# Curso: Seguridad Informática
# Tarea: Tarea Investigación 20%

Jose Eduardo Ramos Pichal 201U0242@alumno.itssat.edu.mx

## Calificación 20%

Calificación:

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

Calificación actual en el libro de calificaciones

**20,00**


# INSTITUTO TECNOLOGICO SUPERIOR DE SAN ANDRES TUXTLA


**CARRERA:**

Ing. Informática 810-A

**MATERIA:**

Seguridad Informática

**DOCENTE:**

Juan Rafael González Cadena

## INVESTIGACIÓN 1

**ALUMNO:**

**JOSE EDUARDO RAMOS PICHAL**

**San Andrés Tuxtla Ver,  febrero de 2024**

# 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%

Jose Eduardo Ramos Pichal201U0242@alumno.itssat.edu.mx

## Entrega

Entregado
Calificado
El estudiante puede editar esta entrega

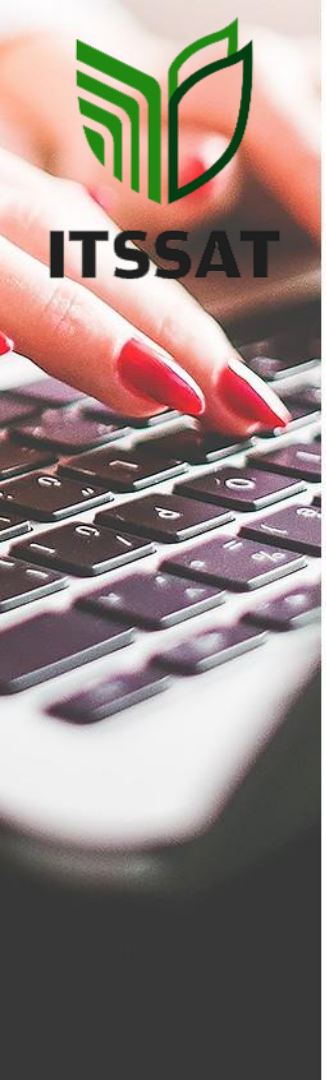
## Calificación

Calificación:

