UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE SAN

         FRANCISCO XAVIER DE CHUQUISACA

       FACULTAD DE TECNOLOGÍA

SIS (316)



TÍTULO DEL PRACTICO:

Modelado de Amenazas

ESTUDIANTES:

Colque García Ariel Rodrigo

Cepeda Choque Álvaro Sebastián

Perka Casillas Celedonio

CARRERA:  Ing. Ciencias De la Computación

MATERIA: SIS (316) Auditoria de Sistemas

La página expone 10 riesgos o peligros de internet que todos deberían saber. Aquí hay una breve explicación de cada uno:

**Ciberdelincuentes y ciberdelitos**: Son personas que utilizan software o técnicas maliciosas para dañar a otros usuarios, dispositivos o redes en línea. Pueden robar información personal, dinero o datos, o causar daños o interrupciones.

**Robo de identidad**: Es cuando alguien usa su información personal, como su nombre, número de Seguro Social o número de tarjeta de crédito, para cometer fraude u otros delitos a su nombre. Pueden abrir nuevas cuentas, hacer compras o presentar impuestos usando su identidad.

**Depredadores en línea:** Estas son personas que usan Internet para atraer a niños o adolescentes a relaciones o situaciones inapropiadas. Pueden fingir ser otra persona en línea y tratar de ganar su confianza e información personal.

**Phishing**: Es cuando alguien te envía un correo electrónico o un mensaje que parece provenir de una fuente legítima, como tu banco, una empresa o un amigo. El mensaje puede pedirle que haga clic en un enlace, abra un archivo adjunto o proporcione información confidencial. El enlace o archivo adjunto puede contener malware que infecta su dispositivo o roba sus datos. La información que usted proporciona puede ser utilizada para robo de identidad o fraude.

**Malware**: Esta es la abreviatura de software malicioso. Es cualquier programa diseñado para dañar su dispositivo, datos, red o actividad en línea. El malware puede incluir virus, gusanos, troyanos, ransomware, spyware, etc.

**Ransomware**: Este es un tipo de malware que bloquea tu dispositivo o encripta tus archivos y exige un rescate por su liberación. Si no paga el rescate, puede perder el acceso a sus datos de forma permanente. El ransomware puede afectar a personas y organizaciones por igual.

**Redes Wi-Fi no seguras**: Son redes inalámbricas que no requieren contraseña ni cifrado para conectarse. Pueden encontrarse en lugares públicos como cafés, aeropuertos u hoteles. Las redes Wi-Fi no seguras pueden exponer su actividad y datos en línea a hackers que pueden interceptarlos o inyectarles malware.

**Estafas en línea:** Estos son esquemas que utilizan Internet para engañar a la gente a dar dinero o bienes por algo que no existe o no es como se prometió. Las estafas en línea pueden tomar muchas formas, como las estafas de lotería, las estafas románticas, las estafas de inversión o las estafas de caridad. Las estafas en línea pueden costarle dinero y tiempo si se enamora de ellos.

**Acoso cibernético**: Es cuando alguien usa Internet o dispositivos digitales para acosar, amenazar, humillar o herir a otra persona. El acoso cibernético puede tomar muchas formas, como enviar mensajes maliciosos, difundir rumores, publicar fotos embarazosas o crear perfiles falsos. El acoso cibernético puede afectar a cualquier persona, pero es especialmente común entre los niños y adolescentes.

**Información errónea:** Se trata de información falsa o inexacta que se comparte por error o sin intención. Puede deberse a una falta de verificación, investigación o comprensión del tema. La desinformación también puede causar confusión, malentendidos o daños a las personas que confían en ella.

