Seguridad Informática

Seguridad Informática

1° Edición

Lic. En Sistemas de Información Claudio Dalmasso

Profesor Universitario

“ La mayor declaración de amor es la que no se hace;
el hombre que siente mucho, habla poco ”

Platón.-

Ciudad de Rosario, Argentina - Abril de 2025

ESUPCOM

TIC Departamento de la Información y las Comunicaciones

Material disponible en Biblioteca Virtual

https://esupcom.unr.edu.ar/bv_tics/

Índice general

1.1. Introducción

En un mundo revolucionado por las Tecnologías de la Información y las Comunicaciones (Tics), es un paso obligado conocer, reconocer e indagar sobre Seguridad Informática. Esta titulación nos resulta familiar dado que en los últimos tiempos resuena con frecuencia; ahora bien, de que se trata? Por qué surge? Quien/es hacen uso de esta prestación? Seguridad es sinónimo de garantía? Todos estos interrogantes los trataremos a lo largo de esta intervención académica.

El punto de partida en esta temática resulta ser *"internet"* y esa posibilidad que tenemos de acceder remotamente a lugares de nuestro interés, como ser la compra de un ticket para un recital, el pago de un impuesto o servicio, la carga de una billetera virtual, la venta de un producto en Mercado Libre, etc.

Internet nos da la posibilidad de estar a un clic de lo que necesitamos, sin importar la distancia física, recordemos que internet resulta ser una red de redes interconectadas. Actualmente todos los dispositivos que mantienen relación con las Tics poseen una placa de red y también cada vez mas electrodomésticos las incorporan como ser heladeras, lavarropas, microondas, de ahí el concepto IoT traducido (Internet de las cosas), surgió la necesidad de tener todo interconectado, de operar remotamente, de acceder desde cualquier plataforma operativa de manera urgente por que así lo requiere hoy el mercado y la inmediatez de los usuarios.

1.2. Concepto de Seguridad Informática

Podemos definir la Seguridad Informática como la disciplina que se encarga de diseñar los procesos, procedimientos, técnicas y métodos para que un sistema de información sea seguro. La confianza es algo que se debe percibir si estamos aplicando Seguridad Informática, aunque debemos de considerar que se perciba mayor confianza no significa que sea más seguro. La principal tarea de la Seguridad Informática es la de minimizar los riesgos, que provienen de muchas partes. Pueden ser de la entrada de datos, del medio que transporta la información, del hardware, que es usado para transmitir y recibir por los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre el objetivo principal es minimizar los riesgos para obtener mejor y mayor seguridad.

1.3. Actores Principales

Existe una triada cuyos ejes individuales dan forma al esquema que representa la Seguridad Informática, ellos son: *los usuarios*, *la información* y *la infraestructura*. Los usuarios (las personas) son el eslabón más débil de la cadena, casi imposibles de controlar, mas allá de que se les capacite y explique sobre efectos y consecuencias, sus acciones ponen en riesgo la seguridad, generalmente por desestimar una alerta, por desconocimiento o bien por curiosidad entre múltiples factores que afectan directamente el trabajo de una o muchas personas en la organización. Aunque resulte paradójico muchas veces el sistema y la información deben protegerse del usuario.

La información es oro en términos de Seguridad Informática, ya que es lo que se desea proteger y debe estar a salvo, en otras palabras se dice que es el principal activo. Cuando surgen ataques informáticos es común ver el cifrado de los datos, es decir, se sobrescribe el formato original del archivo por otro que resulte indescifrable imposibilitando así a su acceso. Esta acción delictiva tiene impactos negativos en el funcionamiento de las organizaciones estimando que la información afectada suele ser de base datos o documentos que contienen datos relevantes y confidenciales como ser: datos personales, movimientos operativos, estados de cuentas, etc.

Por último tenemos la infraestructura, podemos decir que es de los medios mas controlados, no obstante esto, no implica que resulte de menos riesgo, siempre dependerá de los procesos que manejemos, debemos considerar problemas complejos como los de un acceso no permitido, robo de identidad, hasta los daños mas comunes como ser robo de equipos, siniestros como incendios, inundaciones, o cualquier acontecimiento natural que pueda poner en riesgo el material físico de nuestro sistema.