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

Calificación actual en el libro de calificaciones

**40,00**




# INSTITUTO TECNOLOGICO SUPERIOR DE SAN ANDRES TUXTLA

**CARRERA:**

Ing. Informática

**MATERIA:**

Seguridad Informática

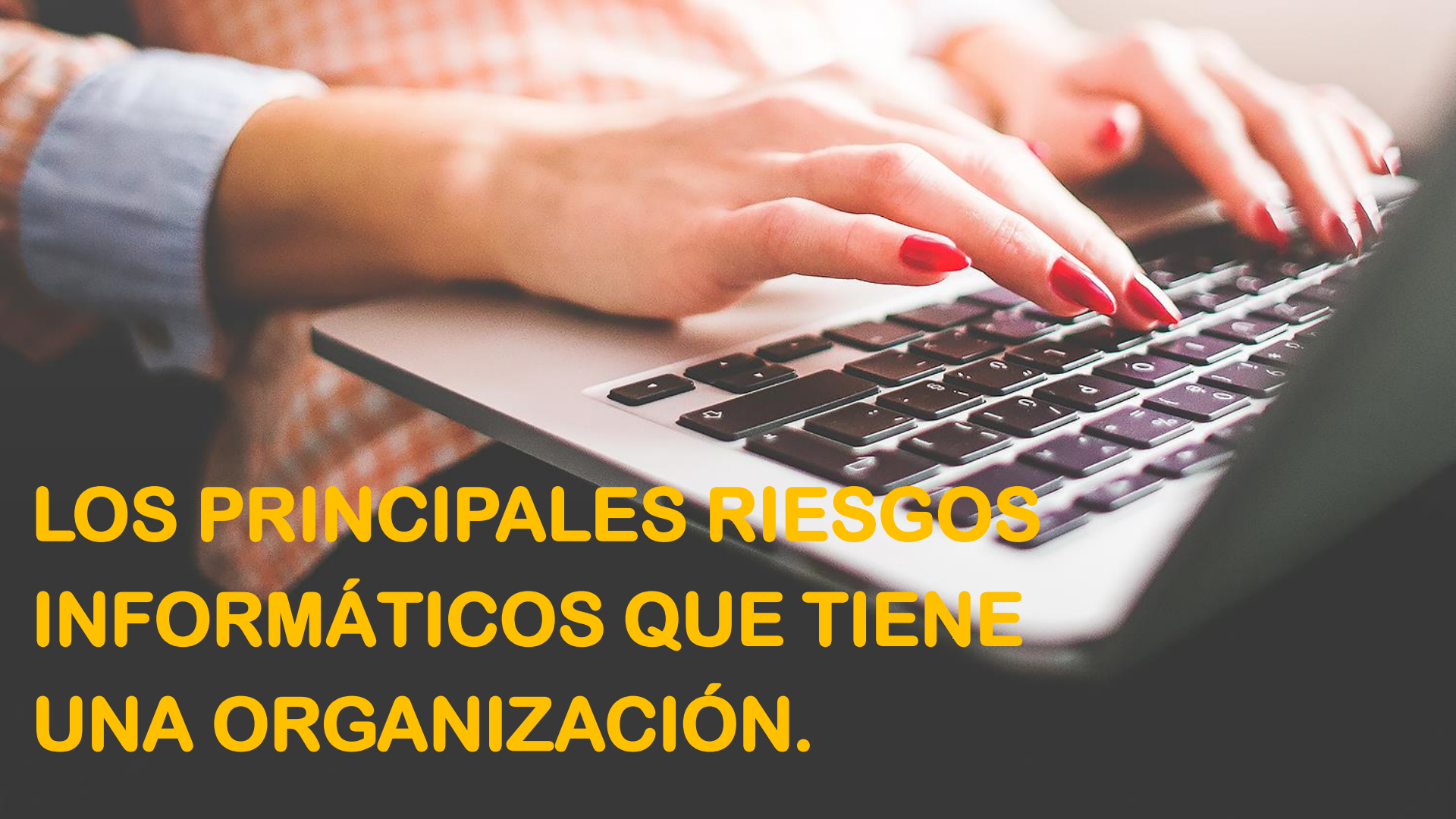
**DOCENTE:**

Juan Rafael González Cadena

**INTEGRANTE:**

José Eduardo Ramos Pichal

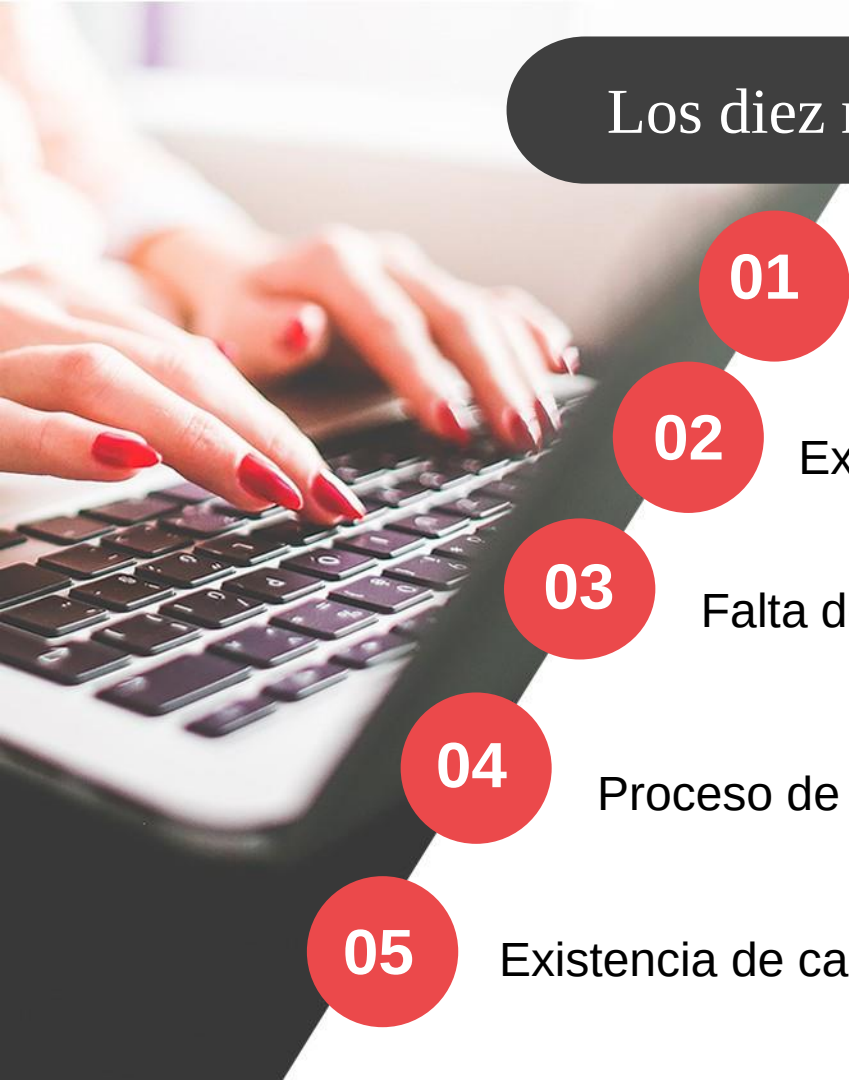
**San Andrés Tuxtla Ver, marzo de 2024.**