# Después de una lectura comprensiva de las 20 recomendaciones para la seguridad en internet, relacione estas medidas de control, con las amenazas anteriormente descritas (muchos controles para una amenaza, o un control para varias amenazas), usando la siguiente Tabla.

|  |  |  |
| --- | --- | --- |
| **Amenaza(s)** | **Impacto Negativo**  **de la Amenaza (riesgo)** | **Control(es)** |
| Ciberdelincuentes y ciberdelitos | Pérdida o robo de datos personales, financieros o confidenciales. Daño a los dispositivos o al rendimiento. Extorsión o chantaje. | Instalar un software de seguridad integral que proteja todos los dispositivos y ofrezca soporte 24/7. Hacer copias de seguridad de los datos importantes. Usar un sistema de gestión de contraseñas. |
| Extraños en línea | Acoso, abuso, explotación o engaño. Exposición a contenidos inapropiados o dañinos. Pérdida de privacidad o reputación. | Enseñar a los niños y adolescentes a no revelar su identidad ni su ubicación en línea, y a no interactuar con desconocidos. Usar un software con controles parentales para bloquear ciertas funciones en los juegos, rastrear la ubicación de los hijos, hacer copias de seguridad de sus datos y gestionar su tiempo de pantalla. Establecer reglas y límites sobre el uso de internet y supervisar las actividades en línea. |
| Revelar demasiada información personal o privada en línea | Robo de identidad, fraude, suplantación o usurpación. Acoso, chantaje o extorsión. Daño a la imagen personal o profesional. | Enseñar a los niños y adolescentes a no compartir información personal como su nombre completo, dirección, número de teléfono, escuela, etc., ni fotos comprometedoras o íntimas en línea. Revisar las políticas de privacidad y las configuraciones de las redes sociales y las aplicaciones que se usan. Ser consciente del valor de la privacidad en línea y recordar que nada es privado en internet. |
| Sitios web inseguros o falsos | Robo o pérdida de datos personales, financieros o confidenciales. Infección por malware, spyware, ransomware u otros programas maliciosos. Estafa o fraude por parte de sitios web falsos que se hacen pasar por legítimos. | Evitar hacer clic en enlaces sospechosos o desconocidos que llegan por correo electrónico u otros medios. Comprobar la veracidad y la seguridad de los sitios web antes de ingresar datos personales o realizar compras en línea (por ejemplo, buscar el candado verde 🔒, el prefijo https://, el sello Seguro🔐, etc.). Usar una VPN (red privada virtual) para cifrar el tráfico web y evitar el rastreo u observación por parte de terceros malintencionados. |
| Conexiones a internet no seguras | Hackeo o interceptación del Router doméstico u otras redes Wi-Fi públicas o compartidas. Acceso no autorizado a dispositivos conectados a internet como sistemas de seguridad doméstica o timbres inteligentes. Robo o pérdida de datos personales, financieros o confidenciales. | Asegurar el Router doméstico con una contraseña difícil de descifrar y considerar un software de seguridad que identifique “intrusos” en la red. Usar una VPN (red privada virtual) para cifrar el tráfico web y evitar el rastreo u observación por parte de terceros malintencionados. Evitar conectarse a redes Wi-Fi públicas o compartidas que no sean seguras o confiables. |
| Software desactualizado | Vulnerabilidad a ataques informáticos que aprovechan las fallas o debilidades del software antiguo. Infección por malware, spyware, ransomware u otros programas maliciosos. Pérdida o robo de datos personales, financieros o confidenciales. Daño a los dispositivos o al rendimiento. | Actualizar el software regularmente, incluyendo el sistema operativo, las aplicaciones, los navegadores y los programas de seguridad. Activar las actualizaciones automáticas cuando sea posible. Desinstalar el software que ya no se usa o que proviene de fuentes desconocidas. |
| Ransomware | Bloqueo del acceso a los archivos valiosos como fotos privadas o información fiscal. Extorsión o chantaje para recuperar los archivos mediante el pago de un rescate. Pérdida definitiva de los archivos si no se paga el rescate o si el atacante no cumple su palabra. Infección por otros tipos de malware que pueden acompañar al ransomware. | Instalar un software de seguridad integral que proteja todos los dispositivos y ofrezca soporte 24/7. Hacer copias de seguridad de los datos importantes en un disco duro externo o en la nube. Evitar hacer clic en enlaces sospechosos o desconocidos que llegan por correo electrónico u otros medios. No pagar el rescate ni negociar con los atacantes, ya que esto puede incentivarlos a seguir cometiendo este tipo de delitos. |
| Redes sociales | Exposición a contenidos inapropiados, dañinos, falsos o engañosos. Acoso, intimidación, difamación o violencia en línea. Robo de identidad, suplantación o fraude. Pérdida de privacidad o reputación. Adicción o aislamiento social. | Ser cuidadoso con lo que se publica y con quién se comparte. No revelar demasiada información personal, financiera o confidencial. Usar configuraciones de privacidad y seguridad para limitar el acceso a los perfiles y el contenido. Verificar la autenticidad y credibilidad de las fuentes y las noticias. Bloquear, denunciar o ignorar a los usuarios que molestan, ofenden o amenazan. Mantener un equilibrio entre el tiempo en línea y el tiempo fuera de línea. |
| Compras en línea | Estafas, fraudes o robos por parte de vendedores falsos o sitios web fraudulentos. Pérdida de dinero, datos personales o financieros. Entrega defectuosa, tardía o nula del producto o servicio comprado. Problemas para devolver, cambiar o reclamar el producto o servicio comprado | Comprar solo en sitios web seguros y confiables que tengan una dirección que empiece por https:// y un candado cerrado en la barra del navegador. Verificar la reputación y las opiniones de los vendedores y los compradores. Usar métodos de pago seguros y evitar transferencias bancarias directas. Guardar los recibos, las facturas y los comprobantes de compra. Leer las políticas de envío, devolución y garantía antes de comprar. |
| Controles parentales insuficientes | Acceso no supervisado ni restringido a contenidos inapropiados, dañinos, falsos o engañosos. Exposición a riesgos como el ciberacoso, el grooming, el sexting o el phishing. Adicción, distracción o aislamiento social por un uso excesivo o inadecuado de internet. Problemas de salud física o mental por falta de sueño, ejercicio o interacción social. | Instalar un software de seguridad con controles parentales que permita bloquear ciertas características en los juegos, rastrear la ubicación de los niños, hacer copias de seguridad de sus datos y gestionar su tiempo de pantalla. Establecer reglas y límites claros sobre el uso de internet y los dispositivos. Dialogar con los niños sobre los beneficios y los riesgos de internet y educarlos sobre cómo protegerse en línea. Respetar la edad mínima recomendada para acceder a las redes sociales y otras plataformas en línea. Supervisar y acompañar a los niños en sus actividades en línea sin invadir su privacidad ni confianza. |

