Curso: Seguridad Informática
Tarea: Tarea Unidad 1 20%

Roberto Carlos Delgado Fermán robertocardefe1234@gmail.com

Entrega

Entregado
Calificado
El estudiante puede editar esta entrega

Calificación

Calificación:

Hoja de presentación	No contien todos los datos 0puntos	Datos incompletos 1puntos	Completo 2puntos
Contenido	No cubre los temas 0puntos	La mitad de los temas 8puntos	Completo 16puntos
Archivo PDF	Sin formato 0puntos	Correcto 2puntos	

Calificación actual en el libro de calificaciones

20,00

INSTITUTO TECNOLOGICO SUPERIOR DE SAN ANDRES TUXTLA

CARRERA:

Ing. Informática 810

MATERIA:

Seguridad Informática

DOCENTE:

Juan Rafael González Cadena

INVESTIGACIÓN 1

ALUMNO:

Roberto Carlos Delgado Fermán

San Andrés Tuxtla Ver, febrero de 2023

SEGURIDAD INFORMÁTICA

1. El autor Álvaro Gómez, en su obra Enciclopedia de la Seguridad Informática, define el concepto de seguridad informática como: “cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.”

2. Sin embargo según plantea el [Decreto-Ley No. 199], “Seguridad Informática es un conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce o conserva por medio de las tecnologías de información”.

3. En el artículo de [Wikipedia, 2006], se formula que “la seguridad Informática, generalmente consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió”.

4. Para [Todos@cicese, 2002], “Seguridad Informática es el conjunto de recursos (métodos, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo e información, disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo”.

5. En [PC-News, 1996-2006], se plantea a la Seguridad Informática como,"el conjunto de reglas, planes y acciones que permiten garantizar la prestación de servicios y asegurar la información contenida en un sistema computacional". A partir de estas definiciones podemos decir que la Seguridad Informática es un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan las demás personas.

6. La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema**.**

7. Por su parte, Kissel (2012) la define como la protección de información y sistemas de información de acceso no autorizado.

8. La seguridad informática es conformada por medidas de seguridad, como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, como es la activación de la desactivación de ciertas funciones de software.

Curso: Seguridad Informática
Tarea: Exposición Unidad I 40%

Roberto Carlos Delgado Fermán robertocardefe1234@gmail.com

Entrega

Entregado
Calificado
El estudiante puede editar esta entrega

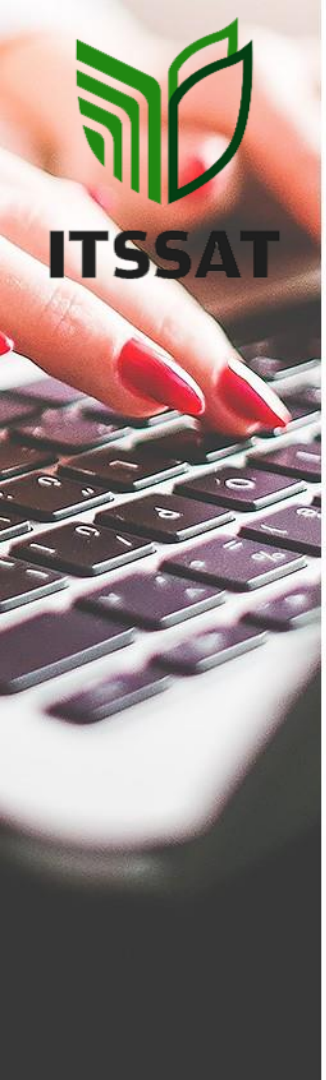
Calificación

Calificación:

Hoja de presentación	No contiene todos los datos 0puntos	Datos incompletos 1puntos	Completo 2puntos
Introducción	No contiene 0puntos	Muy pequeña 2.5puntos	Completa 5puntos
Contenido	No cubre los temas 0puntos	La mitad de los temas 6puntos	Completo 13puntos
Referencias IEEE	No contiene 0puntos	Una o no tiene el formato 2puntos	Más de una y formato correcto 4puntos
Conclusión	No contiene 0puntos	Muy pequeña 2.5puntos	Completa 5puntos
Archivo PDF	Sin formato 0puntos		Correcto 1puntos