# 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:

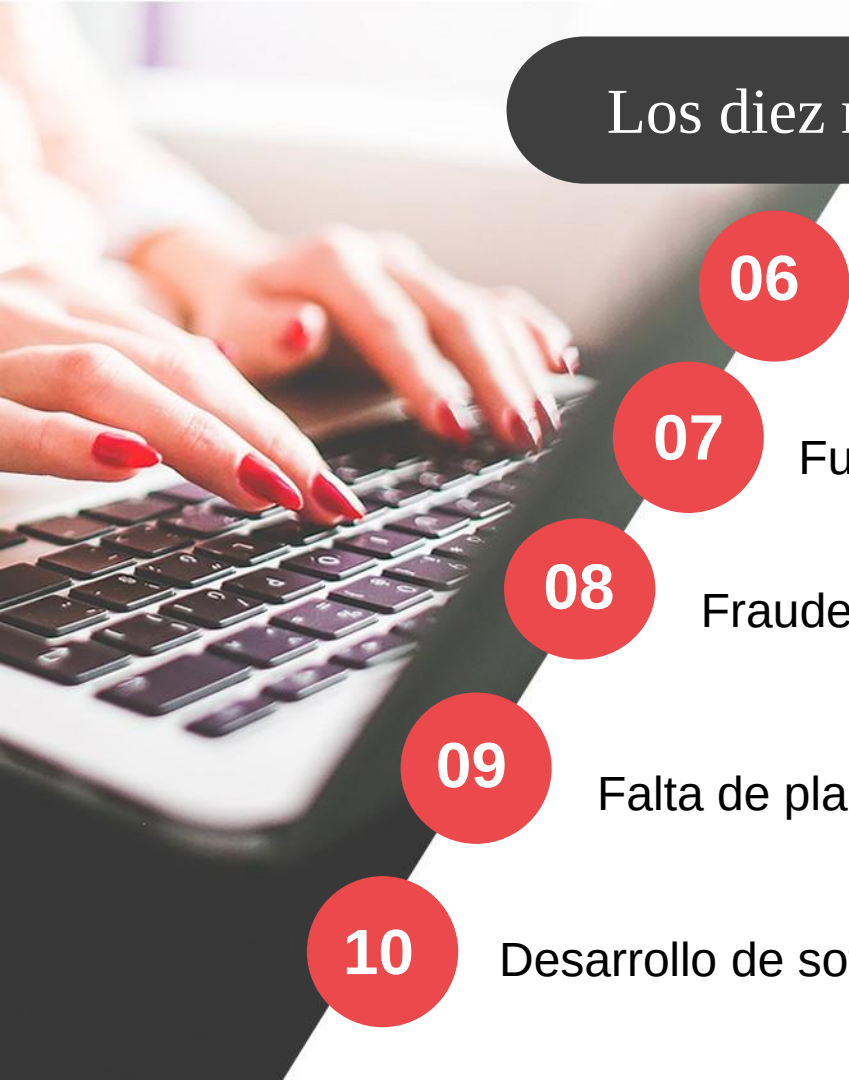
01 Deficiente control de acceso a las aplicaciones.