# Complete también la siguiente tabla que relaciona amenazas con vulnerabilidades. Debe preguntarse qué vulnerabilidades aprovecha una determinada amenaza.

|  |  |
| --- | --- |
| **Amenaza** | **Vulnerabilidades que aprovecha** |
| Phishing | Apertura de correos o archivos fraudulentos que suplantan la identidad de una entidad legítima |
| Denegación de servicio distribuido (DDoS) | Falta de medidas preventivas o reactivas para mitigar el impacto de un ataque masivo que satura los recursos del sistema |
| Malware móvil | Uso de aplicaciones no seguras o desactualizadas que pueden contener código malicioso o explotar las debilidades del teléfono |
| Inyección de scripts | Visita a sitios web legítimos pero vulnerables que han sido comprometidos por hackers para redirigir a los usuarios a recursos maliciosos |
| Ciberdelincuentes y cibercrimen | Falta de conciencia o educación sobre los riesgos asociados a la actividad en línea y las estrategias para prevenirlos o evitarlos. |
| Ransomware | No tener copias de seguridad regulares de los datos importantes que pueden ser bloqueados o cifrados por un software malicioso que exige un rescate. |
| Redes sociales | Revelar demasiada información personal o sensible que puede ser utilizada por terceros con fines maliciosos o publicitarios |
| Conexión a internet insegura | No tener una contraseña difícil de descifrar o un software de seguridad que identifique a los intrusos en la red doméstica |
| Sitios web no seguros | No verificar los indicadores de seguridad como el candado verde, el protocolo HTTPS o el certificado SSL que garantizan la autenticidad y la protección de los datos |
| Robo de identidad | No usar contraseñas fuertes y únicas para cada cuenta o revelar información personal que pueda ser usada para suplantar la identidad |
| Software desactualizado | No instalar las actualizaciones de seguridad que corrigen las vulnerabilidades conocidas que pueden ser explotadas por los hackers |
| Correo electrónico no deseado o spam | No tener un filtro de spam o hacer clic en enlaces o archivos adjuntos sospechosos que pueden contener malware o phishing |

