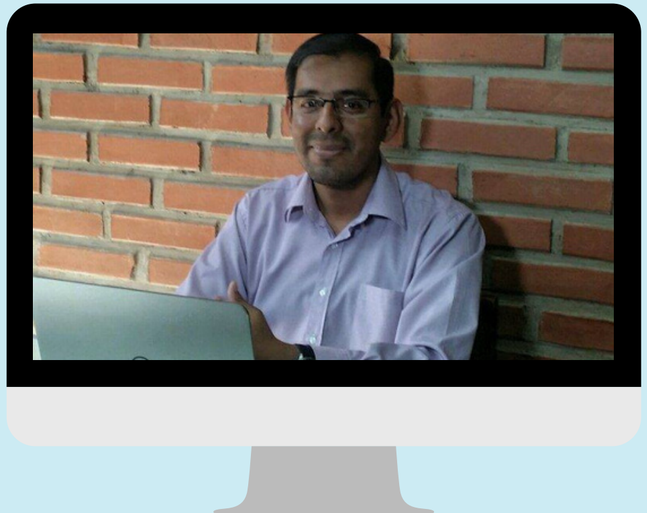
BY JAVIER VASQUEZ CRUZ

Seguridad Informática

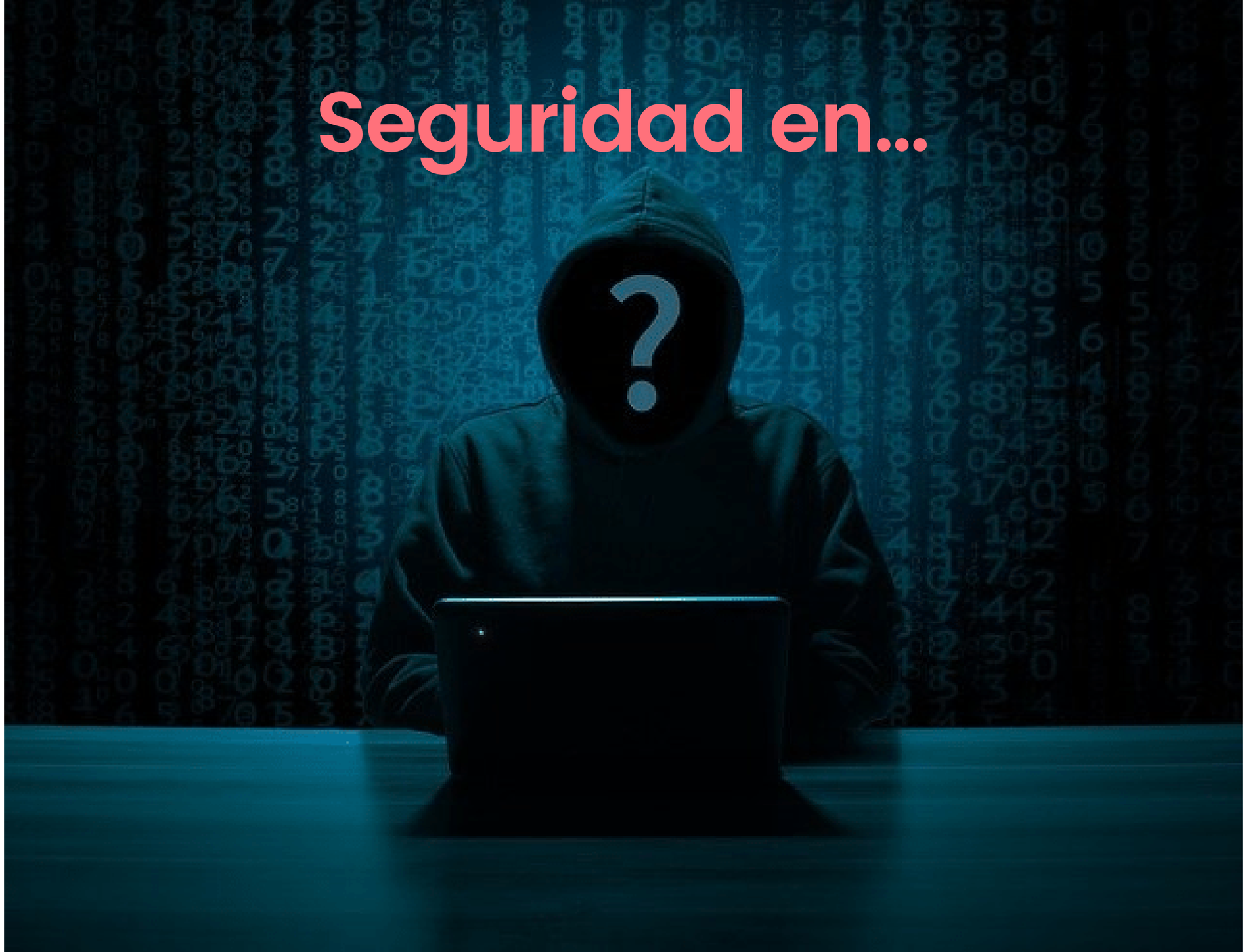


Objetivos

- Realizar una breve introducción a la seguridad informática.
- Describir los conceptos principales de la seguridad informática.
- Plantear agregar elementos de seguridad en los proyectos finales.

La tecnología en el mundo actual

¿Sera necesario brindar un nivel de seguridad?


Seguridad en...
?

Seguridad en...

Software

Hardware

Pero también en...

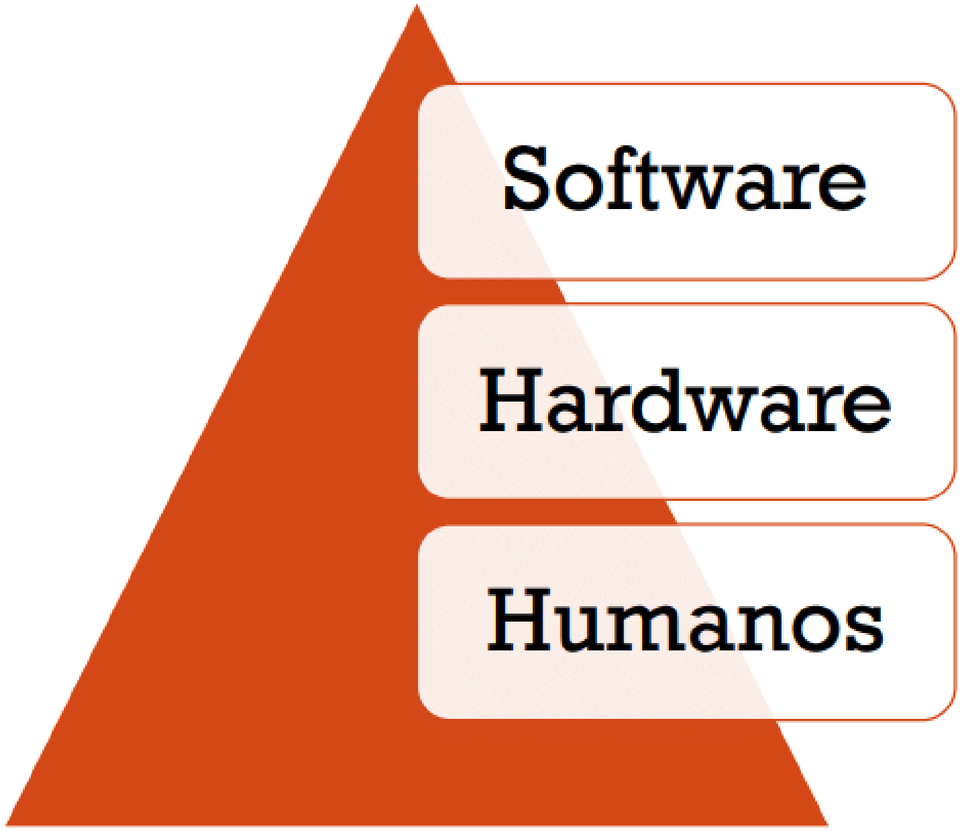
Pero también en...

Este sistema esta conformado por:

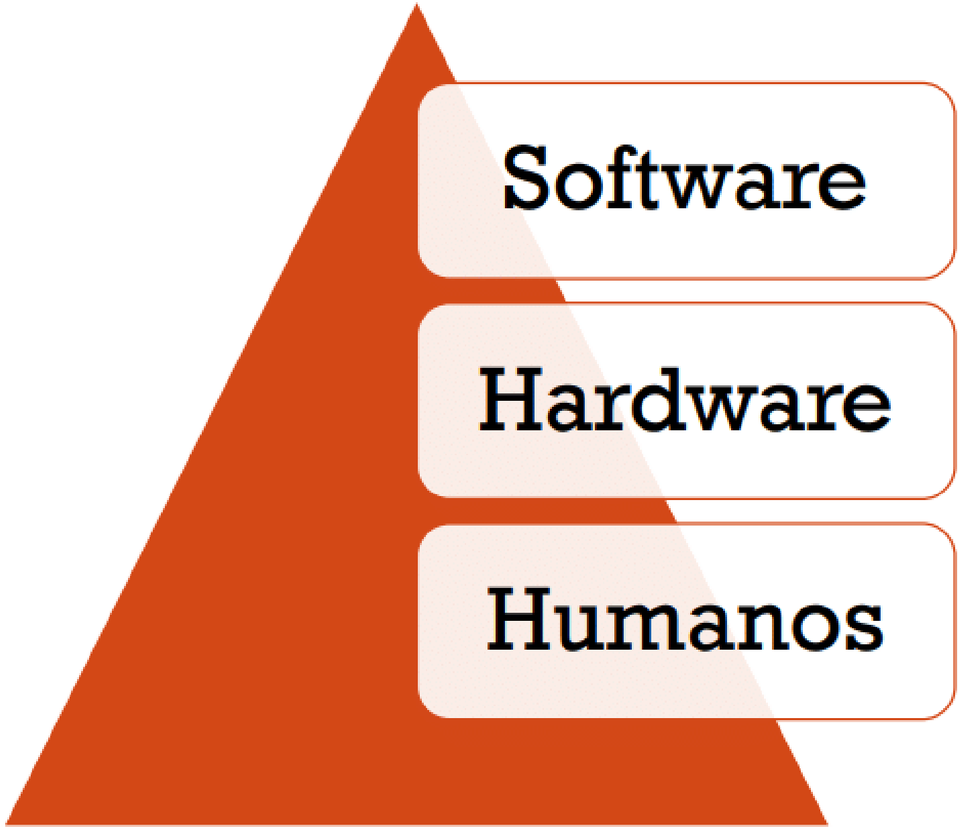
Software

Hardware

Usuario



SEGURIDAD



SEGURIDAD

Algo interesante que puedes observar en el grafico es que los humanos están en la base de la pirámide.
¿Por que?

Seguridad Informática

- Protección
- Recursos Valiosos.
- Posibles peligros.

Proteger

resguardar, defender o amparar a algo o alguien

proactivo

preventivo

GIF

Puntos importantes...

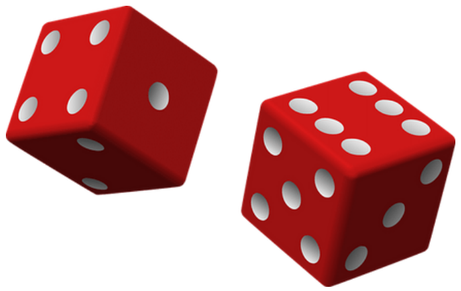
Recurso Valioso

importancia

análisis e identificación

cuantitativo o cualitativo

Posibles Peligros



probabilidad

análisis e identificación

cuantitativo o cualitativo

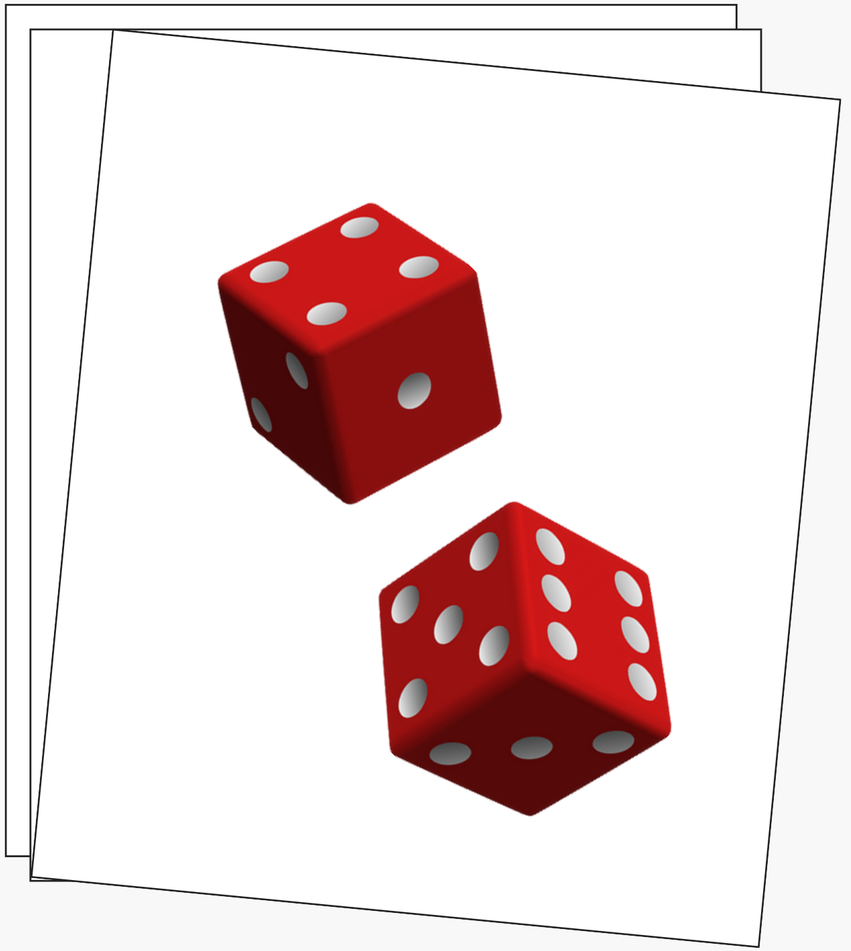
El software (código) es vital para el exito del mismo.

La información que genera o gestiona es de vital importancia.

Necesidad de brindar un nivel de seguridad en software, hardware y el personal que la administra.

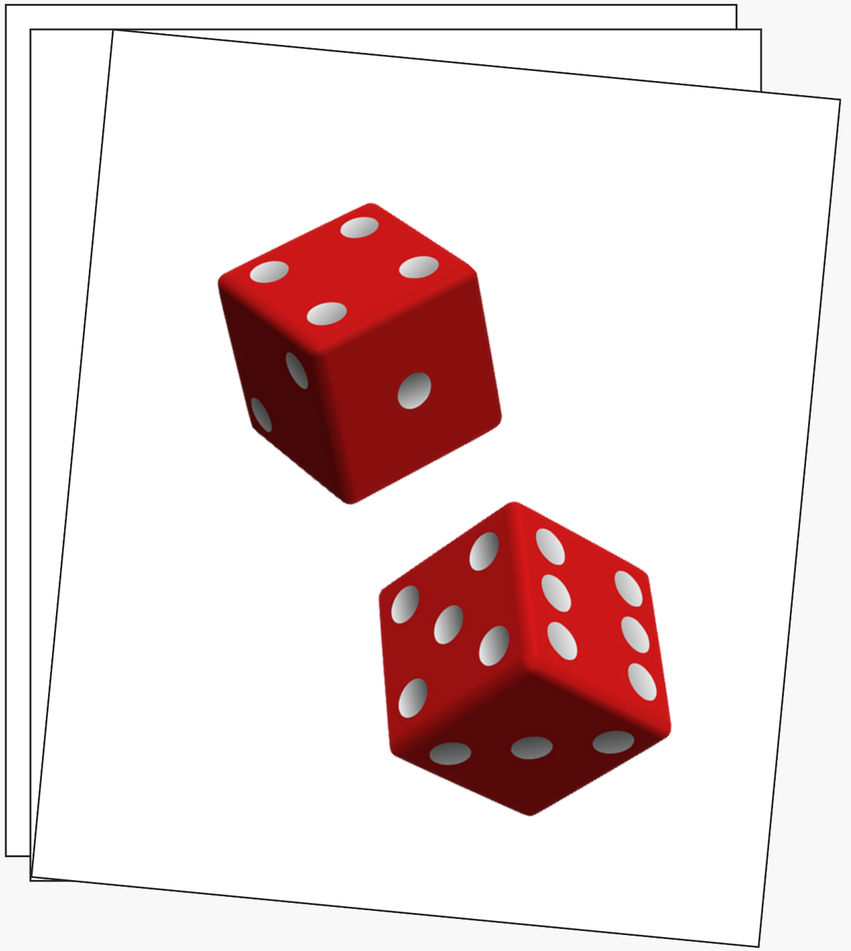
Probabilidad

Existen amenazas, para las cuales hay información suficiente (series históricas, compañías de seguros y otros datos) para establecer con razonable objetividad su **probabilidad de ocurrencia**.



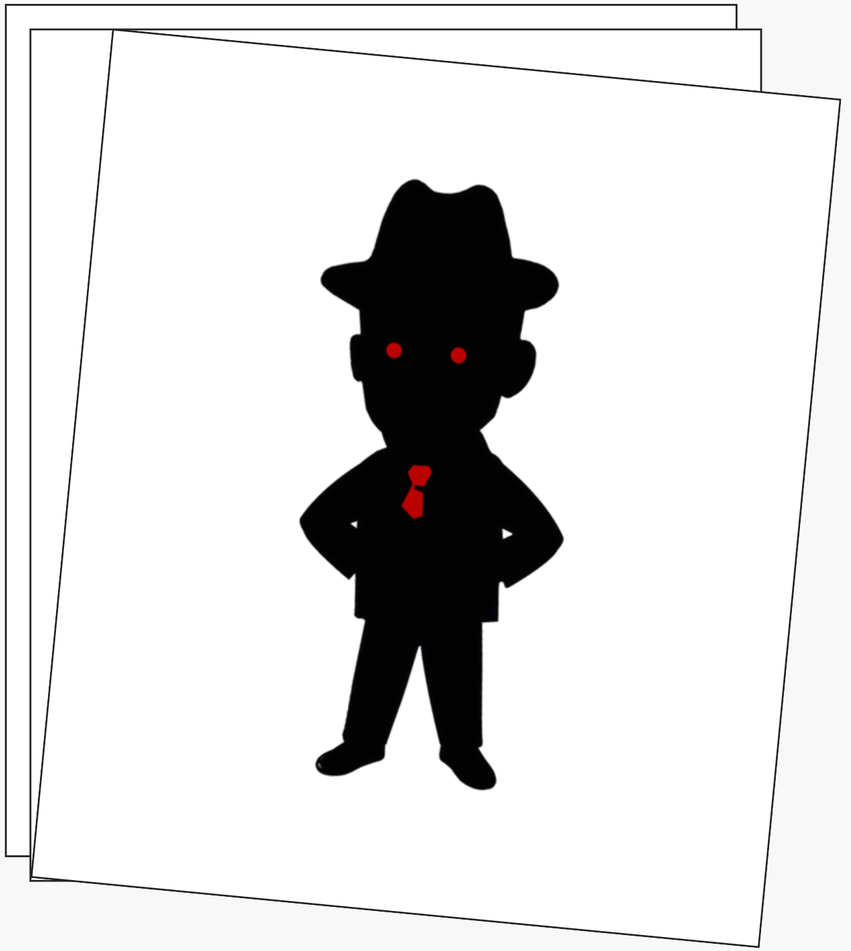
Probabilidad

Otras amenazas presentan mayor dificultad en establecer cuantitativamente la probabilidad. Por ejemplo, el acceso no autorizado a datos; dónde se hacen estimaciones sobre la base de experiencias.



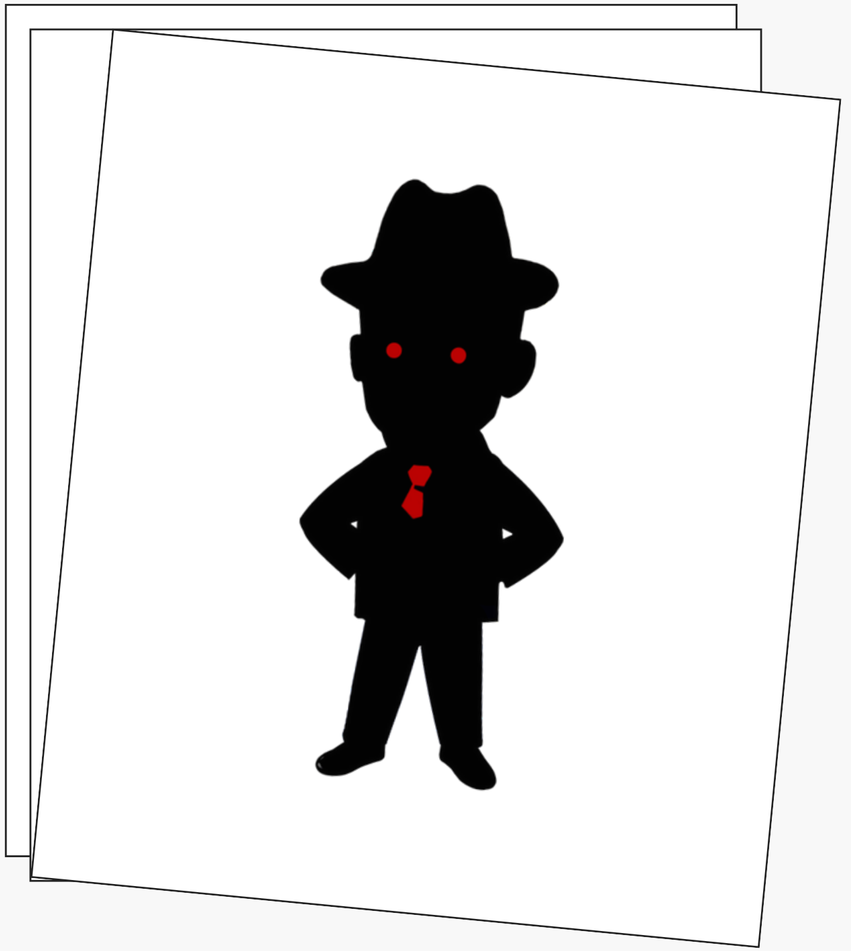
Amenaza

Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, malware, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

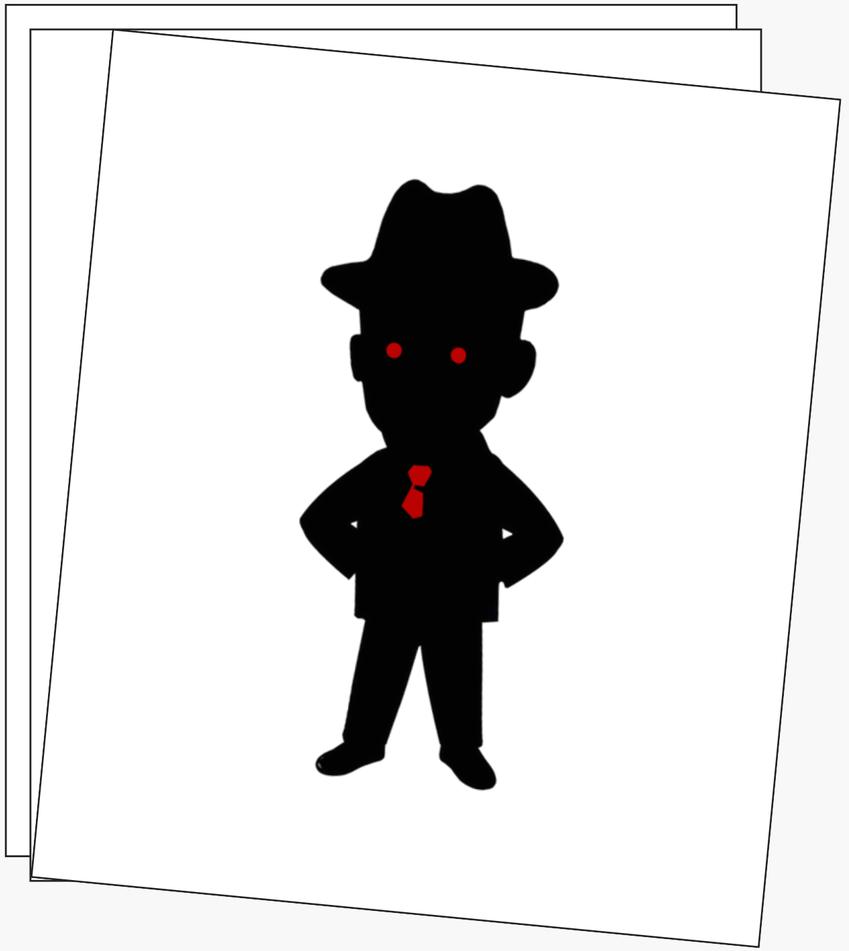


Amenaza

Las amenazas pueden ser de carácter físico o lógico.



¿Qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.??

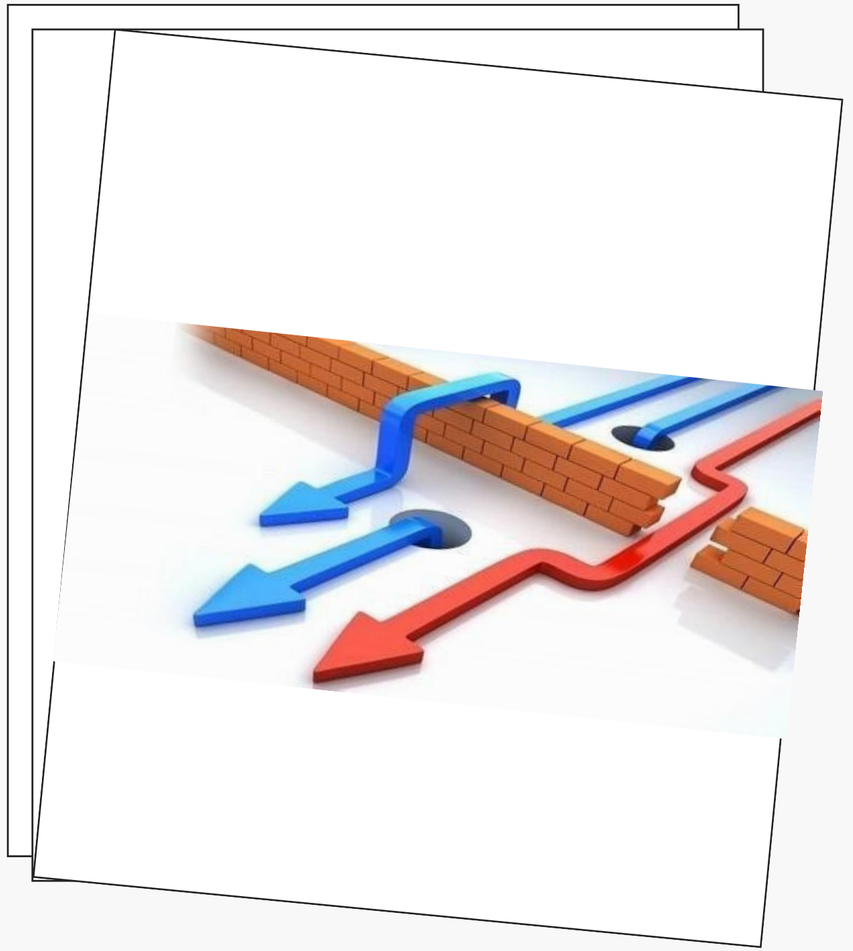


Riesgo

La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole perdidas o daños

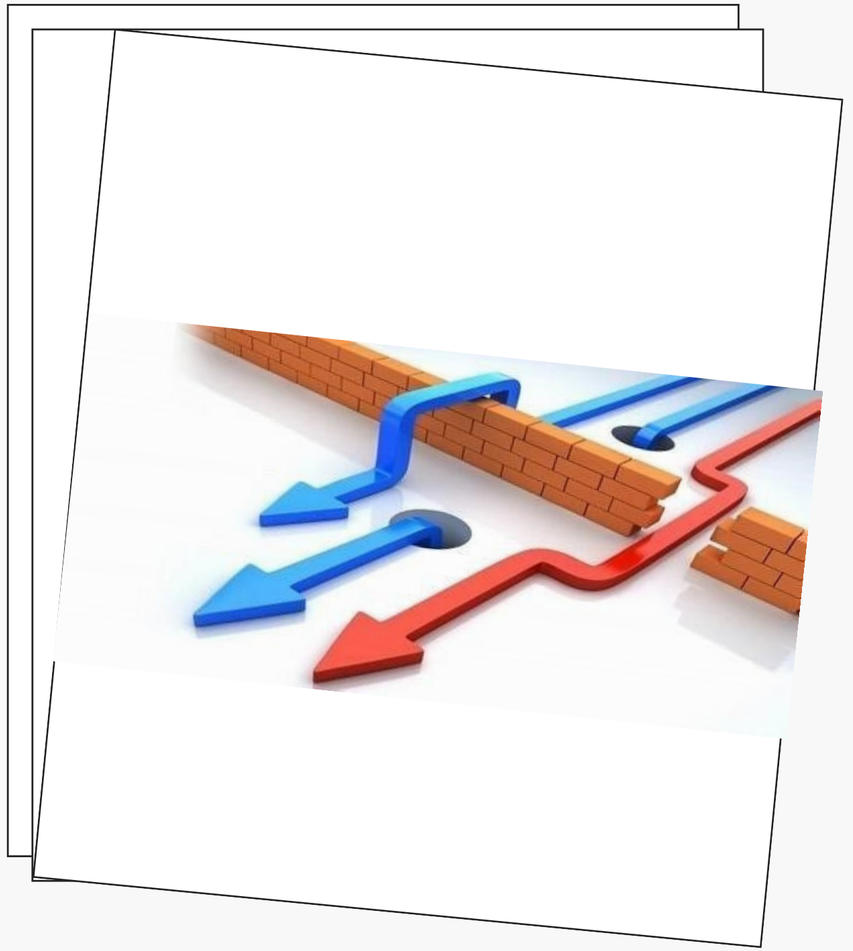
Vulnerabilidades

Las amenazas logran materializarse a través de las debilidades existentes, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.



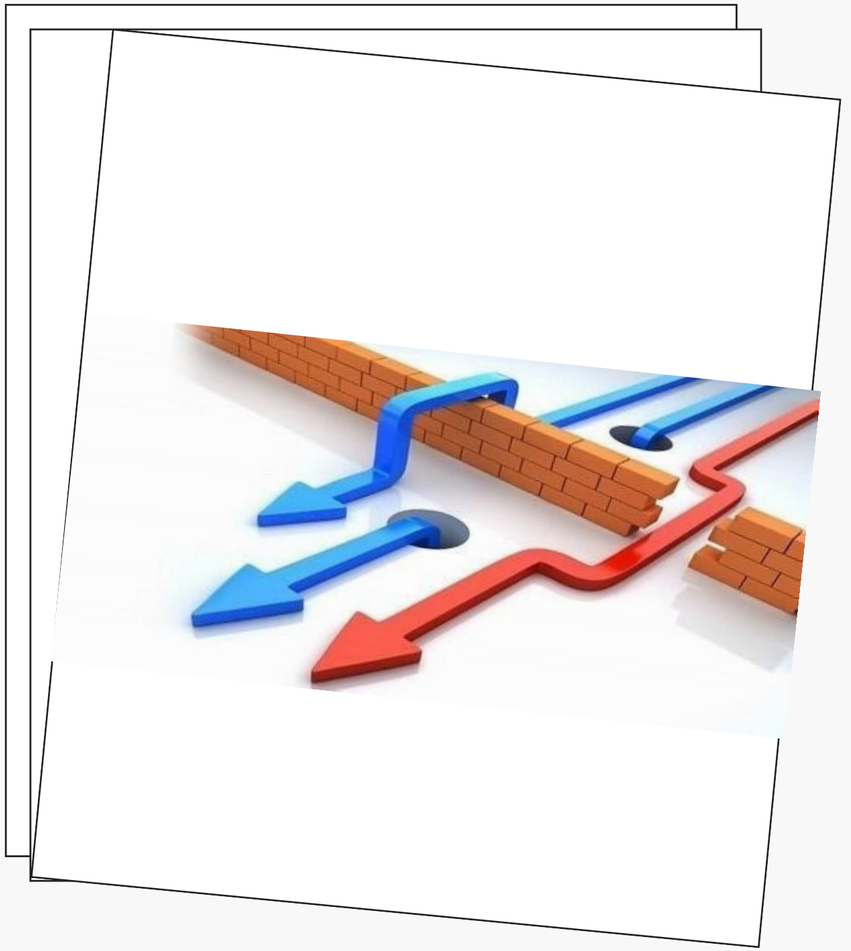
Vulnerabilidades

Estas vulnerabilidades son de naturaleza variada. A modo de ejemplo se citan las siguientes: falta de conocimiento del usuario, tecnología inadecuadamente probada (“testeada”), transmisión por redes públicas,etc.