Calificación actual en el libro de calificaciones

40,00



INSTITUTO TECNOLOGICO SUPERIOR DE SAN ANDRES TUXTLA

CARRERA:

Ing. Informática

MATERIA:

Seguridad Informática

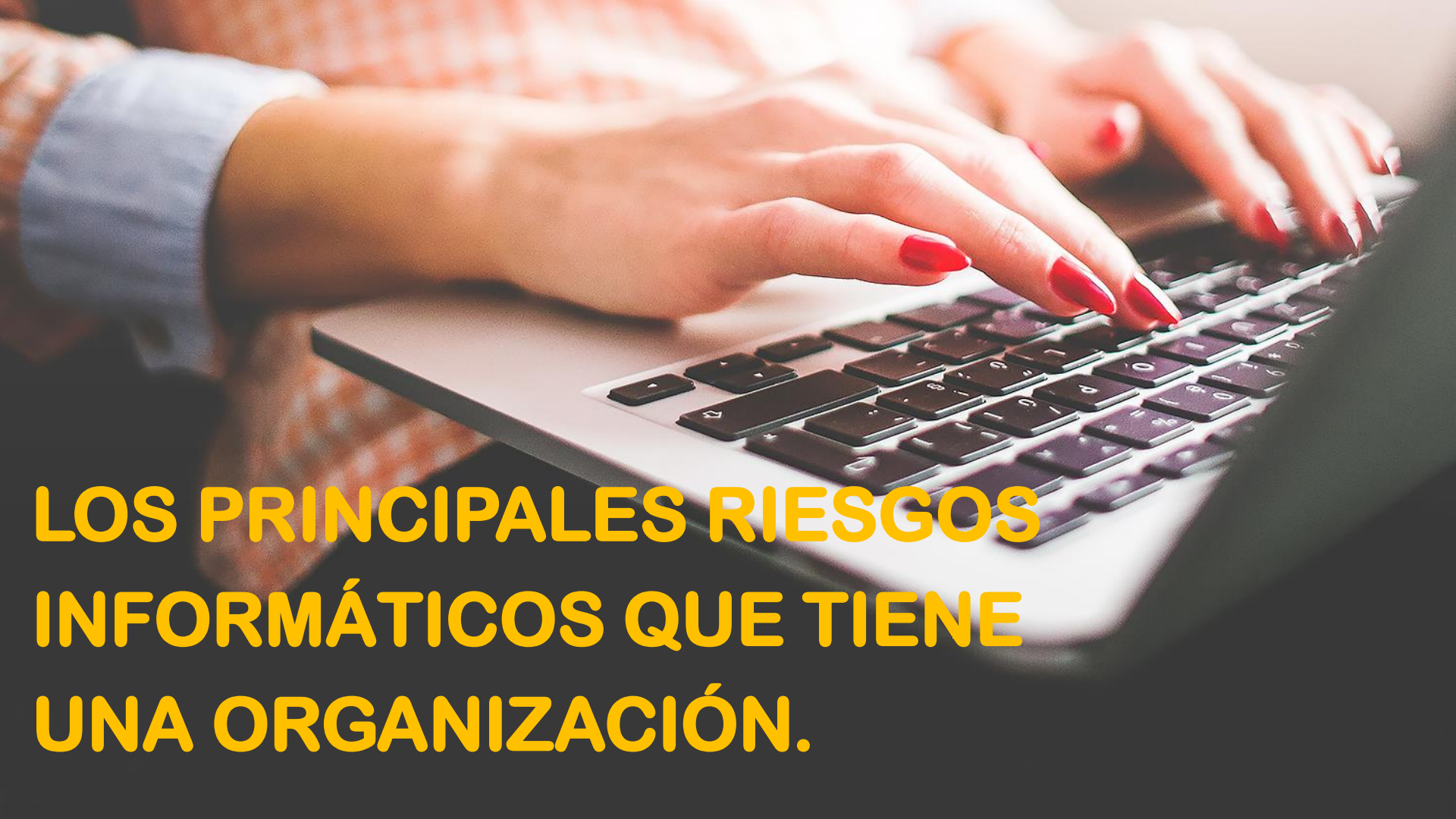
DOCENTE:

Juan Rafael González Cadena

INTEGRANTE:

Roberto Carlos Delgado Fermán

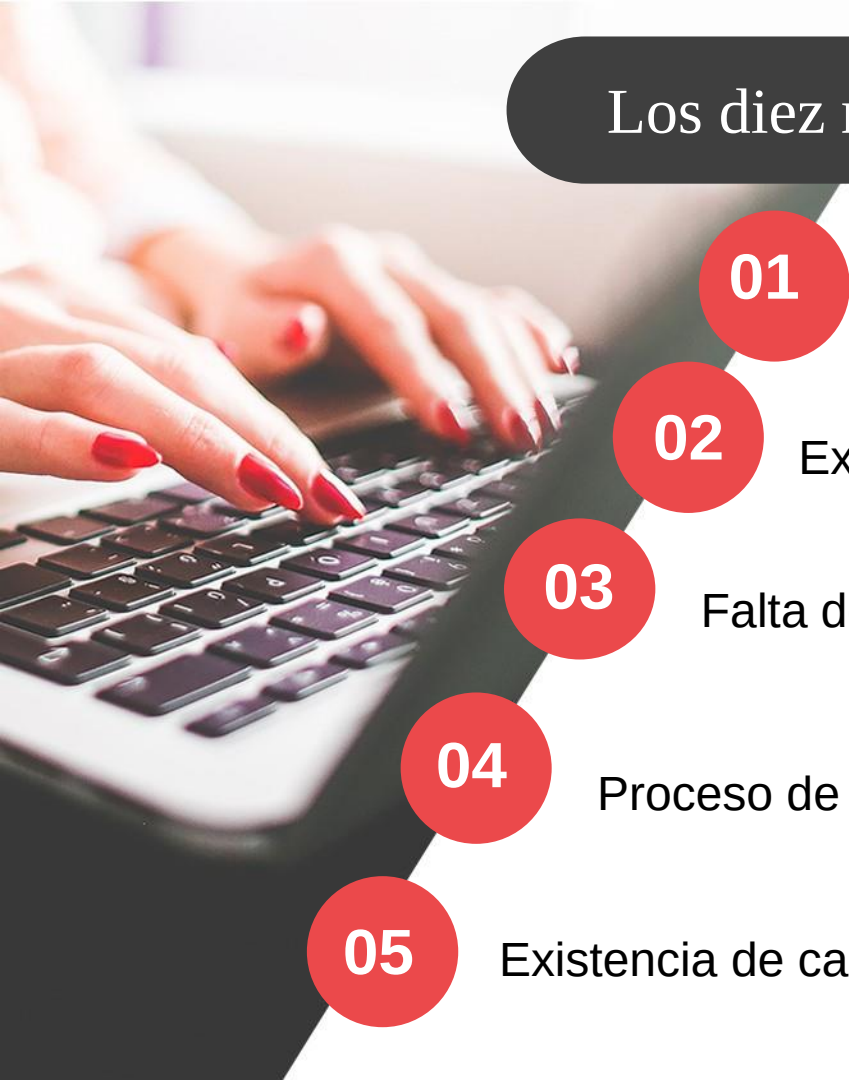
San Andrés Tuxtla Ver, marzo de 2023.



LOS PRINCIPALES RIESGOS INFORMÁTICOS QUE TIENE UNA ORGANIZACIÓN.

INTRODUCCIÓN

A continuación en la presente exposición se dará a conocer los principales riesgos informáticos que puede tener una organización. Los accidentes en los sistemas informáticos son de diversa índole y van desde la ruptura o robo de un dispositivo profesional con documentación relevante hasta cualquier circunstancia que pueda deteriorar el hardware y el software. Es por ello que hablaremos para poder detentar estos riesgos y poder prevenirlos.



