MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE TITULACIÓN

Modalidad Proyecto de Investigación y Desarrollo

Implementación de Campaña de Concientización en Ciberseguridad

Autor: Jonathan Michael Guarnizo Fernández

Guía: Roque Jacinto Hernández Bustos

Presentando como parte de los requisitos para el título de magister en ciberseguridad.

Guayaquil, 1 de marzo del 2024

PROPUESTA DE CLÁUSULA DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE TITULACIÓN

Yo, GUARNIZO FERNÁNDEZ, JONATHAN MICHAEL, autor del trabajo de titulación “Implementación de Campaña de Concientización en Ciberseguridad”, certifico que el ensayo reflexivo es una creación de mi autoría, por lo que sus contenidos son originales, de exclusiva responsabilidad de su autor y no infringen derechos de autor de terceras personas. Con lo cual, exonero a la Universidad Casa Grande de reclamos o acciones legales.

GUARNIZO FERNÁNDEZ, JONATHAN MICHAEL
0926793472

GUARNIZO FERNÁNDEZ, JONATHAN MICHAEL en calidad de autor y titular del trabajo de titulación "Implementación de Campaña de Concientización en Ciberseguridad" para optar por la **Maestría en Ciberseguridad**, autorizo a la Universidad Casa Grande para que realice la digitalización y publicación de este trabajo de titulación en su Repositorio Digital de acceso abierto, con fines estrictamente académicos, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Asimismo, autorizo a la Universidad Casa Grande a reproducir, distribuir, comunicar y poner a disposición del público mi documento de trabajo de titulación en formato físico o digital y en cualquier medio sin modificar su contenido, sin perjuicio del reconocimiento que deba hacer la Universidad sobre la autoría de dichos trabajos.

GUARNIZO FERNÁNDEZ, JONATHAN MICHAEL
0926793472

MAESTRÍA EN CIBERSEGURIDAD

Implementación de Campaña de Concientización en Ciberseguridad

Elaborado por: Ing. Jonathan Guarnizo F.

1/Marzo/2024

Contenido

Ilustraciones

Introducción:

En un mundo digitalizado en constante evolución, la seguridad de la información es una preocupación esencial tanto para individuos como para organizaciones. Con el aumento de las amenazas cibernéticas y los ataques cada vez más sofisticados, la conciencia sobre la ciberseguridad se vuelve fundamental.

> *"La ciberseguridad no es solo una preocupación tecnológica; es una preocupación de seguridad nacional, seguridad económica y seguridad personal." (Schneier, 2019)*

Cada una de las materias mencionadas a continuación me ayudaron a poder gestionar y comprender el papel fundamental en la comprensión y la gestión efectiva de la ciberseguridad en una organización. Aquí detallo la importancia de cada una de ellas:

- Estrategias y Políticas Multilaterales para la Ciberseguridad:

  Esta materia es crucial porque proporciona un marco para la prevención y respuesta a ciberataques. Al profundizar en la importancia de la seguridad a nivel social y organizacional, se establecen políticas integrales que anticipan posibles ataques y garantizan planes de contingencia claros. Estas políticas son esenciales para mantener la continuidad del negocio y proteger los activos de la organización en caso de emergencia. Además, al examinar estrategias para garantizar el cumplimiento efectivo de estas políticas, se promueve una cultura de seguridad en toda la organización.

- Continuidad del Negocio:

  Esta materia es fundamental porque enfoca en la preparación ante la imprevisibilidad de los ciberataques. Al reconocer que rara vez se recibe una advertencia previa, se destaca la importancia de contar con un plan de

continuidad del negocio. Este plan, actualizado y conocido por todo el personal relevante, asegura una respuesta efectiva ante cualquier incidente. La capacidad de mantener las operaciones críticas durante y después de un ciberataque es esencial para la supervivencia y la resiliencia de la organización.

- Gerencia, Operación y Planificación de la Ciberseguridad:

  Esta materia es esencial porque proporciona las habilidades y conocimientos necesarios para gestionar eficazmente la seguridad cibernética en la organización. Al abordar aspectos como el control interno de sistemas, la planificación estratégica y el gobierno corporativo, se establece una base sólida para la implementación de políticas y procedimientos de ciberseguridad. Además, al promover el desarrollo de habilidades de toma de decisiones y la reflexión crítica sobre eventos actuales, se prepara a los estudiantes para enfrentar los desafíos en constante evolución del panorama de la ciberseguridad.