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:

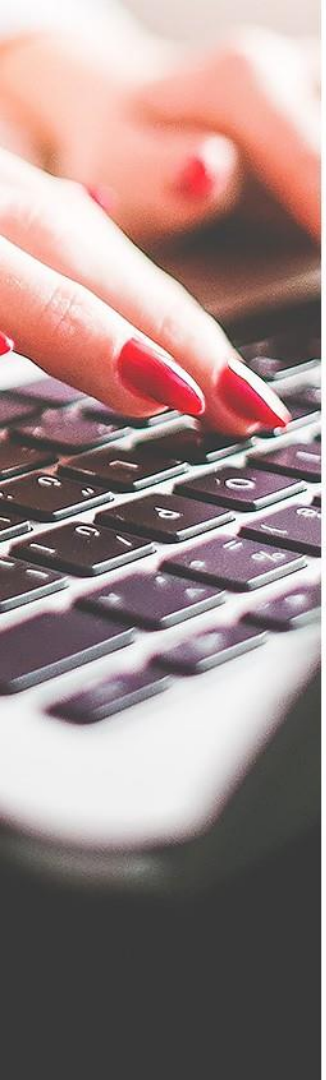
06 Control de acceso a la red.

07 Fugas de información.

08 Fraude y robo de información.

09 Falta de planificación de continuidad de negocio.

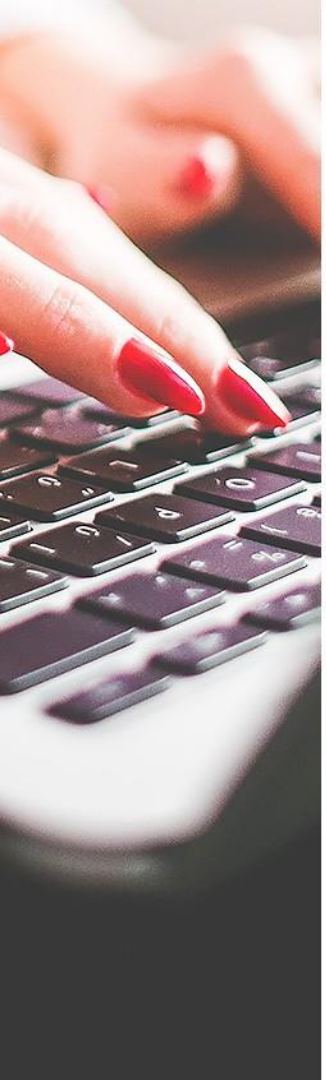
10 Desarrollo de software seguro.



# ¿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.**



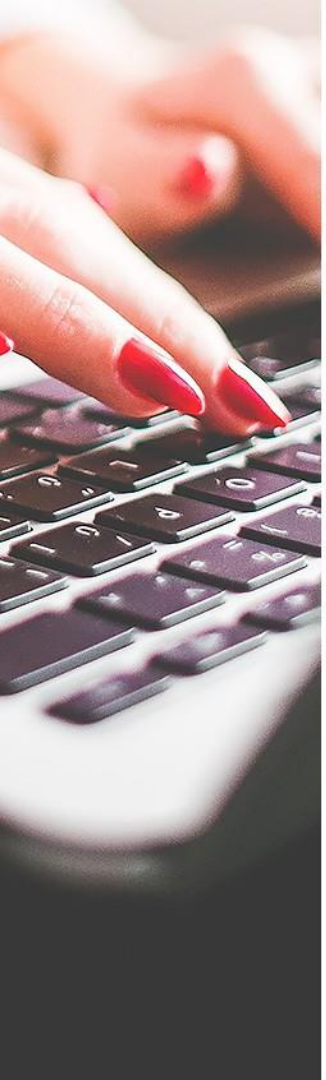
**6. Subir archivos a la Nube sin cifrar.**

**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%

Jose Eduardo Ramos Pichal201U0242@alumno.itssat.edu.mx

## Entrega

Enviado para calificar
Calificado
La tarea fue enviada 4 días 1 hora antes

**Calificación: 40%**

| | | | |
|---|---|---|---|
| Hoja de presentación | No contien todos los datos<br>0puntos | Datos incompletos<br>1puntos | Completo<br>2puntos |
| Introducción | No contiene<br>0puntos | Muy pequeña<br>2.5puntos | Completa<br>5puntos |
| Contenido | No cubre los temas<br>0puntos | La mitad de los temas<br>12puntos | Completo<br>23puntos |
| Referencias IEEE | No contiene<br>0puntos | Una o no tiene el formato<br>2puntos | Más de una y formato correcto<br>4puntos |
| Conclusión | No contien<br>0puntos | Muy pequeña<br>2.5puntos | Completa<br>5puntos |
| Archivo PDF | Sin formato<br>0puntos | | Correcto<br>1puntos |

Calificación actual en el libro de calificaciones

**40,00**

**Ingeniería Informática**


**Instituto Tecnológico Superior**
**de**
**San Andrés Tuxtla.**

**Materia: Seguridad Información**

**Alumno: José Eduardo Ramos Pichal**

**Grupo: 810A**

**Investigación**

# Introducción

La seguridad informática, o ciberseguridad, abarca un amplio espectro de prácticas, tecnologías y procesos diseñados meticulosamente para defender computadoras, redes, programas y datos del acceso, daño o ataque no autorizados. En su esencia, busca asegurar la confidencialidad, integridad y disponibilidad de la información, permitiendo que individuos y organizaciones mantengan la confianza en sus sistemas tecnológicos.

