Carrera de Computación

Título:

Informe Creando Conciencia Universidad Politécnica Salesiana

Asignatura:

Seguridad de la información

Estudiantes:

Adrián Viscaino

Bryam Barrera

Pedro Illaisaca

Docente:

Ing. Jennifer Yepez

Cuenca, 3 de enero 2022

1. **Objetivo del plan.**

   Capacitar a los miembros de la comunidad universitaria sobre las posibles amenazas a las que está expuesta la información de los usuarios dentro del ámbito académico, dándoles a conocer cada una de ellas y cómo actuar respecto a las mismas para evitar situaciones que comprometan la información y afecte al funcionamiento de la institución.

2. **Duración.**

   El tiempo elegido para el presente proyecto de concienciación será de tres meses los cuáles serán aplicados en un periodo académico impar (marzo – agosto del año en curso), aprovechando que en este tipo de periodos no contamos con muchas épocas vacacionales que puedan intervenir con el programa de concientización.

3. **Grupos de usuarios que serán entrenados.**

   - **Personal administrativo**
     Comprende a todas las personas que trabajen en áreas de coordinación académica y que tengan acceso a información crítica de los estudiantes, docentes y administradores de la universidad, si sus cuentas llegan a ser afectadas, la perdida de la información podría comprometer la integridad y disponibilidad de la misma. Algunos ejemplos son, datos de estudiantes, datos de docentes, acceso a cuentas, notas de estudiantes, etc. Además, realizar una capacitación a este grupo de usuarios, derivara en que sus colaboradores también se vean capacitados de manera indirecta, ampliando el alcance de la capacitación con menos recursos.
   - **Docentes**
     Profesores de carrera, tutores y sus colaboradores, son expuestos a robo de información debido a su contacto con estudiantes y a que se movilizan entre aulas y oficinas, quedando expuestos al robo de sus dispositivos físicos o simplemente a que un tercero pueda acceder a sus equipos dentro de un aula de clases, la integridad de la información de los estudiantes, en específico asistencias, notas y registros podría verse comprometida afectando su trabajo y el control de los estudiantes.
   - **Estudiantes**
     Este grupo debe ser capacitado debido al constante ataque e intento de robo de la información por medio de correos electrónicos, además, el compartir contraseñas con compañeros puede comprometer el resto de sus cuentas si no se tiene un correcto manejo y uso de contraseñas distintas para las cuentas.

4. **Temáticas.**

   a. **Ingeniería Social, técnica Phishing**

      Es un modo de operación fraudulento comúnmente usado por atacantes que aprovechan la ingenuidad y desconocimiento de las víctimas para acceder información confidencial por ejemplo contraseñas. Cuando el usuario comprende la finalidad de este tipo de ataque ya no es presa fácil para los ciberdelincuentes. El

cuanto al objetivo en el plan del presente informe el nivel de aportación es alto porque se enfoca principalmente en el usuario.

b. Contraseñas y autenticación

Es un elemento muy sencillo que la mayoría de los usuarios comprende y usa a diario en la mayoría de sus cuentas, sin embargo, estas contraseñas deben cumplir con ciertos parámetros para asegurarse que estas sean seguras y confiables, cuando se utilizan contraseñas no seguras es mucho más sencillo para los ciberdelincuentes robar la información.

c. Seguridad física

La seguridad física comprende cualquier elemento palpable o físico que pueda comprometer la seguridad de las cuentas o de los dispositivos electrónicos, en este tipo de seguridad podemos referirnos a realizar acciones como tener las contraseñas escritas en algún papel junto a una computadora, no asegurar el espacio físico donde se encuentran los dispositivos electrónicos, no utilizar elementos de seguridad como cámaras, métodos de autenticación para el acceso al espacio físico, etc. Si un dispositivo electrónico es descuidado puede verse comprometido a distintos tipos de ataques, desde robo de información y recursos, hasta el acceso a otros equipos de la red.

d. Wi-Fi público

Dentro de este tipo de seguridad es importante concientizar a los usuarios que una red pública está abierta a todos los usuarios, por lo tanto, personas desconocidas pueden acceder a nuestra información por medio de la red, por ello es importante tener conocimiento de si la red por la cual se está conectado es una red de confianza y además de ello tomar medidas necesarias para proteger los dispositivos.

e. Uso de las redes sociales

Las redes sociales se han vuelto uno de los medios de comunicación más utilizados en la actualidad, por ello, la información que exponemos a través de estas es amplia y puede llegar a ser aprovechada por terceros para distintos fines, cuando se comparte información personal como: números de teléfono, correos, nombres de familiares, lugares de residencia, actividades, lugares de trabajo, etc. Estamos brindando a los ciberdelincuentes herramientas para realizar ataques.

