22-1-2024

Universidad del Caribe

2000 CANCUN, QUINTANA ROO, MEXICO

CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

SEGURIDAD DE DATOS

ISMAEL JIMENEZ SANCHEZ (TUXTTER)

SECCION 1

INGENIERIA EN DATOS E INTELIGENCIA ORGANIZACIONAL

KENNY HERNANDEZ PEREZ – 200300661

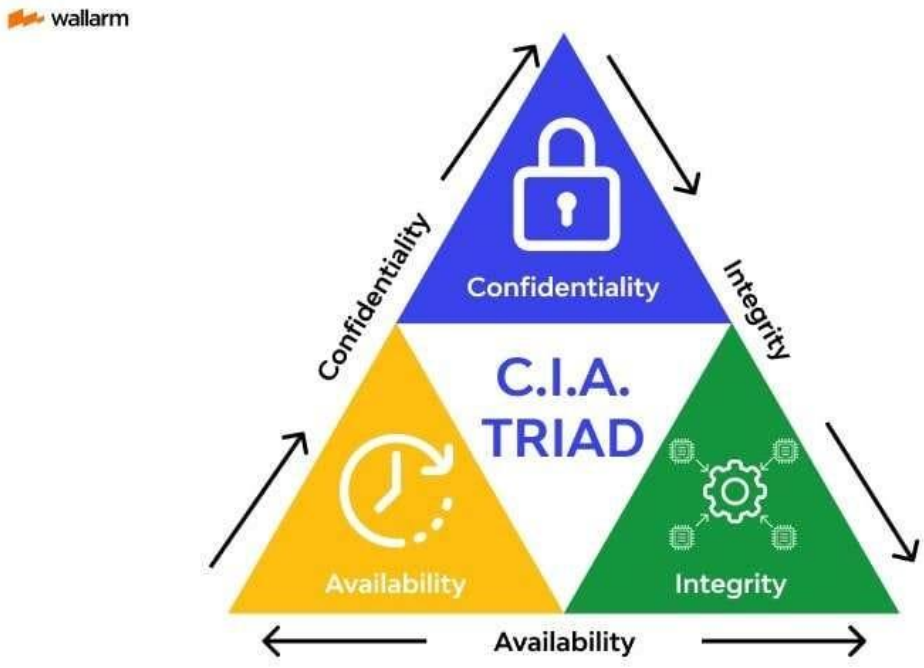
CONCEPTOS BASICOS DE SEGURIDAD

TRIADA CIA

Entre el mar de términos y conceptos básicos de Ciberseguridad que una persona tiene que aprender a lo largo de una Licenciatura o Maestría en Seguridad Informática, el mejor lugar de inicio es lo que se le conoce como la Triada CIA (por sus siglas en inglés). Confidencialidad. Integridad. Disponibilidad.

Es fundamental conocer el significado que estas palabras tienen con el fin de que un hacker ético, o aquellos conocidos como hackers de sombrero blanco; puedan desarrollar políticas de seguridad y protocolos de seguridad informática que no solo protejan la información que se está manejando de ser atacada por piratas informáticos, sino al usuario a quien le pertenecen estos datos o que busca hacer un uso ético (hacking ético) de los mismos.

El sector de la Seguridad Informática sigue en constante crecimiento a nivel mundial. Se necesita una gran cantidad de expertos con un perfil en Ciberseguridad (es decir, hackers éticos o aquellos que hayan tomado cursos online de ethical hacking y/o cursos de ciberseguridad en sistemas informáticos) para cumplir con las demandas que existen actualmente.