Los diez riesgos son los siguientes:

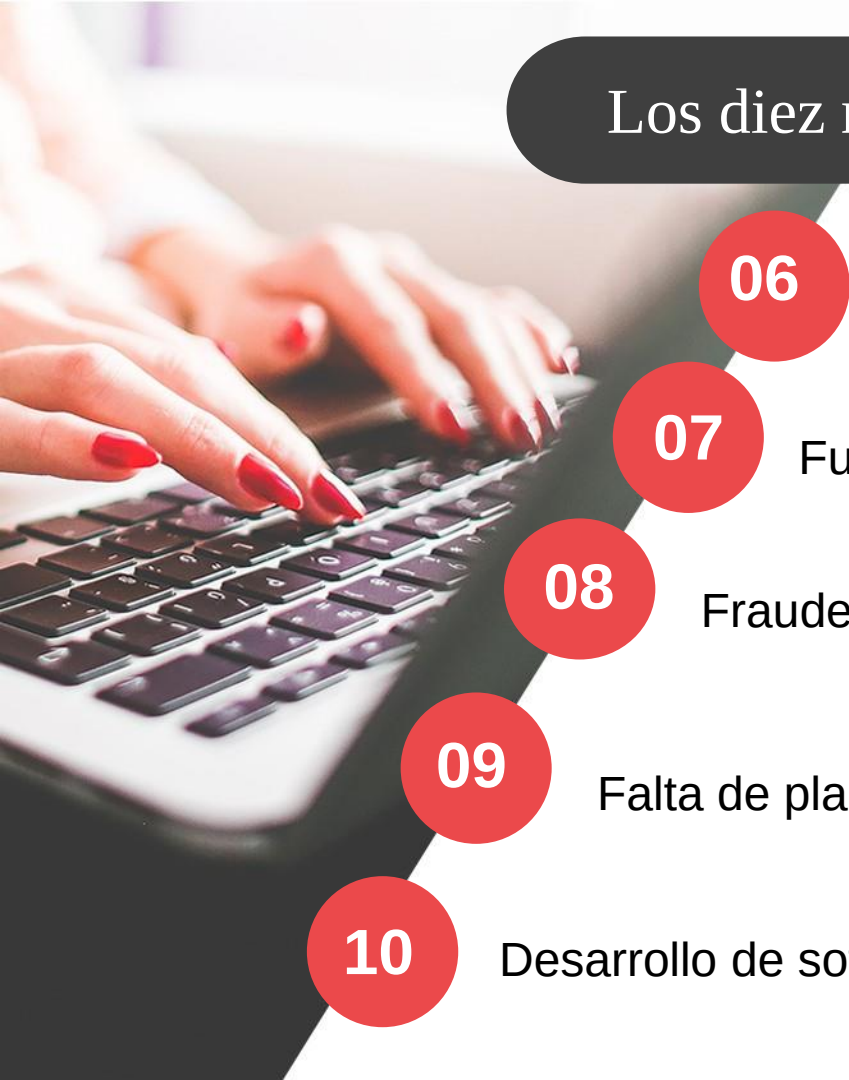
01 Deficiente control de acceso a las aplicaciones.

02 Existencia de vulnerabilidades web.

03 Falta de formación y concienciación.

04 Proceso de gestión de incidentes de seguridad.

05 Existencia de cambios regulatorios.



Los diez riesgos son los siguientes:

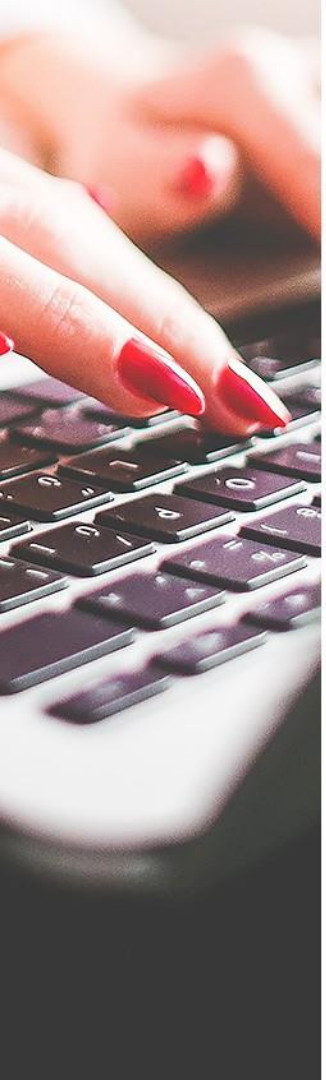
06 Control de acceso a la red.

07 Fugas de información.

08 Fraude y robo de información.

09 Falta de planificación de continuidad de negocio.

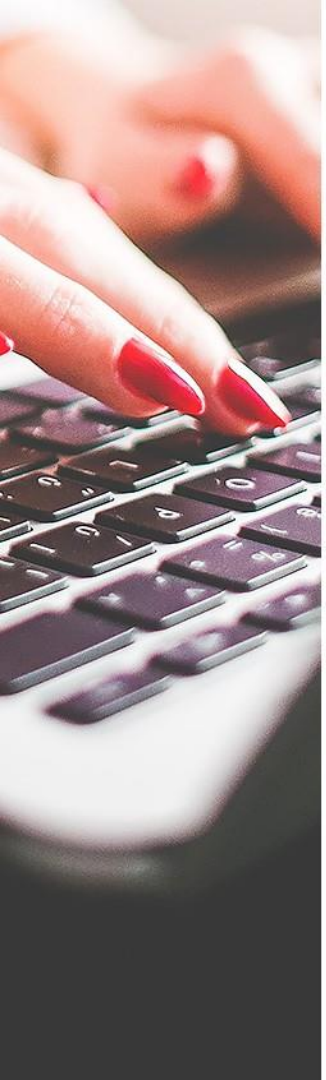
10 Desarrollo de software seguro.



¿QUÉ COMPORTAMIENTOS PROVOCAN RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS?

Las posibilidades de una vulneración de la seguridad informática de las empresas se puede deber tanto a factores externos como internos. Por eso, es importante conocer los comportamientos q ue ponen en riesgo la ciberseguridad de las empresas.

1. **Uso de dispositivos externos en equipos corporativos.**
2. **Uso de Redes Sociales en equipos corporativos.**
3. **Uso inadecuado de dispositivos móviles de la empresa.**
4. **Dejar los equipos sin bloquear o sin cerrar sesión.**
5. **Descargar archivos desde correos personales o Corporativos.**



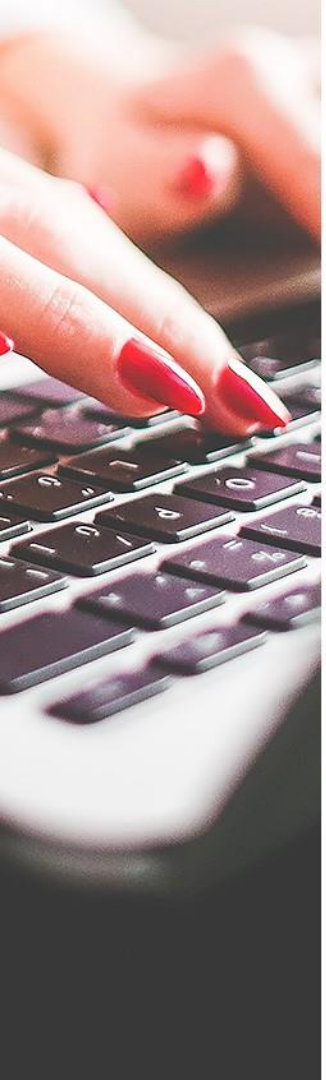
6. Subir archivos a la Nube sin cifrar.