- Hacking Ético y Análisis del Ciberataque:

  Esta materia es vital porque proporciona a los estudiantes una comprensión profunda de las amenazas cibernéticas y las técnicas utilizadas por los actores malintencionados. Al abordar desde conceptos básicos hasta técnicas avanzadas de hacking ético, los estudiantes adquieren habilidades prácticas para identificar y mitigar riesgos de seguridad. Además, al aprender sobre herramientas y contramedidas necesarias para proteger sistemas y redes, los estudiantes están mejor preparados para enfrentar desafíos en el ámbito laboral de la ciberseguridad. La conciencia de estas técnicas y contramedidas ayuda a los empleados a reconocer y responder eficazmente a posibles amenazas, lo que subraya la importancia de las campañas de concientización de ciberseguridad.

- Ciberseguridad Ubicua:

  Esta materia es esencial porque destaca la omnipresencia de la tecnología en la vida cotidiana y resalta la importancia de la seguridad en todos los dispositivos conectados a Internet. Al comprender que estamos constantemente rodeados de tecnología, desde teléfonos inteligentes hasta sistemas de navegación en automóviles, los estudiantes se vuelven más conscientes de los riesgos de seguridad asociados con estos dispositivos. Esta conciencia promueve una cultura de seguridad cibernética en la que los empleados están más alerta y comprometidos con la protección de la información y los sistemas en su entorno digital. Por lo tanto, la implementación de campañas de concientización de ciberseguridad se vuelve aún más crucial para educar a los empleados sobre cómo protegerse adecuadamente en un mundo digitalizado.

Antecedentes:

"La ciberseguridad es un desafío constante en el mundo actual, donde cada vez más nuestras vidas, trabajos y datos están interconectados en línea. Protegerse contra las amenazas cibernéticas es esencial para la supervivencia y el éxito de cualquier empresa." (Mitnick, 2018)

Tomando en consideración 2 análisis, para que se entienda y se vea lo critico e importante el llevar a cabo una campaña de concientización en ciberseguridad, se realizó a través del portal Kasperky.com un monitoreo, y verificando las cantidades de notificaciones recibidas se pudo observar lo siguiente:

En el primero se puede monitorear que hay tráfico relevante que sirve para darnos cuenta de la existencia de ataques a nivel de CORREOS ELECTRONICOS MALICIOSOS, este escaneo fue realizado para el día 17/febrero/2024

Ilustración 1. Escaneo de amenazas sobre Correos Maliciosos

Fuente:https://statistics.securelist.com/es/country/rep%C3%BAblica%20del%20ecuador/mail-anti-virus/day

En el segundo escaneo se puede monitorear que hay tráfico relevante que sirve para darnos cuenta que la existencia de ataques a nivel de SECUESTRO DE DATOS, este escaneo fue realizado de manera mensual, desde 20/Enero/2024 hasta 17/Febrero/2024

Ilustración 2. Escaneo mensual de Secuestro de datos

Fuente:

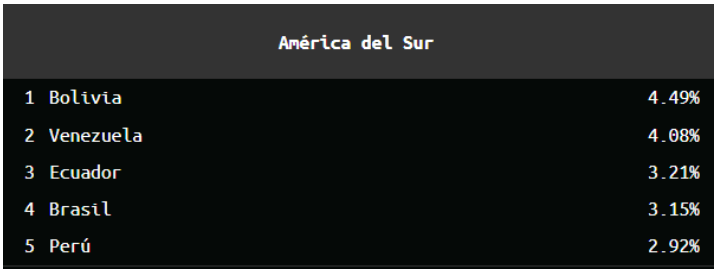
https://statistics.securelist.com/es/country/rep%C3%BAblica%20del%20ecuador/ransomware/month

"En un mundo donde la información es el activo más valioso, la ciberseguridad se ha convertido en una necesidad imperativa. Las empresas deben estar preparadas para defenderse contra los ataques cibernéticos que pueden tener repercusiones devastadoras en su reputación y operaciones." (Payton, 2020)

Para comprender la importancia de las campañas de concientización en ciberseguridad, es crucial reconocer el entorno actual de amenazas cibernéticas en el que operan individuos y organizaciones. El panorama de la ciberseguridad está en constante evolución, con nuevas vulnerabilidades y ataques emergentes con regularidad. Desde el phishing hasta el ransomware, los ciberdelincuentes emplean una variedad de tácticas para comprometer la seguridad de la información y causar daño a usuarios y empresas.

La siguiente imagen nos muestra un escaneo en tiempo real de lo que fue el mes pasado ENERO 2024 solo en América del Sur, en donde se puede observar que Ecuador ocupó el tercer puesto como el país con más generación de trafico de posibles ataques.