A medida que avanzamos hacia un futuro aún más interconectado, con la adopción masiva del Internet de las Cosas (IoT), la inteligencia artificial (IA) y la computación en la nube, los desafíos de seguridad informática se vuelven más complejos y demandantes. Los ciberdelincuentes continúan desarrollando métodos más ingeniosos y encubiertos para comprometer sistemas, lo que requiere una vigilancia constante, innovación y adaptación por parte de los profesionales de la ciberseguridad.

## RIESGOS DE INTERNET

El aumento significativo de ataques cibernéticos que se ha registrado en los últimos meses, no sólo en México sino en el mundo, es un llamado de atención para reforzar la seguridad en todos los sistemas digitales de oficinas, dispositivos móviles y computadoras personales, ante el riesgo de que la información y los datos sean robados y utilizados con fines delictivos, advirtió Anahiby Becerril Gil, colaboradora en la Línea de Investigación en Derecho e Inteligencia Artificial del Instituto de Investigaciones Jurídicas.

De acuerdo con la especialista, la palabra ciberataque sigue generando temor e incertidumbre entre los usuarios, ante la posibilidad de que actores maliciosos, con diversas finalidades, puedan vulnerar la privacidad de las personas dentro de lo que se denomina la ingeniería social. “Desafortunadamente somos el eslabón más débil en esta cadena de la ciberseguridad”, afirmó.

La investigadora explicó que, hasta hoy, todos los softwares son susceptibles de ser vulnerados, y si se toma en consideración que el uso de internet se convirtió. Subrayó que en estos momentos en que la tecnología digital se encuentra prácticamente en todos los espacios de nuestra vida cotidiana, es muy importante conocer las acciones o herramientas que se encuentran a nuestro alcance para reducir riesgos, las cuales muchas son medidas muy simples, como cambiar periódicamente las contraseñas y no compartirlas con nadie, instalar los antivirus adecuados y aplicar las actualizaciones que con frecuencia se indican en dispositivos y equipos de cómputo, toda vez que en la mayoría de esos casos son avisos de que algo está mal porque tal vez detectaron alguna vulnerabilidad y lo que están haciendo es un parche para que justamente el equipo no este expuesto.

## CAPACITACIÓN

Por otra parte, sobre la ciberseguridad institucional, la académica reiteró que no hay una tecnología mágica que garantice una protección total ni tampoco se puede resolver todo con una legislación en la materia, por lo que en todos los casos es necesario acompañar el uso de nuevas tecnologías y las normas legales con una regulación adecuada para aplicar los controles específicos, establecer gestiones de riesgo, pero, sobre todo, poner especial énfasis en la capacitación; “porque por más que se instalen las tecnologías más avanzadas, si el personal no está capacitado para aprovechar esa tecnología a su favor, no va a servir de nada”. Al igual que sucede en el mundo físico, apuntó, en el terreno cibernético no hay ningún sistema infalible. “Todas las computadoras se pueden infectar con

malware, todas pueden ser incautadas con ransomware, todas pueden ser arrastradas a una botnet, pero también, todas las computadoras pueden sanitizarse de forma remota.”

**1. Mantenimiento de Contraseñas**

A continuación se brindan algunos consejos para ayudarte a tomar el control de su seguridad en línea a través de un mantenimiento de contraseñas más sólido. Detalle de todas las cuentas en línea más importantes con las que contás. Tener en cuenta correos electrónicos, cuentas bancarias, redes sociales, servicios públicos, etc.

Configurar un administrador de contraseñas con una contraseña maestra muy sólida y única. Considerar usar una frase de contraseña, como Sandiaeslafrutaquemegusta43. Siempre que sea posible, habilitar un Factor Doble de Autenticación con tu teléfono celular. La mayoría de los sitios web principales te permitirán hacerlo y, si bien es algo inconveniente, es un medio importante para proteger tus cuentas. NOTA IMPORTANTE: NUNCA permitas que tu navegador guarde sus contraseñas. Si tenés contraseñas guardadas en tu navegador, bórralas.

**2. Control de Identidad**

Existen formas por las cuales puede controlar su identidad en línea y dificultar a otras personas poder conectar su identidad real con su persona en línea. Elegí un pseudónimo en línea. Úsalo en las redes sociales y otros sitios con información pública o semipública disponible sobre vos. Asegúrate de compartir este pseudónimo solo con amigos y familiares de confianza. Si trabajas en un lugar donde tengas un correo electrónico y una identidad pública, analiza las opciones con tu empleador. Muchos departamentos de Recursos Humanos ya han evaluado esto antes y los equipos de TI se complacen en facilitarle el uso de un pseudónimo para el correo electrónico y otra información pública

**3. Teléfono**

Considera cambiar tu número de teléfono y opta porque no aparezca en el directorio. No proporciones u número de teléfono a personas que no conozcas. No es necesario obtener un nuevo teléfono celular. Si consideras que tu teléfono real está en peligro, lo mejor es realizar un restablecimiento completo de fábrica.

**4. Equipo Informático**
Si consideras que tu equipo informático está en peligro, lo mejor es que consultes con un profesional en el área. Asegúrate de ejecutar un conjunto de antivirus y cortafuegos de buena calidad. Por ejemplo, Bit Defender o Windows Defender. Descarga una herramienta contra programas dañinos, como Malware Bytes y escanea regularmente tu sistema en busca de problemas. No instales programas con los que no estés extremadamente familiarizado. No descargues archivos adjuntos de correos electrónicos que no esperabas.

**5. Documentación**
Es importante documentar continuamente todo lo que sucede, incluidos los incidentes en línea y de tecnología. Esto puede ayudar a actualizar órdenes judiciales y ayudará a tu abogado a recomendar órdenes judiciales para incluir contactos en línea e interacción con la tecnología. A fin de brindarle a tu abogado más influencia en los tribunales, las denuncias policiales y otras interacciones con los cuerpos de seguridad ayudarán a consolidar tu caso.

**6.Mantenimiento Continuo**
Al combatir el acecho en línea u otras formas de acoso en línea, puede parecer que no pararas de sufrir incidentes. Planifica una hora a la semana para realizar tareas de mantenimiento preventivo y verificar tu presencia en internet.

La seguridad navegando por Internet es en gran medida cuestión de sentido común. Entre los consejos habituales está evitar las páginas webs sospechosas (la mayoría de los antivirus detectan este tipo de virus). Las webs seguras cuentan con un certificado SSL, lo que significa que la url de la web llevará un https en vez de un http.

**Phishing y ataques de ingeniería social:** Los ataques de phishing se han vuelto más sofisticados, utilizando técnicas de ingeniería social para engañar a los usuarios y hacer que revelen información personal o credenciales de acceso. Los ciberdelincuentes también han utilizado eventos actuales, como la pandemia de COVID-19, para crear correos electrónicos y sitios web falsos que parecen legítimos.

**Ransomware:** Este tipo de malware, que cifra los datos del usuario y exige un escate para su liberación, sigue siendo un riesgo significativo para individuos y organizaciones. Los ataques de ransomware han evolucionado para incluir tácticas como el "doble chantaje", donde los atacantes no solo cifran los datos, sino que también amenazan con publicarlos en línea si no se paga el rescate.

**Ataques a la cadena de suministro:** Los ciberdelincuentes han atacado cada vez más la cadena de suministro de software, comprometiendo productos de software legítimos para distribuir malware.

**Explotación de vulnerabilidades de día cero:** Las vulnerabilidades de día cero, aquellas que son desconocidas para los desarrolladores del software en el momento del ataque, representan un riesgo significativo ya que permiten a los atacantes explotar sistemas antes de que se pueda desarrollar y desplegar un parche.

**Amenazas a dispositivos conectados e IoT:** Con más dispositivos conectados a Internet, desde dispositivos domésticos inteligentes hasta infraestructuras críticas, hay un mayor riesgo de ataques que pueden aprovecharse de las debilidades en la seguridad de estos dispositivos.

**Desinformación y manipulación en línea:** La propagación de desinformación y las campañas de manipulación en línea representan un riesgo de seguridad, ya que pueden influir en la opinión pública, interferir en procesos democráticos y causar división social.