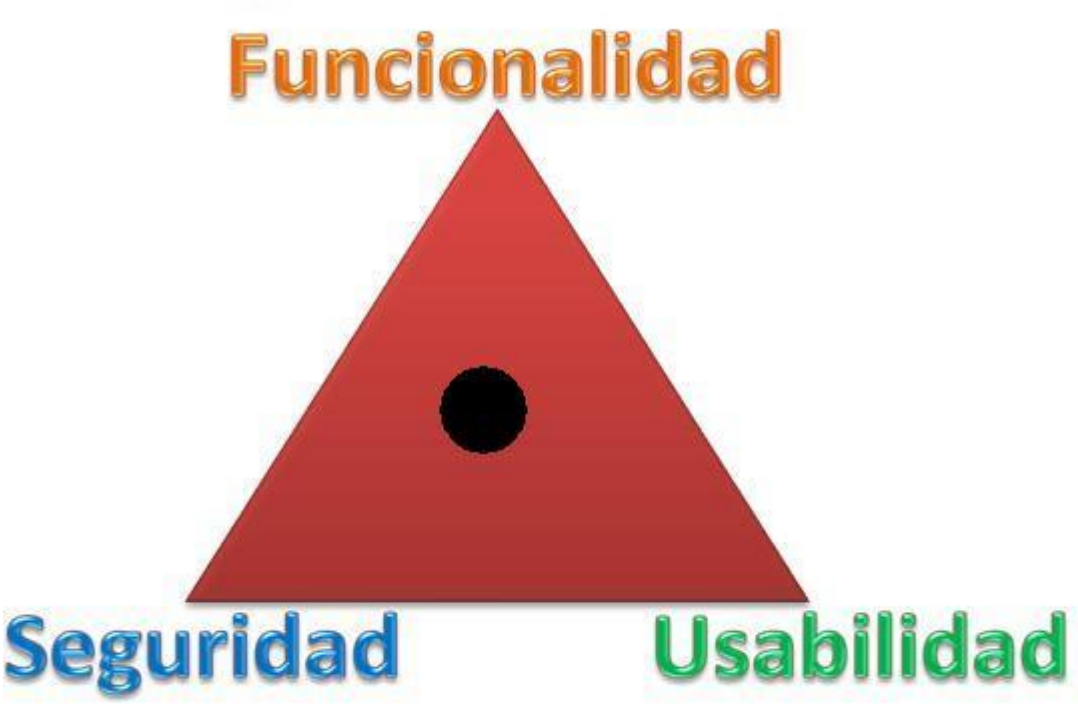


TRIANGULO DE LA USABILIDAD

A la hora de desarrollar productos de Software es necesario saber a quién o qué desarrollamos, pues la respuesta a esas preguntas guiará el tipo de desarrollo que debemos seguir a fin de tener un producto que se adapte a su entorno real.

Partiendo de allí, es pertinente hablar de un triángulo muy curioso, que básicamente busca aclarar esas dudas para el desarrollo, el triángulo FSU, un acrónimo de Funcionalidad-Seguridad-Usabilidad, tres cosas fundamentales a la hora de desarrollar productos de software.

Dependiendo de a quién o qué desarrollaremos, uno de estos tres aspectos podría explotarse más que otro, el punto negro que está en medio del triángulo define que tan seguro, funcional y usable es nuestro producto. Dicho punto puede movilizarse a una esquina del triángulo según sea la necesidad, pero mientras más se acerca a una esquina evidentemente se aleja de las otras.



Si queremos un sitio rico en cuanto a la interfaz, con una buena navegabilidad que ayude al usuario a tener la mejor experiencia posible, entonces es bueno movernos a la esquina de la usabilidad, pero nótese que al hacerlo nos alejamos de las otras dos esquinas.

Normalmente, cuando más fácil es un sistema, menos protegido está, pues la seguridad no va de la mano a las funcionalidades y la usabilidad del producto, es decir; mientras más alejados de estas dos esquinas estemos, más seguro será el producto.

La seguridad en el desarrollo de software es un aspecto importante a tener en cuenta, se basa en asegurar la confidencialidad, la integridad y la disponibilidad de la información, sin embargo certificar una protección dura nos lleva a otro problema significativo; la usabilidad.

Pues, mientras más seguro queramos nuestro producto más alejado de la usabilidad estará, entonces, es aquí donde es importante dejar claro que según el producto y la organización a la que se le desarrollara debemos escoger a que esquina nos acercamos más.

RIESGO EN CIBERSEGURIDAD

El término riesgo de seguridad de la información se refiere al daño potencial causado por ataques a los sistemas de TI. El riesgo de TI incluye una amplia gama de eventos potenciales, como violaciones de datos, acciones de cumplimiento normativo, costos financieros, daños a la reputación y otros. Aunque los términos «riesgo» y «amenaza» se usan con frecuencia indistintamente, no son sinónimos. «Riesgo» es un término más abstracto: algo que puede o no ocurrir. Una amenaza es un peligro específico y presente».

AUTENTIFICACION MULTIFACTOR (MFA)

La autenticación multifactor (MFA) es un proceso de registro en varios pasos que requiere que los usuarios ingresen algo más de información que simplemente una contraseña. Por ejemplo, junto con la contraseña, los usuarios deberán ingresar un código que se envía a su correo electrónico, responder a una pregunta secreta o escanear una huella dactilar. Una segunda forma de autenticación puede ayudar a evitar el acceso no autorizado a una cuenta si la contraseña del sistema se ha visto expuesta.

¿Por qué es necesaria la autenticación multifactor (MFA)?