Ilustración 3. Top 5 del último mes de países con más notificaciones de ataques



Fuente: https://cybermap.kaspersky.com/es/stats

En este contexto, la concientización se convierte en una defensa fundamental contra las amenazas cibernéticas. Las campañas de concientización en ciberseguridad tienen como objetivo educar a los usuarios sobre las mejores prácticas de seguridad, desde la creación de contraseñas seguras hasta la identificación de correos electrónicos maliciosos. Al aumentar el conocimiento y la comprensión de las amenazas cibernéticas, los individuos pueden tomar medidas proactivas para protegerse a sí mismos y a sus organizaciones.

La importancia de estas campañas se vuelve aún más evidente cuando se considera el impacto potencial de un ataque cibernético. Las consecuencias de una violación de seguridad pueden ser devastadoras, desde la pérdida de datos confidenciales hasta el daño a la reputación y la pérdida financiera. Por lo tanto, invertir en la concientización en ciberseguridad no solo es una medida preventiva, sino también una estrategia de gestión de riesgos esencial para mitigar el impacto de posibles ataques.

En el caso específico mencionado en la introducción, donde se solicitó la implementación de una campaña de concientización en ciberseguridad en el lugar de trabajo, se reconoce la iniciativa proactiva de la empresa para abordar esta preocupación crítica. Al aprovechar el conocimiento y la experiencia en ciberseguridad del personal, se puede desarrollar una campaña efectiva que se adapte a las necesidades y desafíos específicos de la organización.

La propuesta de una campaña de concientización en ciberseguridad debe considerar una variedad de temas relevantes, desde la protección de contraseñas hasta la detección de amenazas en línea. Además, es importante utilizar múltiples canales de comunicación, como correos electrónicos, carteles y sesiones de capacitación, para llegar a todos los miembros de la organización y garantizar la máxima participación y comprensión.

Además de la implementación de la campaña en el entorno laboral, también es esencial extender la concientización sobre la ciberseguridad a otros aspectos de la vida cotidiana. Con la creciente dependencia de la tecnología en el hogar y en la sociedad en general, la educación sobre ciberseguridad se vuelve igualmente relevante para proteger la información personal y familiar.

Implementación

Se presento 2 propuestas de campañas a Gerencia, en la cual se basa en informar mediante Flayer informativos temas sobre la seguridad de la información, estos temas serán presentados mensualmente y enviado a los correos de cada usuario. La propuesta escogida fue la segunda (Se puede observar en el archivo ***Propuesta de campaña de concientización.pdf***), en la cual se especifica que dentro de cada mes muy aparte de socializar el tema, se realizará una evaluación tipo trivia con preguntas y respuesta y de

esta manera poder conocer y monitorear la cultura de seguridad que tienen los usuarios de la empresa y así sacar conclusiones para de ser el caso reforzar temas.

Esta implementación se esta ejecutando en este momento, y se comenzó con el tema: ESTAFAS EN LINEA, para lo cual trabaje en ideas puntuales que pueden ayudar al usuario a tomar precauciones cuando se topen con posibles estafas.

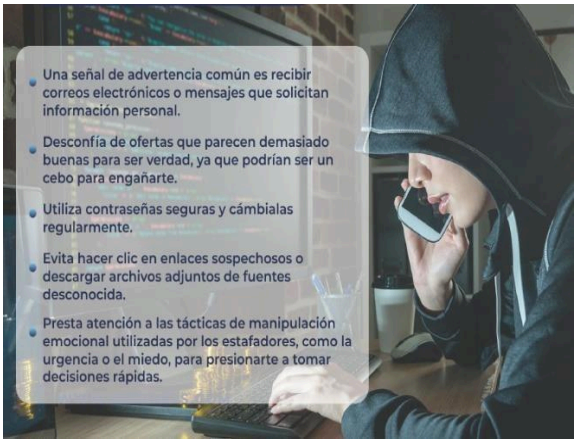
A continuación, se muestra una imagen donde se evidencia el trabajo realizado en mi lugar de trabajo, donde una vez finalizada mis ideas del tema, fueron pasadas para que sean plasmadas en unos Flayer.

Ilustración 4. Evidencia de trabajo de elaboración de Flayer

Como producto final se obtuvo estos 3 Flayer que posteriormente se enviaron por correo a todas las empresas del Grupo.