7. Mala gestión de contraseñas y de permisos.

8. Falta de copias de seguridad.

9. Envío de correos masivos a clientes.

10. No informar de incidentes o problemas con los dispositivos corporativos.



TÉCNICAS MÁS UTILIZADAS PARA VULNERAR LA SEGURIDAD DE LOS DATOS

Un informe de Symantec revela datos importantes sobre amenazas de seguridad. Un 54,6% de los correos electrónicos que reciben los usuarios son spam. Además, cada usuario recibe una media de 16 emails maliciosos al mes.

Phishing: es la técnica más común. El ciberdelincuente recrea un sitio web conocido y confiable. A través de un enlace a dicha web clonada, el usuario comparte su información personal.

Vishing: consiste en el uso del Protocolo Voz sobre IP (VOIP) para suplant ar la identidad del usuario. Se usa una llamada telefónica para obtener infor mación sensible del afectado.

CONCLUSIÓN

Es importante tener en cuenta cuales son los riesgos pueden sufrir una organización ya que esto servirá para la detección de incidentes, es necesario mantener un estado de alerta y actualización.
Debido a la 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 grandes pérdidas.

BIBLIOGRAFÍA

elEconomista.es, “Las principales amenazas tecnológicas que sufren las empresas españolas,” *elEconomista.es*, 25-Nov-2014. [Online].

Disponible en: https://www.eleconomista.es/emprendedores-innova/noticias/6272627/11/14/Las-principales-amenazas-tecnologicas-que-sufren-las-empresas-espanolas.html. [Accesado: 16-Mar-2021].

Marketing, “¿Cuáles son los riesgos de ciberseguridad en las empresas?,” Tuyú Technology, 15-Apr-2019. [Online]. Disponible en: https://www.tuyu.es/riesgos-ciberseguridad-empresas/. [Accedido: 16-Mar-2021].

Curso: Seguridad Informática
Tarea: Examen Unidad I 40%

Roberto Carlos Delgado Fermán robertocardefe1234@gmail.com

Entrega

Entregado
Calificado
El estudiante puede editar esta entrega

Calificación 35%

Calificación:

Hoja de presentación	No contien todos los datos 0puntos	Datos incompletos 1puntos	Completo 2puntos
Introducción	No contiene 0puntos	Muy pequeña 2.5puntos	Completa 5puntos
Contenido	No cubre los temas 0puntos	La mitad de los temas 6puntos	Completo 18puntos
Referencias IEEE	No contiene 0puntos	Una o no tiene el formato 2puntos	Más de una y formato correcto 4puntos
Conclusión	No contien 0puntos	Muy pequeña 2.5puntos	Completa 5puntos
Archivo PDF	Sin formato 0puntos		Correcto 1puntos
Participación	NO 0puntos		SI 5puntos

Calificación actual en el libro de calificaciones

35,00

INSTITUTO TECNOLOGICO SUPERIOR DE SAN ANDRES TUXTLA

CARRERA:

Ing. Informática 810

MATERIA:

Seguridad Informática

DOCENTE:

Juan Rafael González Cadena

Principales Amenazas por Internet

ALUMNO:

Roberto Carlos Delgado Fermán

San Andrés Tuxtla, Ver. marzo de 2023

INTRODUCCIÓN

En el siguiente documento se abarcará sobre el tema de las principales amenazas del internet, hoy en día hay muchos tipos de amenazas y peligros presentes en la red. Son muchos los problemas que pueden afectar a nuestros dispositivos y poner en peligro nuestra seguridad y privacidad.

Están son causados por las vulnerabilidades que son fallos en el software informático que crean debilidades en la seguridad de tu ordenador o de tu red. Las vulnerabilidades también pueden producirse por configuraciones inadecuadas del ordenador o de la seguridad. Los piratas informáticos explotan estas debilidades, causando daños al ordenador o su información.

Cabe mencionar que las amenazas en internet han llegado a afectar instituciones como es el de la NASA, empresas como Facebook, Microsoft, Sony, gobiernos de todo el mundo y hasta millones de usuarios comunes que simplemente tomaron una mala decisión en línea.