Vulnerabilidades

2.1. ¿ A que se refiere la expresión vulnerable en Informática ?

Algo es vulnerable cuando puede ser herido, lesionado, en términos informáticos este daño se puede ocasionar de múltiples formas, y entendemos que una vulnerabilidad es el origen de un ataque que puede sucederse en un sistema de información, contemplemos que existen múltiples plataformas y dispositivos que albergan sistemas operativos, programas, app's, etc; no debemos reducir la posibilidad solo a computadoras, cualquier dispositivo que esté vinculado a internet puede ser víctima de un ataque. La Seguridad Informática surge precisamente en un intento de dar protección y de este modo reducir la posibilidad de ataques a través de métodos preventivos. La prevención se da en un contexto de procedimientos ordenados y rigurosos que ejecutan los especialistas informáticos intentando *"blindar"*acciones maliciosas, que tienen objetivos precisamente *"no operativos"*, ni vinculados a las prestaciones legítimas que ofrece el sistema, simplemente la intención es ocasionar daño y con ello el caos.

Citemos un escenario posible; un servidor web sufre un ataque informático, ¿cual fue el evento que lo originó?….. lo cierto es que se pudo dar por una o más vulnerabilidades en alguno de los sistemas que posee instalados, o bien que den soporte al propio servidor, otra posibilidad es dejar librados usuarios y contraseñas por defecto, sistemas operativos con otorgamiento de privilegios excesivos, fallos en el protocolo del diseño de comunicación, o bien errores de usuarios inexpertos que operan sistemas de información con información valiosa, sistemas operativos desactualizados tengamos presente que las actualizaciones refuerzan fallos o *"huecos"* en los sistemas y evitan serias complicaciones.

Consideraciones a tener en cuenta en Seguridad Informática

3.1.

- ✔ Seguridad en la red :

  La mayoría de los ataques se suceden por red, en este sentido es importante identificar y bloquear amenazas que surjan por este medio, incluyendo la protección de los datos, controles de acceso y seguridad perimetral.

3.2.

- ✔ Seguridad en la nube:

  Es indispensable proteger las implementaciones en la nube de una organización como ser aplicaciones, datos, websites, etc; esta protección se da a través de soluciones integradas, controles temporales, políticas y servicios de seguridad.

3.3.

- ✔ Seguridad endpoints:

  Esta acción consiste en proteger los endpoints (equipos de escritorio y portátiles) frente a potenciales amenazas, se implementa mediante controles de seguridad en la red y en los datos, endpoints también interviene en la prevención y reparación de daños ocasionados por ataques.

3.4.

- ✔ Seguridad móvil:

  Abarca tablets y smartphones que tienen acceso a datos corporativos y procura proteger de app’s maliciosas, Phishing, ataques de día cero y mensajería instantánea.

3.5.

- ✔ Seguridad zero trust:

  Intenta blindar los activos valiosos de las organizaciones a través de una autenticación constante de toda persona o dispositivo que tome contacto con los sistemas de información de la organización.

3.6.

- ✔ Seguridad de usuario final: tiene como objetivo educar al usuario final en sus intervenciones como operador, intentando concientizar sobre la importancia de las buenas prácticas de seguridad, y evitar que debido a un error humano, ingresen virus u otras amenazas a la organización.

3.7.

- ✔ Seguridad de aplicaciones:

  Contribuye en proteger las vulnerabilidades de las app’s evitando modificaciones u otro tipo de invasión no deseada. Controla los accesos no autorizados. Son importantes las actualizaciones de las app's ya que contienen *“parches”* que protegen espacios que pueden resultar vulnerados.

¿ Que beneficios ofrece la Ciberseguridad ?

Gestionar plataformas de seguridad conlleva proteger la red corporativa evitando ciber-ataques, a través de herramientas de protección y estableciendo estándares de seguridad que en su desarrollo proporcionan:

4.1.

- ✔ **PRIVACIDAD**

El servicio de seguridad brinda la posibilidad de conservar de forma efectiva los datos privados de empleados y clientes en caso de empresas u organización. Desproteger los datos habilita la posibilidad de sufrir ataques en los momentos menos esperados.

4.2.