**Deepfakes y manipulación de medios:** La tecnología deepfake, que puede crear contenido audiovisual falso pero convincente, plantea riesgos en términos de desinformación, extorsión y manipulación.

**Ataques a infraestructuras críticas:** Los ataques dirigidos a infraestructuras críticas, como sistemas de energía, agua y transporte, representan un riesgo significativo para la seguridad nacional y la salud pública.

**Explotación de vulnerabilidades en tecnologías emergentes:** A medida que se adopten nuevas tecnologías, como el 5G, la computación cuántica y las

interfaces cerebro-computadora, surgirán nuevas vulnerabilidades. Los ciberdelincuentes buscarán explotar estas tecnologías antes de que se establezcan prácticas de seguridad robustas.

**Ataques a cadenas de bloques y criptomonedas:** A medida que el interés y la inversión en criptomonedas y tecnología de cadena de bloques continúan creciendo, también lo hacen los incentivos para atacar estas plataformas.

**Desinformación y manipulación a través de deepfakes mejorados:** La tecnología para crear deepfakes está mejorando rápidamente, lo que podría resultar en una proliferación de contenido falso más convincente. Esto podría usarse para manipular elecciones, dañar reputaciones o cometer fraudes financieros.

**Amenazas a la privacidad debido a la vigilancia y recolección de datos:** A medida que las empresas y los gobiernos recolectan y analizan más datos personales, el riesgo de violaciones de datos y el uso indebido de información personal aumenta.

**Fraudes y estafas relacionados con la inteligencia artificial:** Podríamos ver un aumento en los fraudes y estafas que utilizan la IA para crear métodos de engaño más sofisticados, como la imitación de voces para el vishing (phishing por voz) o la creación de identidades falsas convincentes para el fraude bancario

# Conclusión

En conclusión, los riesgos en seguridad informática representan una de las mayores amenazas para la sociedad digital contemporánea. A medida que nuestra dependencia de la tecnología crece, también lo hace nuestra vulnerabilidad a una amplia gama de ciberataques, desde el robo de identidad y la filtración de datos hasta el sabotaje de infraestructuras críticas y la propagación de malware. Estos riesgos no solo tienen el potencial de comprometer la privacidad y la seguridad de individuos, sino que también plantean graves amenazas a la estabilidad económica, la seguridad nacional y la confianza en el ecosistema digital global.

La naturaleza dinámica de las amenazas cibernéticas, impulsada por la constante evolución de la tecnología y las tácticas de los atacantes, exige una respuesta igualmente dinámica y proactiva. Esto incluye no solo la adopción de tecnologías de seguridad de vanguardia, sino también la promoción de una cultura de seguridad que priorice la educación y la concienciación sobre ciberseguridad en todos los niveles de la sociedad.

Además, la colaboración entre empresas, gobiernos y organizaciones internacionales es fundamental para desarrollar estrategias de defensa más efectivas y para establecer normas y regulaciones que refuercen la seguridad informática a nivel mundial. Solo mediante esfuerzos conjuntos podremos esperar mitigar los riesgos asociados con la seguridad informática y proteger nuestro futuro digital contra las amenazas emergentes.

# Referencias


https://merida.anahuac.mx/noticias/principales-riesgos-informaticos-en-mexico

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjc47Cs5d6EAxXN_8kDHSyVCYgQFnoECBQQAQ&url=https%3A%2F%2Fwww.grupocibernos.com%2Fblog%2Fciberseguridad-riesgos-herramientas-formacion-para-empresas&usg=AOvVaw1-brDv2eeAeXHgGFgbbUcQ&opi=89978449

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjc47Cs5d6EAxXN_8kDHSyVCYgQFnoECCwQAQ&url=https%3A%2F%2Fwww.gadae.com%2Fblog%2Friesgos-de-seguridad-informatica%2F&usg=AOvVaw0jjSGNQKwHTwTaoMf_kJ_q&opi=89978449

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjc47Cs5d6EAxXN_8kDHSyVCYgQFnoECDMQAQ&url=https%3A%2F%2Fwww.ambit-bst.com%2Fblog%2Fan%25C3%25A1lisis-de-riesgos-inform%25C3%25A1ticos-y-ciberseguridad&usg=AOvVaw35cZS7_KanDyEnTUAm2dmV&opi=89978449