A continuación, vamos a explicar qué amenazas podrían fácilmente atacarnos en Internet.

Principales Amenazas por Internet

En los últimos años, Internet se ha convertido en una herramienta indispensable para muchos y que nos puede acompañar en actividades tan cotidianas como hacer la compra o consultar nuestros extractos bancarios.

Cada vez más dispositivos se pueden conectar a la red**.** Dispositivos que, en muchos casos, llevamos encima, como es el caso de los smartphones, con los que es muy sencillo compartir en pocos segundos información tan delicada como nuestra ubicación. En la actualidad existen numerosas amenazas en la red tales como: virus informáticos, estafas, usurpación de datos personales... que pueden causarnos problemas innecesarios y hacer que nuestra experiencia en Internet sea totalmente amarga.

Cuando hablamos de amenazas en la red, lo primero que nos suele venir a la cabeza son los virus informáticos y los daños que pueden producir en nuestro equipo. Lo cierto es que este tipo de amenazas son muy reales y, en la actualidad, existe una gran cantidad de software malicioso circulando por la red esperando a ser instalado en algún equipo para actuar.

Sin embargo, las amenazas que podemos encontrar no son solo de esta naturaleza, ya que, podemos ser víctimas de engaños, anuncios falsos, abusos en las redes sociales... sin necesidad de que nuestro equipo se vea afectado.

MALWARE

Una de las principales amenazas con las que nos podemos encontrar en la red es el malware que se puede introducir en nuestro equipo. El término malware, hace referencia a "Malicious software", es decir, software malicioso. Al fin y al cabo, todo tipo de programa o código informático que tiene como objetivo dañar un equipo o causar su mal funcionamiento**.**

El malware puede llegar a nuestro equipo por distintas vías sin nosotros ser conscientes de ello. Estas son alguna de las principales fuentes por donde llega el malware a nuestro ordenador:

- **Correo electrónico:** Podemos recibir correos electrónicos con algún archivo adjunto malicioso y descargarlo en nuestro equipo.
- **Páginas web con descargas maliciosas:** Existen numerosas páginas donde podemos descargar sin saberlo archivos que pueden dañar nuestro equipo.
- **Chats:** Páginas para chatear con otros usuarios donde pueden compartirnos archivos dañinos haciéndonos creer que son inofensivos.
- **Medios extraíbles:** Los pendrives, CDs, DVDs... que conectamos a nuestro equipo pueden contener malware y sin nosotros saberlo, abrir estos archivos y que la seguridad de nuestro equipo se vea afectada.
- **Plugins para el navegador:** Los pequeños programas que se pueden añadir al navegador conocidos como pluggins, también pueden contener malware, sobre todo cuando se obtienen de fuentes desconocidas.
- **Instalación de software no original:** El software que no es original, no recibe el respaldo ni las actualizaciones del fabricante por lo que puede contener malware.
- **Programas P2P:** Programas en los que se comparten archivos directamente entre usuarios.

PHISHING.

Son la amenaza digital más común: los hackers envían correos electrónicos desde compañías, organizaciones falsas, o fingiendo ser otra persona, para recolectar información financiera, personal o claves de acceso.

Esta estrategia suena poco agresiva, pero es una de las más peligrosas. A veces logran redactar y presentar los correos de forma tan realista que para algunos resulta imposible pensar que no es la empresa o la persona que dice ser.

El phishing no es una técnica exclusiva de Internet, también existe el phishing telefónico, llegando a pedirnos contraseñas o datos bancarios directamente por teléfono.

Consejos para detectar el phishing:

1. Los mensajes suelen ser habitualmente en nombre de grandes empresas (Google, Apple, PayPal, entidades bancarias...) y son muy diferentes al tipo de comunicaciones que suelen dar las mismas.
2. Son impersonales con saludos genéricos: "estimado cliente", "querido amigo"...
3. Son alarmistas en muchas ocasiones. Pueden decirte que si no sigues con el proceso te van a cerrar la cuenta, te van a realizar algún cobro...
4. Los mensajes presentan fallos gramaticales o están mal redactados.
5. Nos obligan a tomar una decisión inminente. Nos dicen que disponemos de pocas horas para responder, realizar el pago... y de esta manera hacer que actuemos sin pensarlo detenidamente.