- ✔ **PROTECCIÓN**

Proteger es sinónimo de cuidar y todo aquello que se cuida tiene mayor durabilidad, aplica en muchos sentidos, en este caso nos referimos a dotar seguridad tanto al hardware como el software para mantener un funcionamiento estable en términos de tiempo.

4.3. ✔ INTEGRIDAD

Una herramienta que proporciona soluciones integrales es el antivirus, entre otros, ya que además de proteger vulnerabilidades en el sistema operativo también provee asistencia para las aplicaciones, evita la manipulación de datos garantizando que la información sea verdadera y precisa.

4.4. ✔ PREVENCIÓN

Contar con un adecuado sistema de Seguridad Informática permite prevenir y evitar riesgos, funciona como alarma ante las intrusiones obstaculizando el peligro. Para poder implementar estos sistemas es necesario tener en cuenta las necesidades de la organización para de este modo poder intervenir de manera efectiva y profesional.

4.5. ✔ AUTENTICACIÓN

La autenticación otorga acceso a la información siempre y cuando se concedan los permisos a usuarios que están autorizados, generalmente se gestiona mediante códigos de verificación. Ej: al abrir un correo electrónico de Gmail en una Pc que no se utiliza con frecuencia, solicitará al usuario validar su identidad ejecutando una aplicación desde el móvil, puede ser YouTube entre otras, la autenticación validará los permisos en caso de que el usuario pueda cumplir con estos requerimientos, en este caso cumpliendo con lo solicitado, de lo contrario, restringe los permisos, aún poseyendo Usuario y Contraseñas correctas.

4.6. ✔ PRODUCTIVIDAD

Es importante considerar el tiempo operativo y el dinero que las organizaciones pierden al momento de padecer ataques cibernéticos si no cuentan con un plan de seguridad adecuado, con el hecho consumado es difícil establecer tiempos de puesta a punto para retomar la rutina normal de trabajo; es por este motivo que es de extrema necesidad contar con un plan de seguridad íntegro, que se encuentre actualizado para poder estar a la vanguardia y también contar con un plan de contingencia ante el peor escenario, el objetivo principal es que la productividad no se detenga o esté detenida el menor tiempo posible.

4.7. ✔ CONTROL

Posibilita realizar comprobaciones internas, observar el estado de los equipos en tiempo real y también de manera asincrónica inspeccionando las amenazas. El control permite anticipar, visualizar, ejecutar medidas de modo tal que el ataque quede solo en un intento. Es una labor de día a día que dificulta la misión de los espías.

4.8. ✔ ACCESIBILIDAD

En términos de ciberseguridad, la accesibilidad tiene que ver con la posibilidad de garantizar que todos tengan acceso igualitario a las herramientas y recursos necesarios para protegerse de las ciberamenzas, incluidos aquellos usuarios con acceso físico limitado a los dispositivos digitales, habilidades técnicas limitadas u otras barreras. La accesibilidad debe ser segura y accesible valga la redundancia.

Causales relevantes de ataque

5.1.

- ✔ Falta de controles de Seguridad: medidas de seguridad deficientes como por ejemplo el Firewall mal administrado, sistema de detección de intrusos o controles de acceso, son indispensables para no dejar a la organización desprovista de seguridad y en consecuencia se torne vulnerable.

5.2.

- ✔ Contraseñas poco seguras: es frecuente que los usuarios coloquen contraseñas predecibles o convencionales, esto facilita el acceso no autorizado a los datos y por ende representa una de las principales vulnerabilidades de seguridad en las organizaciones.

5.3.

- ✔ Backups irregulares: la falta de copias de seguridad periódicas de los datos críticos de la organización, resultan negligentes y puede ocasionar perdidas parciales o totales, la irresponsabilidad trae consecuencias con costos demasiados elevados. El backup es indispensable en las organizaciones.

5.4.

- ✔ Falta de formación sobre Seguridad Informática: son muchos los usuarios que operan sistemas sin tener claros muchos conceptos y esto conlleva a que se cometan errores que terminan generando problemas significativos, el Phishing aumenta la posibilidad de caer en estas trampas ocasionando caos en la organización. El 80% de los ciber-ataques a empresas u organizaciones son causados por errores humanos.