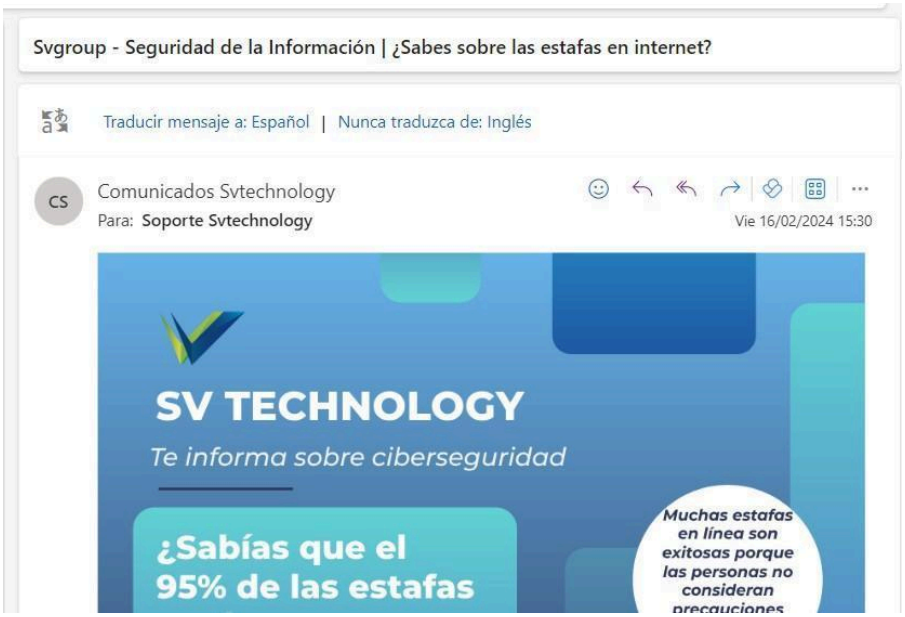
Ilustración 5. Flayer informativos sobre ESTAFAS EN LINEA


SV TECHNOLOGY
Te informa sobre ciberseguridad
¿Sabías que el 95% de las estafas en línea ocurren por errores humanos?
Muchas estafas en línea son exitosas porque las personas no consideran precauciones antes de navegar en internet
Te damos 5 tips para que tengan en cuenta y estén alertas ante cualquier intento de una posible estafa en línea:


Una señal de advertencia común es recibir correos electrónicos o mensajes que solicitan información personal.
Desconfía de ofertas que parecen demasiado buenas para ser verdad, ya que podrían ser un cebo para engañarte.
Utiliza contraseñas seguras y cámbialas regularmente.
Evita hacer clic en enlaces sospechosos o descargar archivos adjuntos de fuentes desconocida.
Presta atención a las tácticas de manipulación emocional utilizadas por los estafadores, como la urgencia o el miedo, para presionarte a tomar decisiones rápidas.


Ejemplo de una estafa hecha a Supermaxi
SUPERMAXI
MEGAMAXI
+593 98-029-4436
https://lafavoritaec.com
FALSO
COMUNICADO OFICIAL

Ilustración 6. Flayer socializado con todas las empresas



Conclusión

En resumen, las campañas de concientización en ciberseguridad desempeñan un papel fundamental en la protección de la información y la mitigación de riesgos en un mundo digitalizado. Al educar a los usuarios sobre las amenazas cibernéticas y las mejores prácticas de seguridad, se fortalece la postura de seguridad de las organizaciones y se reduce la probabilidad de sufrir un ataque cibernético costoso. Por lo tanto, es imperativo que las empresas y los individuos inviertan en la concientización en ciberseguridad como una medida preventiva y proactiva para salvaguardar sus activos digitales y protegerse contra las crecientes amenazas en línea. La implementación de

campañas efectivas de concientización en ciberseguridad no solo protege a las organizaciones y a los individuos de posibles ataques, sino que también contribuye a la creación de una cultura de seguridad cibernética en la que todos puedan participar activamente en la protección de la información sensible y en la prevención de incidentes cibernéticos. En última instancia, la concientización en ciberseguridad no es solo una necesidad, sino una responsabilidad compartida que requiere la colaboración de todos los involucrados para garantizar un entorno digital seguro y protegido para las generaciones futuras.

Referencias

Mitnick, K. (12 de Marzo de 2018). Forbes - "The Importance of Cybersecurity in Today's Digital World". Nueva York, Estados Unidos.

Payton, T. (5 de Julio de 2020). CNN Business - "The Critical Need for Cybersecurity in Modern Business". Atlanta, Georgia, Estados Unidos.

Schneier, B. (09 de Septiembre de 2019). The Washington Post - "Why Cybersecurity Matters for National Security". Washington D.C., Estados Unidos.

ANEXO 1

Enlace a Evidencias de Aprendizaje

https://jonathanguarnizo.wixsite.com/maestriaucg/portfolio

ANEXO 2

Enlace a Proyecto y/o Propuesta de Implementación

https://jonathanguarnizo.wixsite.com/maestriaucg/presentaci%C3%B3n