación, comenzaremos definiendo algunos conceptos importantes como:

CC BY NC SA

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 8 – Número 1
enero-junio 2025
pp. 65-72

La Seguridad informática son aquellas actividades que permiten prevenir y sobre todo detectar el uso no autorizado de un sistema informático. Estas actividades son las medidas de seguridad como el uso de antivirus, firewall, y las medidas que dependan del usuario como el uso adecuado de los equipos informáticos, los recursos de red o de Internet (Universidad Internacional de Valencia, 2018, p.1).

Según ISACA, la ciberseguridad se define como: "La protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados " (M.A. Mendoza, 2015, p.1).

Ambos conceptos se enfocan en proteger la información, pero la seguridad informática se enfoca en proteger la información contra los riesgos que pueden afectarla. Mientras que la ciberseguridad se centra en proteger la información en forma digital y los sistemas interconectados a esta. Es decir, la seguridad informática abarca más aspectos e involucra a la ciberseguridad (M.A. Mendoza, 2015, p.1).

Esto nos lleva a la siguiente pregunta, ¿Por qué es importante tomar conciencia en ciberseguridad?

Un aspecto por tomar en cuenta es que el usuario debe entender el por qué debe formarse en ciberseguridad, es decir, mostrarle el panorama de lo que está aconteciendo, el por qué y el cómo de las cosas. No es solamente darle a conocer todos los ataques y medidas, sino que al concienciarlo sobre el tema el mismo se involucre y gestione también la protección de su propia seguridad, es decir que forme parte en la lucha contra los ciber ataques (Universidad de Cadiz, s.f. p.1).

La concienciación es tan importante también a nivel interno de la institución ya que son los empleados los que gestionan la información. Son los encargados de modificarla, transmitirla, eliminarla y procesarla, por lo tanto, la necesidad de aplicar un plan de concienciación se hace cada vez más necesario. "El 80% de los ciberataques corporativos están dirigidos a los empleados. En este sentido, la directora de Fosensic de Grant Thornton también alertó de que, según la compañía, ocho de cada diez ataques cibernéticos que sufren las empresas están dirigidos a empleados, a través malware o phishing" (Elderecho.com. 2024, p.1).

Plan de concienciación en ciberseguridad

Abarcado los puntos anteriores, la implementación de un plan de concienciación se basó en el kit de concienciación en ciberseguridad ofrecido por el Instituto Nacional de Ciberseguridad (INCIBE) y la planificación de este se realizará por medio de técnicas y herramientas en administración de empresas de la guía PMBOK del PMI.

El plan de concienciación está compuesto por fases, en la cuales se realizará una evaluación inicial para identificar el nivel de concienciación del usuario en la materia, en las siguientes fases el colaborador pasará por un proceso formativo de nueve meses. Por último, nuevamente se evaluará el nivel de concienciación del usuario con el propósito de evaluar si el proceso formativo fue realmente entendible y se realizará

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 8 – Número 1
enero-junio 2025
pp. 65-72

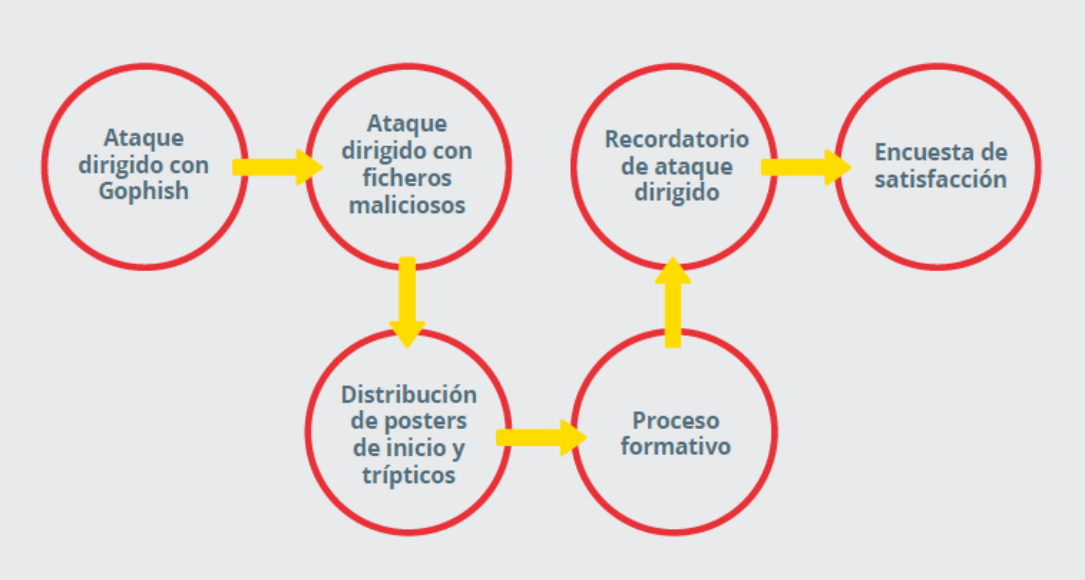
una encuesta de satisfacción (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion).