La seguridad digital es fundamental en el mundo de hoy, ya que tanto empresas como usuarios almacenan información confidencial en línea. Todo el mundo interactúa con aplicaciones, servicios y datos que se almacenan en Internet mediante cuentas en línea. Una filtración o mal uso de esta información en línea puede tener consecuencias graves en el mundo real, como un robo financiero, una interrupción de la actividad empresarial o la pérdida de privacidad.

Aunque las contraseñas protegen los activos digitales, esta protección no es suficiente. Los ciberdelincuentes expertos intentan buscar contraseñas de manera activa. Al descubrir una contraseña, se puede obtener acceso de manera potencial a varias cuentas para las que es posible que haya reutilizado la contraseña. La autenticación multifactor actúa como una capa adicional de seguridad para evitar que usuarios no autorizados accedan a dichas cuentas, incluso cuando se ha robado la contraseña. Las empresas utilizan autenticación multifactor para validar identidades de usuarios y brindar un acceso rápido y práctico a los usuarios autorizados.

¿Cuáles son los beneficios de la autenticación multifactor?

Reduce el riesgo de seguridad

La autenticación multifactor reduce los riesgos derivados de errores humanos, contraseñas extraviadas y dispositivos perdidos.

Permite iniciativas digitales

Las organizaciones pueden llevar a cabo iniciativas digitales con confianza. Las empresas utilizan autenticación multifactor para ayudar a proteger los datos de la organización y de los usuarios, de modo que puedan realizar interacciones y transacciones en línea de manera segura.

Mejora la respuesta de seguridad

Las compañías pueden configurar un sistema de autenticación multifactor para enviar de manera activa una alerta en cuanto se detecten intentos de inicio de sesión sospechosos. Esto ayuda tanto a compañías como a individuos a responder más rápido a ciberataques, lo que reduce cualquier daño potencial.

VULNERABILIDAD EN CIBERSEGURIDAD

En informática, una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas y pueden ser explotadas o utilizadas por intrusos o atacantes.

Para entenderlo mejor, una vulnerabilidad puede ser, por ejemplo:

- Un servicio de un sistema de computación corriendo en un determinado puerto lógico.
- Sistemas y aplicaciones no actualizados o parcheados que presentan múltiples vulnerabilidades.
- Una red Wifi abierta.
- Un puerto abierto en un firewall.
- Un insuficiente o inexistente control de acceso físico a las instalaciones.
- La no aplicación de una política de gestión de contraseñas.
- Tipos de vulnerabilidad informática

Algunos tipos de vulnerabilidades típicas de sistemas y aplicaciones son:

Buffer overflow o desbordamiento de buffer: se da cuando las aplicaciones no controlan la cantidad de datos que copian en el buffer y que al sobrepasar el tamaño de este pueden modificar zonas de memoria contiguas afectando a los datos que albergan.

Condición de carrera: las aplicaciones o sistemas no implementan exclusiones mutuas en el acceso a recursos compartidos, como por ejemplo una variable, y varios procesos acceden a ella al mismo tiempo obteniendo valores no esperados.

Error de formato en cadenas: cuando las aplicaciones no validan los datos de entrada que introduce el usuario a las mismas, pudiendo ejecutar por ejemplo comandos o instrucciones que pueden permitir al atacante obtener datos confidenciales o dañar el sistema.

Cross Site Scripting: se basa en que los atacantes incrustan scripts en páginas web legítimas afectadas por esta vulnerabilidad y por las que navega el usuario. Este introduce datos como por ejemplo, su usuario y su contraseña, pero no en la web legítima si no en la del atacante, que roba así sus datos.

Inyección de SQL: cuando no se validan los datos de entrada a formularios que se comunican con bases de datos se podría ejecutar código SQL malicioso que por ejemplo permitiera obtener datos confidenciales o corromper los datos de las tablas.

AMENAZA EN LA CIBERSEGURIDAD

Una amenaza en ciberseguridad abarca cualquier acción malintencionada o situación que ponga en riesgo la seguridad de tus dispositivos y datos en el mundo digital. Las crean ciberdelincuentes que buscan acceder, dañar o robar información privada.

Ya sabés que una amenaza cibernética es cualquier evento que atenta contra los sistemas y datos personales en el entorno digital. Son delitos informáticos que responden a distintas motivaciones:

- robo de información
- sabotaje
- espionaje
- extorsión
- interrupción de servicios

Al igual que la tecnología, las amenazas cibernéticas también están en constante evolución. Esto es un problema, porque se vuelven cada vez más sofisticadas y eficientes.