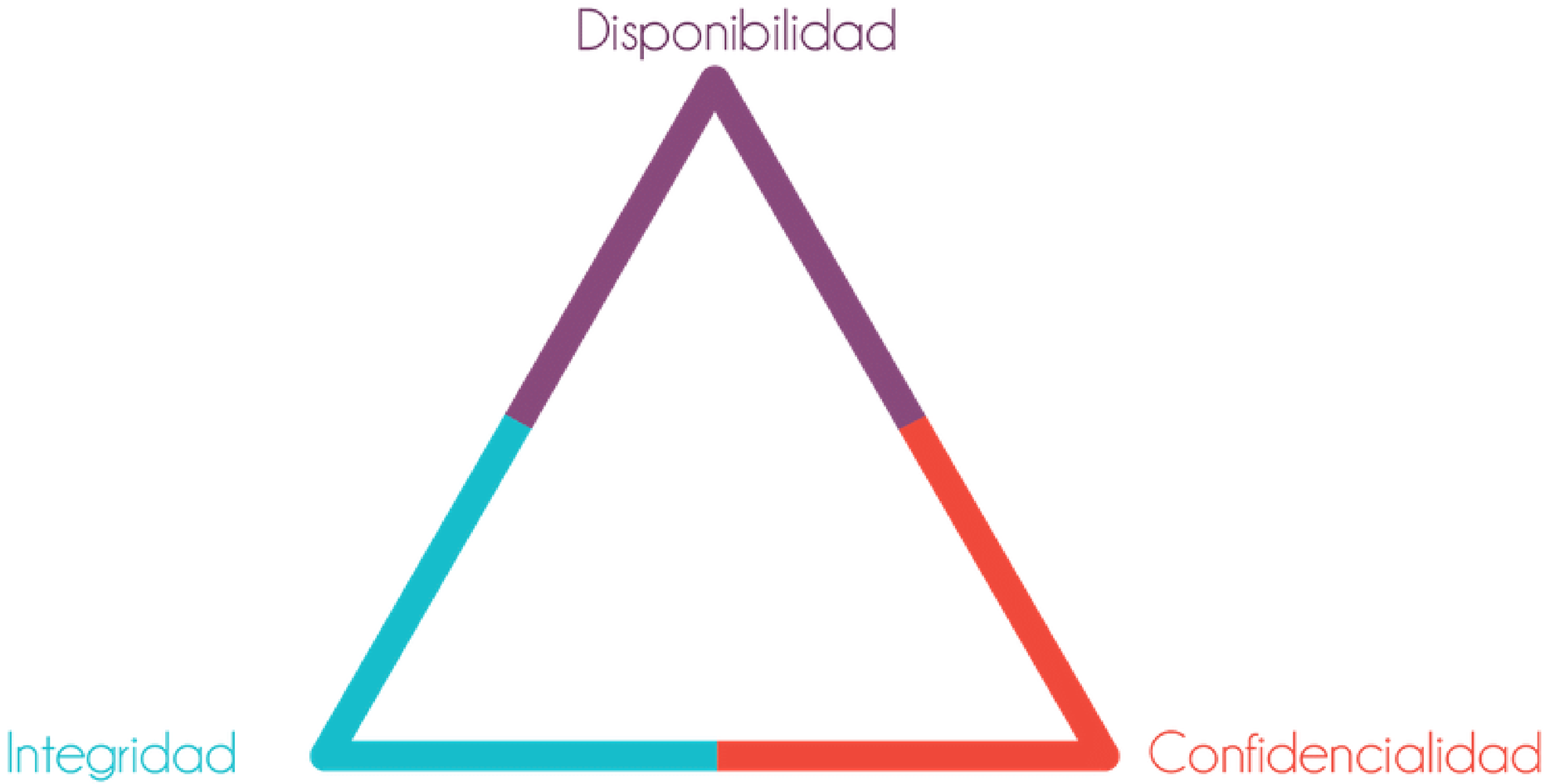


Vulnerabilidades

Una vulnerabilidad común es contar con antivirus no actualizado o mal configurado, la cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado la amenaza (virus) si bien potencialmente seguiría existiendo no podría materializarse.



Principios o Pilares



Integridad

Un elemento permanezca integro, o sea modificado o eliminado por un elemento autorizado.

Integridad

La integridad asegura que:

- No se realizan modificaciones de datos en un sistema por personal o procesos no autorizados.
- No se realizan modificaciones no autorizadas de datos por personal o procesos autorizados.
- Los datos son consistentes, es decir, la información interna es consistente entre si misma y respecto de la situación real externa.

Hackean bases de datos, usuarios y claves de seis sitios web gubernamentales

Publicado el 31/05/2016

Un hacker chileno, que en el Twitter se denomina @JoshuaProvoste, vulneró la seguridad de sitios web del estado boliviano y logró acceder a sus bases de datos, usuarios y claves de sitios, lo que no había ocurrido en ocasiones anteriores, cuando lo único que conseguían los hackers era cambiar el aspecto de las webs.

Link

Confidencialidad

Un elemento solo pueda ser accedido (leído) por un elemento autorizado.
La confidencialidad intenta prevenir la revelación no autorizada, intencional o no, del contenido de un mensaje o de información en general.

La advertencia de que se están hackeando las cámaras de vigilancia de los bebés

Publicado el 3 marzo 2020

Las cámaras de seguridad y los monitores de vigilancia de bebés se han convertido en un jugoso objetivo para los piratas informáticos.

Link

Disponibilidad

Un elemento tiene que estar disponible para quienes la necesiten y cuando la necesiten,si están autorizados.

Disponibilidad

La disponibilidad asegura que el acceso a los datos o a los recursos de información por personal autorizado se produce correctamente y en tiempo. Es decir, la disponibilidad garantiza que los sistemas funcionan cuando se les necesita.

¿Cómo un único ciberataque pudo dañar a varios sitios populares como Twitter, Spotify y Netflix al mismo tiempo?

Publicado el 21 octubre 2016

Un ciberataque este viernes literalmente rompió internet.Páginas de servicios populares como Twitter, Spotify, Netflix, Airbnb, SoundCloud, Amazon y hasta diarios como The New York Times se cayeron o funcionaron a baja velocidad durante varias horas.

Link

Breve historia de los "hackers" y sus andanzas

El mundo está lleno de hackers, o eso es al menos lo que parece. En los últimos meses apenas ha pasado un día en el que no se haya dado a conocer una nueva violación de seguridad informática.

Link

Resumen

Se debe identificar claramente cuales son los recursos valiosos para una organización.

Se debe brindar un nivel de seguridad adecuado a los recursos valiosos de acuerdo a las posibilidades de la organización.

Es importante identificar las amenazas, riesgos y vulnerabilidades asociadas a un recurso valioso.

La seguridad de la información se basa en 3 pilares: integridad, confidencialidad y
disponibilidad.

Ejemplo

1. En el instituto Alvarez Plata Nocturno.
2. Identifica los recursos valiosos (mínimo 3) y ordénalos según importancia (asignar un peso).
3. Identifica de cada uno los:
    a. Riesgos.
    b. Amenazas.
    c. Vulnerabilidades.

Practica

1. Elige una institución donde realizaras la practica.
2. Identifica los recursos valiosos (mínimo 10) según importancia (asignar un peso).
3. Identifica 5 recursos valiosos e identifica de cada uno los:
    a. Riesgos.
    b. Amenazas.
    c. Vulnerabilidades.