Cabe recalcar que el kit, lo proporciona INCIBE desde su página web como un archivo comprimido con toda la información y software para ser implementado en cualquiera entidad.

Este plan basado en el kit puede ser adaptado de acuerdo con las necesidades de la empresa o cualquier la institución del cual sector. Dicho esto, describiremos paso a paso las fases del kit (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion). Las fases que conforman el plan son: ataque dirigido con Gophish, ataque dirigido con ficheros maliciosos, distribución de inicio y trípticos, proceso formativo, recordatorio de ataque dirigido y encuesta de satisfacción (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion). Ver figura 1.

Figura 1.

Fase del Kit de concienciación



Fuente: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

Descripción y desarrollo de las fases.

Fase I: Ataque Dirigido con Gophish.

De acuerdo con el Manual de Implementación de Gophish en el Kit de Concienciación del Instituto Nacional de Ciberseguridad de España, *"Gophish es un entorno de trabajo que permite la simulación de ataques de phishing para poner a prueba los conocimientos en la identificación de correos maliciosos y suplantaciones, en este caso, de los empleados de nuestra empresa"* (Instituto Nacional de Ciberseguridad. S.f. Manual de Implementación de la Herramienta Gophish, España).

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 8 – Número 1
enero-junio 2025
pp. 65-72

En esta primera fase se evaluará el nivel de concienciación del colaborador en cuanto a ataques de tipo phishing. Este ataque consistirá en suplantar a un servicio, en nuestro caso el sistema de asistencia, el sistema de correo institucional con el propósito de obtener las credenciales de dichos sistemas a través de las víctimas, es decir los colaboradores que formaran parte del plan de concienciación. Al final el usuario verá el peligro y las consecuencias de no tomar las precauciones debidas ante este tipo de ataque (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion).

Fase II: Ataque dirigido con ficheros maliciosos.

En esta fase, se está todavía en proceso de evaluación del nivel de concienciación del usuario.

La fase II se enfoca en concienciar sobre los ataques dirigidos con ficheros maliciosos, es decir, aquellos ataques en los que el empleado ejecuta malware (fichero malicioso) por descargar y ejecutar un fichero malicioso recibido como adjunto a través de un correo fraudulento donde el remitente se hace pasar por el departamento de informática, algún cliente inclusive alguna entidad de servicios bancarios y del sector públicos como las empresas que se dedican a ofrecer servicios de agua, luz, internet o teléfono. También por la ejecución de ficheros maliciosos en memorias USB o dispositivos extraíbles. Al final, el ataque dirigido se dará por dos vectores distintos a través de una memoria USB o por medio del correo electrónico. Un mismo ataque, pero medios distintos (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion).

Fase III: Distribución de posters de inicio y trípticos.

Se comienza la fase de concienciación en ciberseguridad. Se distribuyen los posters de inicio y trípticos del kit de concienciación. Los posters y trípticos serán colocados en lugares visibles para ser leídos por los colaboradores que empezarán el proceso formativo (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion).

Fase IV: Proceso formativo

El proceso formativo se distribuirá los recursos formativos del kit que incluye 9 recursos formativos distribuidos en 6 temáticas distintas, las cuales son: la información, el correo electrónico, contraseñas, el puesto de trabajo, Boyd y teletrabajo, por último, las redes sociales. Cada uno de los temas será impartido por el instructor en ciberseguridad (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion).

Fase V: Recordatorio de ataque

Se pondrá a prueba nuevamente al usuario y se evaluará por última el nivel de concienciación en ciberseguridad después de haber recibido el proceso formativo para esto se realizarán los siguientes ataques: ataque dirigió con Gophish, Ataque dirigido mediante enlace malicioso en el correo y Ataque dirigido mediante USB, cada uno de ellos será realizado con un nivel de dificultad mayor para dificultar la detección por el usuario (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion).

Fase VI: Encuesta de satisfacción

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 8 – Número 1
enero-junio 2025
pp. 65-72

Finalizadas las fases, se proporcionará a los usuarios formados una encuesta para conocer el nivel de satisfacción de esta experiencia y así obtener críticas constructivas para mejor el plan de ser necesario (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion).