IMPACTO EN LA CIBERSEGURIDAD

El impacto de la seguridad de la información es la consecuencia de una violación de la política de seguridad de la información. Es el impacto que resulta de un ataque o intento de ataque a la postura de seguridad de la información de una organización. La evaluación de riesgos de una organización identifica los tipos y la magnitud de tales amenazas, así como su vulnerabilidad a ellas, dicha evaluación de riesgos debe incluir todas las violaciones de datos conocidas, las pérdidas u otros incidentes que hayan ocurrido en el pasado, pero también examinar las amenazas actuales a las que se enfrenta una organización.

Tipos de impacto en la seguridad de la información

En resumen, un impacto en la seguridad de la información es cuando existe una amenaza a la seguridad informática y esta logra atravesar las medidas de defensa, bien sea malware, virus, etc. cualquier tipo de ataque informático que pueda poner en peligro cualquier tipo de información, datos, etc.

Los impactos en la seguridad de la información pueden ser de diferentes tipos, entre los que destacan:

Impactos financieros

Son los impactos directos en el costo operacional de una organización debido a brechas de seguridad o incidentes de ciberseguridad. Por ejemplo, si un atacante logra ingresar a un sistema de procesamiento de pagos y roba información de tarjetas de crédito, esto puede resultar en multas significativas para la empresa, además de los costos de reparación del sistema y posiblemente compensaciones a los clientes afectados.

Impactos operacionales

Son las interrupciones en los procesos de negocio debido a incidentes de seguridad. Por ejemplo, un ataque de denegación de servicio (DoS) podría hacer que un sitio web de comercio electrónico no esté disponible, interrumpiendo las ventas y afectando la operatividad del negocio.

Impactos legales y regulatorios

Las organizaciones están sujetas a una variedad de leyes y regulaciones que requieren ciertos niveles de seguridad de la información. Los incumplimientos de seguridad pueden llevar a sanciones legales. Por ejemplo, el Reglamento General de Protección de Datos (GDPR) en la Unión Europea impone multas severas por incumplimientos de seguridad que comprometen los datos personales.

Impactos en la reputación

Los incidentes de seguridad pueden dañar la reputación de una empresa y su relación con los clientes, socios y el público en general. Por ejemplo, si una red social sufriera una brecha de seguridad y los datos de los usuarios se filtraran, la confianza del público en esa red social podría disminuir, lo que podría llevar a una pérdida de usuarios y anunciantes.

Impactos estratégicos

Algunos ataques pueden comprometer la ventaja competitiva de una empresa. Por ejemplo, si un competidor lograra obtener acceso a la propiedad intelectual o a los secretos comerciales de una empresa a través de un ciberataque, podría utilizar esa información para su propio beneficio.

BIBLIORAFIA

Sociales, R. (2021, 23 febrero). *Conceptos básicos de ciberseguridad: triada CIA*. UNIAT. https://www.uniat.edu.mx/conceptos-basicos-de-ciberseguridad/#:~:text=Entre%20el%20mar%20de%20t%C3%A9rminos,Disponibilidad.

Cercado, C. (2015, 31 julio). *La funcionalidad, la usabilidad y la seguridad en el desarrollo de software.* Cultura Informatica. https://culturatics.wordpress.com/2015/07/26/la-funcionalidad-la-usabilidad-y-la-seguridad-en-el-desarrollo-de-software/

Financial Crime Academy. (2023, 11 diciembre). Definición de fuentes de riesgo de seguridad de la información: Gestión de riesgos de seguridad de la. *Financial Crime Academy*. https://financialcrimeacademy.org/es/definicion-de-fuentes-de-riesgo-de-seguridad-de-la-informacion-gestion-de-riesgos-de-seguridad-de-la-informacion-paso-1/#:~:text=El%20t%C3%A9rmino%20riesgo%20de%20seguridad,a%20la%20reputaci%C3%B3n%20y%20otros.

¿Qué es la autenticación multifactor? - Explicación de la autenticación multifactor - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/mfa/

Santander, B. (s. f.). *Vulnerabilidad*. Banco Santander. https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica%2C%20una%20vulnerab

ilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.

Argentina, B. (2023, 23 octubre). ¿Qué es una amenaza en ciberseguridad? EJEMPLOS - Bitso Blog. *Bitso*. https://blog.bitso.com/es-ar/seguridad-ar/que-es-una-amenaza-en-ciberseguridad#:~:text=Una%20amenaza%20en%20ciberseguridad%20abarca,da%C3%B1ar%20o%20robar%20informaci%C3%B3n%20privada.

Khoyotte, & Khoyotte. (2023, 25 mayo). *Para comprender el impacto en la seguridad de la información vamos a read more*. Seguridad en la informática. https://seguridadenlainformatica.com/que-se-entiende-por-impacto-en-la-seguridad-de-la-informacion/