f. Uso de Internet y del correo electrónico

El uso de internet en la vida cotidiana se ha vuelto tan necesario que la mayor parte de las actividades se realizan a través de él, sin embargo, al usar esta tecnología estamos abriendo las puertas de nuestros dispositivos al mundo, una de las formas de utilizarlos es haciendo uso del correo electrónico, por el cual muchos atacantes consigue información de sus víctimas por medio de correos maliciosos, correos falsos, que buscan engañar y obtener información de los usuarios, además de, el uso de contraseñas simples y repetidas muchas veces pueden facilitar los ciberataques.

g. Seguridad en la nube

La computación o seguridad en la nube ha sabido revolucionar a grandes y pequeñas empresas y la forma de almacenar y acceder a los datos. Estas aplicaciones transforman empresas, pero el hecho de que se esté almacenando una gran cantidad de datos privados de manera remota atrae el riesgo de que se produzcan hackeos de alto nivel. Grandes empresas que se dedican a la seguridad de la información están trabajando en la protección de datos, pero si elegimos a un proveedor de servicios en la nube adecuado, el almacenamiento en la nube puede ser una forma mucho más segura y rentable de almacenar los datos de una empresa.

5. Recursos formativos.

a. Seguridad Física
b. Seguridad en la nube
c. Pishing

6. Distribución de los recursos formativos.

Tomando en cuenta que disponemos de tres recursos y tres meses de tiempo procedemos a aplicar un recurso por mes, el recurso **Ingeniería Social, técnica Phishing** será el primer en ser lanzado por medio del correo institucional de los tres grupos objetivo, el segundo mes el recurso **Seguridad Física** debe ser aplicado para ello se podría aprovechar alguna reunión como, por ejemplo, para el grupo de estudiantes realizarla en la asamblea de carrera. Finalmente, el último recurso **Seguridad en la Nube** será aplicado por el medio de la plataforma virtual para el grupo de estudiantes donde se les pedirá realizar el Quiz como por ejemplo las evaluaciones a los docentes, con el fin de educar a los estudiantes sobre la seguridad de su información.

7. Anexos

a. Seguridad Física Posteada en: https://www.pinterest.com.mx/pin/653936808403941060/

SEGURIDAD FÍSICA

La informacion corre peligro tanto en los sistemas como en los equipos donde es almacenada y tratada

¿QUÉ ES?

ES EL PROCESO POR EL CUAL APLICAMOS UNA SERIE DE BARRERAS DE TIPO FÍSICO, ASÍ COMO PROCEDIMIENTOS DETERMINADOS AL REDEDOR DE LOS EQUIPOS INFORMATICOS DE MANERA QUE EL ACCESO A ESTOS NO SEA SENCILLO, DE ESA FORMA LA INFORMACIÓN CONFIDENCIAL QUE EXISTA EN NUESTRO NEGOCIO SIEMPRE ESTÉ A BUEN RECAUDO.

¿DE QUE HAY QUE PROTEGERSE?

ACCESO NO AUTORIZADO

Los equipos físicos deben ubicarse en instalaciones seguras, para que solo las personas que tengan acceso a ellos puedan acceder, el uso de tarjetas o lectores biométricos son de gran ayuda.

ROBO DE EQUIPOS

Una de las situaciones mas comunes, sobre todo cuando se tiene la necesidad de llevar un dispositivos a distintos lugares. Se debe asegurar los equipos informáticos para evitar su perdida, por ejemplo el uso de candados para laptops, además de las perdidas materias, los computadores personales y celulares puede contener información delicada como contraseñas y cuentas.

ERRORES HUMANOS

Para un sistema, el usuario es su principal amenaza, los equipos pueden quedar vulnerables cuando un usuario descuida sus contraseñas y el acceso a los equipos, se deben evitar situaciones como escribir contraseñas en papeles o recordatorios y dejarlos a la vista, no usar metodos de autenticacion en los equipos o olvidar cerrar puertas de acceso a los equipos., para esto se hace uso de tecnicas como la doble autenticacion, el bloqueo automatico, etc.

DESASTRES NATURALES

Estos eventos son impredecibles, sin embargo, las instalaciones adecuadas reducirian en gran magnitud la perdida de la informacion, algunas situaciones que pueden presentarse son: incendios, inundaciones, terremotos, etc. Por ello es importante asegurar que la infraestructura de los equipos este adecuada a estas situaciones.

UTILIZA MECANISMOS DE PROTECCION PARA TUS EQUIPOS Y NO LOS DESCUIDES, EN ELLOS SE ENCUENTRA TU INFORMACION.

b. **Ingeniería Social, técnica Phishing**

Video

Crear Conciencia Phishing

c. **Seguridad en la nube**

Prueba de evaluación de conocimientos

https://TopgradeApp.com/playQuiz/seguridad-en-la-nube-quiz