SPAM.

Es basura electrónica que llega por medio del correo. Alcanza los 90 mil millones de mensajes diarios en todo el mundo. Normalmente se distribuye cuando un Troyano (software malicioso que se presenta como un programa legítimo) se introduce en la computadora del usuario, toma las direcciones de correo electrónico de la agenda de contactos y hace un envío masivo de mensajes.

El correo basura mediante el servicio de correo electrónico nació el 5 de marzo de 1994. Este día una firma de abogados, Canter and Siegel, publica en Usenet un mensaje de anuncio de su firma legal; el día después de la publicación, facturó cerca de 10 000 dólares por casos de sus amigos y lectores de la red. Desde ese entonces, el marketing mediante correo electrónico ha crecido a niveles impensados desde su creación.

El correo basura por medio del fax (spam-fax), es otra de las categorías de esta técnica de marketing directo, y consiste en enviar faxes masivos y no solicitados a través de sistemas electrónicos automatizados hacia miles de personas o empresas cuya información ha sido cargada en bases de datos segmentadas según diferentes variables.

SPYWERE.

Es un software que secretamente se instala en la computadora del usuario, para luego monitorear su actividad o interferir en el uso de su equipo.

es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

Un programa espía típico se autoinstala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.

Sin embargo, a diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.

CONCLUSIÓN

Como acciones para cuidarse al navegar en internet de manera segura es navegar en páginas con protocolo https, borrar spam y procurar no abrir correos extraños, mantener activado el firewall y los pasos que a continuación se presentan:

- **Mantener el sistema operativo y el navegador actualizados**. Los virus aprovechan los agujeros del SO y navegador para infectar los dispositivos.
- **Cuidar las contraseñas.** Al introducirlas se debe estar seguro de que es la página correcta, ya que puede parecer idéntica a la legítima y tratarse de una suplantación (phishing).
- **No hacer clic en enlaces que resulten sospechosos.** Se debe ser precavido antes de seguir un enlace al navegar, en el correo, en la mensajería instantánea o en una red social.
- **Tener cuidado con lo que se descarga.** No hay que precipitarse y descargarse cualquier cosa, ya que nuevas amenazas surgen cada día y los antivirus no pueden combatirlas todas.
- **Utilizar antivirus:** mantenerlo actualizado.
- **Uso de redes sociales:** Mediante las redes sociales los ciberdelincuentes tratan de obtener información para posibles ataques.
- **Encripta tu información importante** para mantenerla segura y secreta.

REFERENCIAS BIBLIOGRÁFICAS

Kaspersky, “Las siete principales amenazas de ciberseguridad a las que debes estar atento,” latam.kaspersky.com, 13-Jan-2021. [Online]. Disponible en: https://latam.kaspersky.com/resource-center/threats/top-7-cyberthreats. [Accedico: 23-Mar-2021].

Oriol, “Conoce los Principales Riesgos y Amenazas de Internet,” ComputerNewAge, 05-Jul-2019. [Online]. Disponible en: https://computernewage.com/2013/05/19/conoce-las-7-principales-amenazas-de-internet/. [Accedido: 23-Mar-2021].

Pablo Rodríguez, “Ciberseguridad: 10 tipos de amenazas”, AMBIT BST, 19-Mar-2020. [Online]. Disponible en: https://www.ambit-bst.com/blog/ciberseguridad-10-tipos-de-amenazas. [Accedido: 23-Mar-2021].

Nación321, “¿Cuáles son las principales amenazas en internet y cómo protegernos?”, Ciberseguridad, 09-JUL-2019. [Online]. Disponible en: https://www.nacion321.com/ciudadanos/cuales-son-las-principales-amenazas-en-internet-y-como-protegernos. [Accedido: 23-Mar-2021].