# finalmente establezca el tipo de amenaza en función al contravalor de seguridad que provoca (recordar que los valores de seguridad son: Integridad, Confidencialidad, Disponibilidad, No Repudio y Autenticidad, y sus contravalores sus contrarios).

|  |  |  |
| --- | --- | --- |
| **Amenaza** | **Contravalor** | **Justificación** |
| Virus | Integridad | Un virus informático altera el funcionamiento normal de los programas y archivos infectados |
| Malware | Confidencialidad | Un malware puede robar o filtrar información sensible o privada del sistema víctima |
| Spam | Disponibilidad | Un spam puede saturar el correo electrónico o la red con mensajes no deseados que dificultan el acceso a los recursos legítimos |
| Ransomware | Disponibilidad y Confidencialidad | Un ransomware cifra o bloquea los datos del usuario y pide un rescate para liberarlos, afectando tanto a la disponibilidad como a la confidencialidad de la información |
| Phishing | Autenticidad y Confidencialidad | Un phishing suplanta la identidad de una entidad legítima para engañar al usuario y obtener sus credenciales o datos personales, vulnerando la autenticidad y la confidencialidad. |
| Ciberdelincuentes y cibercrimen | Integridad, confidencialidad, disponibilidad | Los ciberdelincuentes pueden alterar, robar o destruir la información mediante ataques como el phishing, el ransomware o el malware. |
| Redes sociales e internet | Confidencialidad, integridad, no repudio | Las redes sociales e internet pueden exponer la información personal o profesional de los usuarios a terceros no autorizados o malintencionados. Además, pueden facilitar la difusión de noticias falsas o contenidos inapropiados que afecten a la reputación o credibilidad de las personas o entidades. |

# Bibliografía

[¿Cuáles son los principales tipos de amenazas informáticas? | Tokio (tokioschool.com)](https://www.tokioschool.com/noticias/tipos-amenazas-informaticas/)

[Las amenazas de seguridad informática más importantes para 2022, según Kaspersky | ManageEngine Blog](https://blogs.manageengine.com/espanol/2022/02/08/amenazas-de-seguridad-informatica-para-2022.html)

[DerecPenalyCriminXXIX.indd (core.ac.uk)](https://core.ac.uk/download/pdf/230095193.pdf)

[Is private browsing really private? Short answer: No (norton.com)](https://us.norton.com/blog/privacy/your-private-browser-is-not-so-private-after-all)

[Norton online privacy protection: Online privacy solutions](https://us.norton.com/products/privacy)

[What is ransomware? Ransomware explained and how it works | Norton](https://us.norton.com/blog/malware/ransomware-5-dos-and-donts)

[Data backups 101: A complete guide for 2023 - Norton](https://us.norton.com/blog/how-to/data-backup)

[How to Secure Your Wi-Fi in 7 Simple Steps | Norton](https://us.norton.com/blog/iot/keep-your-home-wifi-safe)

[10 reasons to get parental controls | Norton](https://us.norton.com/blog/kids-safety/top-reasons-to-use-parental-controls)

[What is spyware? And how to remove it (norton.com)](https://us.norton.com/blog/how-to/catch-spyware-before-it-snags-you)

[Public Wi-Fi: What are the risks? + how to stay safe - Norton](https://us.norton.com/blog/privacy/public-wifi)