La planificación este plan se hará de acuerdo con la propuesta planteada en la **Tabla 1** (INCIBE, s.f. Kit de Concienciacion, Manual de Implantacion), esta será gestionada a nivel de proyecto de acuerdo con los cinco grupos de la administración de proyectos (Inicio, Planificación, Ejecución, Monitoreo y Control, y Cierre) planteados en la guía PMBOK de administración de proyectos de la organización Project Management Institute (PMI).

Tabla 1.

Duración de las diferentes partes del Kit

Tarea	Duración
Ataque dirigido con Gophish	5 días laborales
Descanso entre ataques	5 días laborales
Ataque dirigido memoria USB	5 días laborales
Descanso entre ataques	5 días laborales
Ataque enlace malicioso correo	5 días laborales
Distribución posters presentación y trípticos	1 días laborales
Recurso formativo	9 meses
Ataque dirigido con Gophish	5 días laborales
Descanso entre ataques	5 días laborales
Ataque dirigido memoria USB	5 días laborales
Descanso entre ataques	5 días laborales
Ataque enlace malicioso correo	5 días laborales
Encuesta de satisfacción	1 días laborales

CC BY NC SA

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Correo: faeco.sapiens@up.ac.pa
Volumen 8 – Número 1
enero-junio 2025
pp. 65-72

Fuente: https://www.incibe.es/protege-tu-empresa/kit-concienciacion

CONCLUSIONES

La tecnología utilizada en las universidades debe ir de la mano con medidas de ciberseguridad para su protección. Siempre apoyándose una a la otra, esto requiere aspectos como el uso de herramientas de seguridad informática por parte del departamento de seguridad, profesionales idóneos en el área preparados para contrarrestar y proteger a las universidades de ciber ataques y asistir en problemas de seguridad informática, pero, sobre todo usuarios concienciados en ciberseguridad.

Se requiere despertar a la comunidad académica y administrativa de las universidades en Panamá sobre el peligro de no tomar medidas adecuadas para salvaguardar tanto su información personal como la información sensitiva de la institución, por lo tanto, el instruir al usuario de que su información no está 100% protegida, que en sí la seguridad no solo depende de los profesionales del área sino de todos nosotros, es decir, es un trabajo en conjunto, entonces veremos cambios y así una reducción de riesgos en seguridad. Con la implementación de este plan lograremos el comienzo de un despertar sobre la importancia de educarnos sobre ciberseguridad y así poco a poco crear una cultura de concienciación, de tal manera que se realicen planes de concienciación anuales a los diferentes departamentos que conforman la universidad y sobre todo ir generando campañas de concienciación con el propósito de que la ciberseguridad sea un tema de importancia en nuestras vidas.

REFERENCIAS BIBLIOGRÁFICAS

Deloitte, «Deloitte.com,» junio 2018. https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/ciberamenazas-alertan-universidades.html.

Elderecho.com. 3 junio 2024. El 80% de los ciberataques corporativos están dirigidos a los empleados. https://elderecho.com/el-80-de-los-ciberataques-corporativos-estan-dirigidos-a-los-empleados#:~:text=recuerda%20Mu%C3%B1oz%2DAycuens.-,El%2080%25%20de%20los%20ciberataques%20corporativos%20est%C3%A1n%20dirigidos%20a%20los,a%20trav%C3%A9s%20malware%20o%20phishing

Guía PMBOK de administración de proyectos de la organización Project Management Institute (PMI). 2021.

Instituto Nacional de Ciberseguridad (INCIBE), s.f. Manual de Implementación de la Herramienta Gophish, España.

Kit de Concienciacion, Manual de Implantacion, Instituto Nacional de Ciberseguridad, incibe.es, s.f. https://www.incibe.es/empresas/formacion/kit-concienciacion

M. Á. Mendoza, 16 junio 2015. https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/.

Noelia García, «elEconomista.es,». 17 octubre 2019.. https://www.eleconomista.es/ecoaula/noticias/10144866/10/19/Ciberseguridad-Las-universidades-son-las-terceras-instituciones-mas-atacadas.html

O. A. Jaramillo, 20 agosto 2019. https://www.prensa.com/impresa/panorama/Contencion-llega-educacion-superior_0_5376962304.html

Rodolfo Pilipiak, 2 agosto 2019. https://www.metrolibre.com/opinion/riesgos-de-ciberseguridad-en-las-universidades-PDML134865.

Universidad de Cádiz, s.f.. https://sistinfo.uca.es/seguridad/pdcon/.

Universidad Internacional de Valencia, universidadviu.com, 21 marzo 2018. https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/.