5.5.

- ✔ Conexión a redes públicas desprotegidas: el acceso a redes Wi-Fi públicas y no seguras, puede permitir a los atacantes interceptar y comprometer el tráfico de datos, poniendo en riesgo la confidencialidad de la información.

5.6.

- ✔ Bases de datos expuestas: una configuración inadecuada puede llevar a una exposición no intencionada de datos sensibles, dejando la información vulnerable a sustracciones. Es decir, cuando la base de datos no está protegida correctamente, la información sensible puede quedar expuesta y ser accesible a personas no autorizadas, esto podría incluir información confidencial de clientes, datos financieros, documentación, contraseñas u otra información privada.

Tipos habituales de ciber-ataques

6.1. ✔ MALWARE

Son programas dañinos destinados a interrumpir, dañar u obtener acceso no autorizado a los sistemas informáticos. El malware puede infectar dispositivos a través de una variedad de rutas, incluidos archivos adjuntos de correo electrónico, sitios web comprometidos, y descargas de software. Una vez instalado en el sistema genera acciones maliciosas como el robo de datos, secuestro del sistema e incapacidad del dispositivo.

6.2. ✔ PHISHING

Es un tipo de ciberataque que consiste en el envío de correos electrónicos genéricos por parte de ciberdelincuentes que se hacen pasar por legítimos. Estos correos poseen enlaces fraudulentos para robar información privada del usuario. Utilizan membretes de entidades reconocidas a nivel mundial como ser Netflix, Mercado Libre, YouTube, etc, para de este modo generar confianza en el usuario ya que accede por creer reconocer el remitente.

6.3. ✔ RANSOMWARE

El ransomware es el malware que cifra los datos tantos locales del equipo como en red. Tiene un proceder muy rápido, y propone un rescate económico para descifrarlo. Se entiende que este malware es uno de los mas perjudiciales ya que daña los datos al cifrarlos y los torna inaccesibles, a diferencia de otros que solo se infectan. Se recomienda jamás negociar el rescate con la intención de que esta práctica extorsiva algún día finalice.

✔ TROYANO

Es un tipo de malware que engaña a los usuarios disfrazándose de software legítimo. Un troyano oculta su intención maliciosa bajo el encubrimiento de una aplicación inofensiva, embaucando a los usuarios para que ejecuten código dañino en sus dispositivos. Un troyano puede realizar varias acciones maliciosas por ej. proporcionar una entrada de puerta trasera para hackers, acceder a datos, contraseñas e información confidencial.

✔ INGENIERÍA SOCIAL

La Ingeniería Social es un tipo de ataque distinto al que veníamos viendo ya que intenta encontrar la vulnerabilidad en la persona y no en el equipamiento, es decir, a través del engaño intenta persuadir a las víctimas para que pongan en peligro su seguridad o bien rompan las prácticas recomendadas para obtener de este modo una ganancia financiera o informativa. El objetivo principal es influir, piratear la mente en lugar de un sistema. Muchos de estos *exploits* dependen de la buena naturaleza de las personas o del miedo a situaciones negativas. La ingeniería social es popular entre los atacantes por que dadas las medidas de seguridad informática es resulta aveces mas fácil explotar a las personas en lugar de intentar vulnerabilidades de la red y el software.

7.1. Bibliografía

[1] Q. Kiser, (2020)

Ciberseguridad Una Simple Guía para Principiantes sobre Ciberseguridad, Redes Informáticas y Como Protegerse de Hacking en Forma de Phishing, Malware, Ransomware e Ingeniería Social. Amazon Digital Services LLC Independently published – Kdp. Chicago.

[2] G. Baca Urbina, (2017)

Introducción a la Seguridad Informática. Primera Edición. Grupo Editorial Patria. México.

[3] M. I, Romero Castro, G. L, Figueroa Morán, D. S, Vera Navarrete, J. E, Álava Cruzatty, G. R, Parrales Anzúles , C. J, Álava Mero, Á. L, Murillo Quimiz,M. A, Castillo Merino, (2018). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades. 3Ciencias. España.

[4] Fundación Sadosky, (2023)

Buenas Prácticas en Seguridad de la información y ciberseguridad. https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf