

Introducción a SGSSI

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Introducción a SGSSI



DOI

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



¿Qué es la seguridad informática?

Bienes / activos: aquello que se desea proteger (Datos, software, hardware, infraestructura, personal, información, etc.)

Riesgos / amenazas: posibilidad de que algún bien sufra daños o desaparezca (Robo, modificación, suplantación, interceptación, etc.)

¿Qué es la seguridad informática?

Todas las acciones que se toman para asegurar que:

- Los bienes / servicios son usados como se debe
- Los bienes / servicios sólo dan acceso a quien tiene permiso para ello
- Los bienes / servicios cumplen la legislación vigente

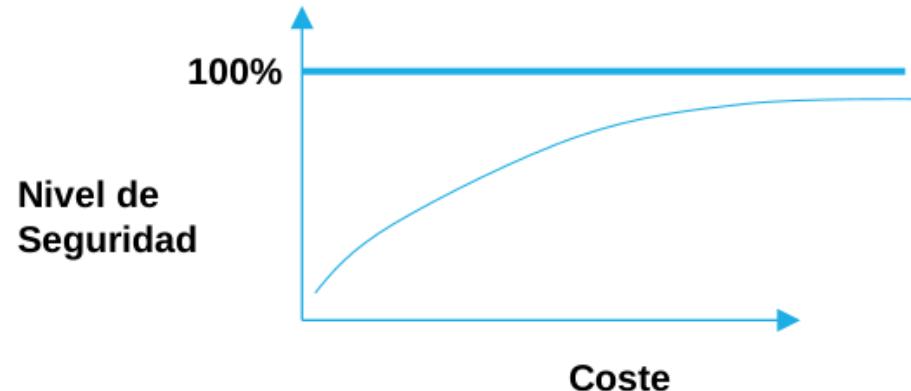
¿Qué es la seguridad informática?

Objetivos:

- Detectar los riesgos y amenazas para evitar que se produzcan o minimizar su efecto
- Garantizar el uso adecuado de los bienes
- Limitar las posibles pérdidas y asegurar la recuperación del sistema lo antes posible
- Cumplir la legislación correspondiente

¿Qué es la seguridad informática?

Es imposible lograr el 100% de seguridad: la seguridad es un proceso, no un estado



¿Quién se encarga?

- Administración de seguridad
- Dirección
- Usuarios

¿Quién se encarga?

Administración de seguridad:

- Responsable de identificar bienes a proteger y riesgos
- Realiza el plan de seguridad y lo implementa

¿Quién se encarga?

Dirección:

- La seguridad debe ser un objetivo estratégico
- Hay que invertir dinero
- Organizar el departamento de seguridad

¿Quién se encarga?

Usuarios:

- Deben recibir formación
- Deben conocer la política de seguridad de la empresa
- Deben involucrarse en la seguridad
- Deben conocer la legislación

Análisis de riesgos

Identificar los bienes a proteger

Estimar el valor (V) de esos bienes

Identificar las amenazas que sufren dichos bienes

Estimar la probabilidad (P) de que esas amenazas realmente se produzcan

Análisis de riesgos

Analizar las medidas necesarias para eliminar esas amenazas

Estimar el coste (C) de implantar esas medidas

$C < P * V$ (Cuando el coste es menor que la probabilidad multiplicada por el valor, aplicar las medidas)

Principios de seguridad

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad
- No repudio

Confidencialidad

Se garantiza que la información transmitida o almacenada en un sistema informático sólo podrá ser leída por su legítimo destinatario

Si dicha información cae en manos de terceras personas no podrán acceder al contenido original

Integridad

Se garantiza que la información no ha sido modificada desde su creación o durante su transmisión

Permite detectar si se ha añadido, modificado o eliminado parte de la información almacenada, procesada o transmitida

Disponibilidad

La información debe estar disponible para sus legítimos usuarios y propietarios

Se garantiza el correcto funcionamiento del sistema informático mediante un diseño suficientemente robusto frente a ataques e interferencias

Autenticidad

Se puede comprobar la identidad del usuario que crea o accede a la información

También se habla de autenticidad de un equipo que se conecta a una red o intenta acceder a un servicio

No repudio

Se demuestra la autoría de la información mediante un mecanismo probatorio que impida al usuario que la ha creado y enviado negar esta circunstancia

Se aplica la misma situación al destinatario de la información

Especialmente importante en transacciones comerciales

Ejemplos

El ciberataque de Wanna Cry que ha afectado a casi todo el mundo

El viernes, 12 de mayo, nos hacíamos eco de una noticia que afectaba a varias empresas españolas, entre ellas, Telefónica. Esta teleoperadora, entre otras compañías, había sufrido un ciberataque en su red corporativa informática. Se trata del "**ransomware**" **Wanna Cry**, un virus informático malicioso tipo "malware". Este virus ha afectado a más empresas, entre ellas, a la compañía aérea Iberia.

<https://www.elrincondelombok.com/internet/el-ciberataque-de-wanna-cry-que-ha-afectado-a-casi-todo-el-mundo/>





Ejemplos

The screenshot shows a news article from the website GENBETA. The title of the article is "Un ciberatacante destruye miles de bases de datos MongoDB y Elasticsearch y deja sólo una firma: 'miau'" (A cyberattacker destroys thousands of MongoDB and Elasticsearch databases and leaves only a signature: 'miau'). Below the title, there is a small image of a cat's face with some code overlaid. At the bottom of the image, there is a snippet of MongoDB shell command output showing IDs like 148273801, 148273802, and 1482738402.

<https://www.genbeta.com/seuridad/ciberatacante-destruye-miles-bases-datos-mongodb-elasticsearch-deja-solo-firma-miau>



Ejemplos

AGOSTO 15, 2020 — JULIO SAN JOSÉ

MAPFRE víctima de un ataque de ransomware.

El ransomware y lo cibercriminales no descansan ni en vacaciones.

Hace escasas horas, la aseguradora admitía en una publicación por Twitter, que el retraso en su atención se debía que estaba siendo víctima de un ataque de ransomware:

Angélica C. @acf77 · 15 ago. 2020
Hay cosas en la vida que no se entienden bien... Dónde está @MAPFRE_Atiende cuando se necesita? Pues parece que no están...

MAPFRE España @MAPFRE_ES
Te pedimos disculpas porque no estamos pudiendo atenderte con la calidad habitual de MAPFRE. Desde hace unas horas estamos actuando sobre nuestros sistemas informáticos para repeler un ataque de ransomware. Estamos trabajando en ello para resolverlo en el menor plazo posible.

5:32 p. m. - 15 ago. 2020

35 56 personas están twitteando sobre esto

<https://derechodelared.com/mapfre-victima-de-un-ataque-de-ransomware/>

Ejemplos

LinkedIn, «hackeada», recomienda a los usuarios a cambiar la contraseña

https://www.abc.es/tecnologia/redes/abci-linkedin-hackeada-recomienda-usuarios-cambiar-contrasena-201605191319_noticia.html

Ejemplos

CIBERDELINCUENCIA • Malware informático

Un empleado deja un virus informático en su antigua empresa para robar sus clientes

<https://www.elmundo.es/madrid/2019/05/22/5ce5280afddff7b688b46a2.html>

Ejemplos

El ordenador de Merkel en el Bundestag sufrió un ciberataque

EFE / BERLÍN | Día 14/06/2015 - 10.22h

- ▶ El equipo de la canciller se utilizó también para enviar correos electrónicos infectados a otros políticos



<https://www.abc.es/internacional/20150614/abci-ordenador-merkel-ciberataque-201506141013.html>

Ejemplos

The screenshot shows a news article from [www.eldiario.es](https://www.eldiario.es/turing/vigilancia_y_privacidad/nsa-programas-vigilancia-desvelados-snowden_1_4974573.html). The article title is "Todos los programas de espionaje de la NSA desvelados por Snowden". It discusses the MYSTIC program, which allows for the recording of 100% of phone calls. Below the main text, there are two additional paragraphs: one about the NSA's cyberespionage activities and another linking to a section on how NSA surveillance programs work.

Todos los programas de espionaje de la NSA desvelados por Snowden

El último de los programas de espionaje masivo desvelado por Edward Snowden es MYSTIC, que permite la grabación del 100% de las llamadas telefónicas de un país

El cibercapacitación de la NSA incluye desde el análisis de metadatos a la recopilación de mensajes de texto (SMS) o la propagación de virus informáticos ("malware")

Cuáles son y cómo funcionan los programas de espionaje de la NSA

https://www.eldiario.es/turing/vigilancia_y_privacidad/nsa-programas-vigilancia-desvelados-snowden_1_4974573.html

Ejemplos

"Quien renuncia a su libertad por seguridad, no merece ni libertad ni seguridad" B. Franklin

Vigilancia permanente. Edward Snowden. Grupo Planeta, 2019

Ejemplos

La web para infieles 'hackeada' disponía de 39.000 perfiles de ciudadanos vascos

Bilbao, con 10.523 inscritos en Ashley Madison, lidera la lista de contactos vascos, seguida por Durango y San Sebastián. Vitoria sólo cuenta con 311 afiliados



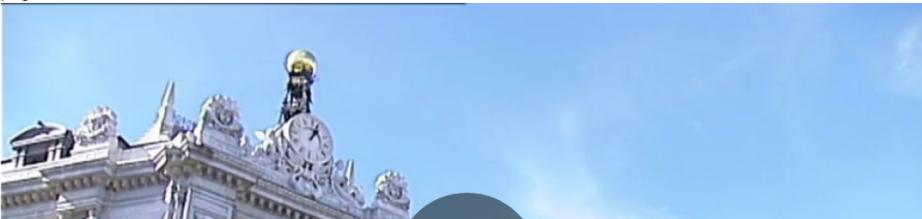
<https://www.elcorreo.com/bizkaia/tecnologia/internet/201508/23/para-infieles-hackeada-disponia-20150821190325.html>

Ejemplos

NOTICIAS > ECONOMÍA LOS TRABAJADORES NO TIENEN PROBLEMAS

Un hackeo de la web del Banco de España la deja prácticamente inoperativa

Aunque desde la institución defienden que no existe riesgo de filtración de datos, el funcionamiento normal de la página web todavía no ha vuelto.



https://www.antena3.com/noticias/economia/hackeo-web-banco-espana-deja-practicamente-inoperativa_201808275b8427f90cf26ed5cf1aaf4e.html

Ejemplos

The screenshot shows a news article from La Sexta. At the top, there are navigation links for 'NOTICIAS' and 'ESPAÑA', and a category 'DURANTE EL DEBATE DE INVESTIDURA'. On the right, there are social media sharing icons for a magnifying glass, Twitter, and Facebook. The main title of the article is 'Anonymous hackea la página web del Congreso de los Diputados para "rodearlo a nuestra manera"'. Below the title, a subtext reads: 'Un grupo de activistas aprovecha el debate de investidura de Mariano Rajoy para utilizar la página web del Congreso de los Diputados para "rodearlo", mientras miles de personas asisten a la convocatoria de 'Rodea el Congreso''. The article content includes a URL 'www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?inj=' followed by several lines of Java error code, indicating a successful exploit.

lada. java.lang.NumberFormatException: For input string:

las que la impericia del programador ([modo pitorreo sans on] amiguetes, las excepciones en JavaScript hay que saber gestionarlas cuando se curra para tan elevada cantidad [modo pitorreo sans off]) nos permite interesantes (por llamarlos de alguna forma). Este es uno de esos casos, y aunque queda feo escribir sus acentos y obviando algunos caracteres para mejorar la visibilidad del texto, la vamos a utilizar para "ro

https://www.lasexta.com/noticias/nacional/hackean-la-pagina-web-del-congreso-de-los-diputados-para-rodearlo_201610295814e4680cf24962cc0c6aba.html

Ejemplos

Home Videos Twitter Archive Mobile RSS Search

**CUESTIÓNALO
TODO**

La Nueve

We are Anonymous,
We are Legion,
We are One.
Expect Us...
Inglourious
/b/asterds...

Text Agosto 02, 2020 6 notas

Half-track en AVALMADRID

Tras tanta demora y vista la expectación, vamos a desvelarlos dónde estaba uno de nuestros half-tracks: en AVALMADRID 🤪

¿Y qué hacíamos allí tanto tiempo? Pues ver documentos y documentos de préstamos, de embargos... A los periodistas les encataría 😊 El caso es que a nosotras más que encantarnos, nos divierte.

Y es que, por ejemplo, ahora sabemos que Elena González-Moñux Vázquez, ex concejala del Ayuntamiento de Madrid y diputada en la Asamblea de Madrid por el Partido Popular, tenía su sueldo y sus cuentas corrientes bajo amenaza de embargo en 2019. ¿Qué habrá pasado?

AL JUZGADO 1 INSTANCIA 10 DE MADRID

Ejecución Título No Judicial: [REDACTED]
Parte demandante: AVALMADRID. S.G.R.
Parte demandada: ELENA GONZALEZ MONUX, RICARDO JOSE FERNANDEZ GIL, PLANBEN S.A.

Ejemplos

The screenshot shows the homepage of The Register. At the top, the site's logo 'The Register' is displayed with the tagline 'Biting the hand that feeds IT'. Below the logo is a navigation bar with categories: DATA CENTRE, SOFTWARE, SECURITY, DEVOPS, BUSINESS, PERSONAL TECH, SCIENCE, EMERGENT TECH, BOOTNOTES, VENDOR VOICE, and a user icon. A search bar is also present. A banner at the top features the Dynatrace logo and a badge stating 'Leader Gartner 2020'. The main headline reads: 'Intel NDA blueprints – 20GB of source code, schematics, specs, docs – spill onto web from partners-only vault'. A subtext below the headline says: 'Leaker only 'a bit concerned' about getting sued'. The URL of the article is provided at the bottom of the screenshot.

https://www.theregister.com/2020/08/06/intel_ndu_source_code_leak/

Ejemplos

JUSTICIA CIERRA TEMPORALMENTE EL PORTAL

Un fallo en el sistema telemático de Justicia permitió acceder a todos los casos abiertos

Un fallo de permisos en el sistema telemático del Ministerio de Justicia ha dado acceso durante horas a abogados y procuradores a los casos judiciales del resto de profesionales en el sistema



https://www.elconfidencial.com/tecnologia/2017-07-27/lexnet-justicia-sistema-telematico_1421771/

Ejemplos

Una ciudad de Florida pagará más de 600.000 \$ por un rescate de ransomware

<https://news.sophos.com/es-es/2019/06/24/una-ciudad-de-florida-pagara-mas-de-600-000-por-un-rescate-de-ransomware/>

Ejemplos

TELEFONÍA MÓVIL >

El timo de la SIM duplicada: si su teléfono hace cosas raras, revise la cuenta bancaria

El fraude conocido como 'sim swapping', muchas veces precedido por el robo de otros datos, ha ganado relevancia en los últimos años, según la Guardia Civil y los expertos

https://elpais.com/economia/2019/05/21/actualidad/1558455806_935422.html

Ejemplos

SEGURIDAD

Criminales utilizan deepfakes de audio para hacerse pasar por CEOs y robar a empresas

By Jorge Quijije - Jul 22, 2019

<https://www.tekcrispy.com/2019/07/22/deepfakes-audio-empresas/>

Ejemplos

NAVARRA

Salud debe pagar 125.000 euros por un acceso "ilegítimo" a un historial clínico

DILES PAMPLONIA A A*

Los datos fueron consultados 2.825 veces por 417 usuarios integrados en 55 servicios y procedentes de todos los centros sanitarios, cuando la paciente "sólo estuvo en un hospital y en cuatro servicios"

Actualizada 22/02/2012 a las 18:26

Comentarios 14

Anuncios Google Salud Médico Médico Salud Médica Salud La Salud

Twitter 34

Me gusta 38

Tuenti

G+ 2

La Sala de lo Contencioso-Administrativo del **Tribunal Superior de Justicia de Navarra** (TSJN) ha confirmado una condena de 125.000 euros al **Servicio Navarro de Salud** por el acceso "ilegítimo" y masivo, por parte del personal sanitario, al historial clínico de una paciente fallecida.

La sentencia, que es firme y obliga a retirar las **fotografías de la historia clínica**, establece que se ha producido un funcionamiento "anormal" en el sistema sanitario público navarro "en la medida en que ha

https://www.diariodenavarra.es/noticias/navarra/mas_navarra/salud_debe_pagar_125_000_euros_por_acceso_illegitimo_historial_una_paciente_70815_2061.html

Ejemplos

El punto débil de los Tesla: una empresa de ciberseguridad consigue abrir y arrancar un Model 3 atacando el móvil del dueño

Miguel Ángel Moreno 17 may. 2022 12:05h.



Coches eléctricos Tesla Model 3 cargándose en China. REUTERS/Aly Song/File Photo

<https://www.businessinsider.es/consiguen-abrir-arrancar-tesla-model-3-traves-movil-dueno-1062031>

Ejemplos

Log4Shell es la vulnerabilidad crítica 'de proporciones catastróficas' que amenaza con destrozar internet



<https://www.xataka.com/seuridad/log4shell-vulnerabilidad-critica-proporciones-catastroficas-que-amenaza-destrozar-internet>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228>

Ejemplos

Doki, el nuevo malware de Linux fija como objetivo las APIs de contenedores docker mal configurados

29 julio, 2020 Por Daniel Piña — Deja un comentario

Descubierto un **malware de Linux indetectable** que explota técnicas indocumentadas para permanecer bajo el radar y apunta a servidores Docker de acceso público alojados en plataformas de cloud populares, incluidas AWS, Azure y Alibaba Cloud.



<https://unaaldia.hispasec.com/2020/07/doki-el-nuevo-malware-de-linux-fija-como-objetivo-las-apis-de-contenedores-docker-mal-configurados.html>

Ejemplos

El ransomware llega a las máquinas de café:
hackean una cafetera para soltar agua hirviendo y
pedir un rescate

NOTICIA



<https://computerhoy.com/noticias/tecnologia/ransomware-maquinas-cafe-cafetera-726041>