Introducción a SGSSI

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Introducción a SGSSI

DOI 10.5281/zenodo.5483661

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

Indice

- Definiciones
- ¿Qué es la seguridad informática?
- Consecuencias (Ejemplos reales)
- Principios de seguridad (CIDAN)
- ¿Quién se encarga?
- Análisis de riesgos

Definiciones

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

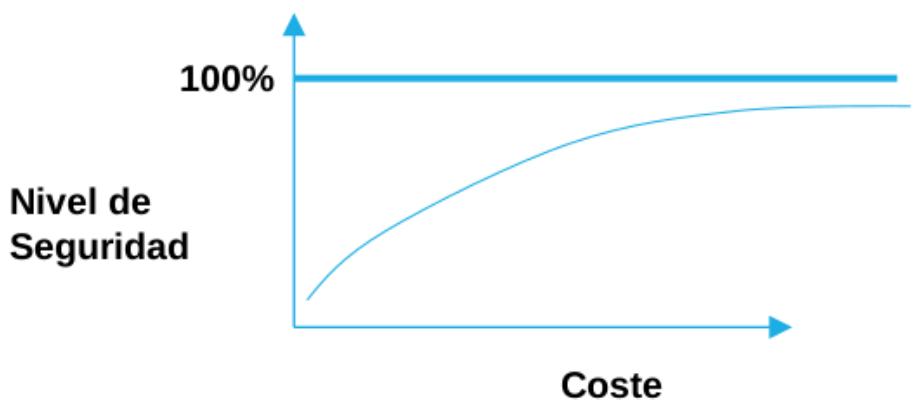
¿Qué es la seguridad informática?

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



Consecuencias

- Robos y estafas
- Espionaje y robo de información confidencial
- Sabotaje
- Pérdida de propiedad intelectual
- Pérdida de información confidencial
- Pérdida monetarias
- Pérdidas de derechos
- Riesgo para la vida

Robos y estafas

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/

Robos y estafas

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

AMATECH GROUP
EUROHELP
CONSULTING

Robos y estafas

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/

Robos y estafas

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

Robos y estafas

CIBERDELINCUENCIA • Malware infórmatico

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

https://www.elmundo.es/madrid/2019/05/22/5ce5280afdddff7b688b46a2.html

Robos y estafas

TECNOLOGÍA

Instagram confirma el robo de datos de sus usuarios más populares

TWITTEAR COMPARTIR Por Mónica Redondo 31/08/17 - 02:05

La red social fue víctima de un fallo en la programación de la interfaz, lo que provocó el robo de números de teléfono y correos electrónicos de celebridades.

https://www.elmundo.es/madrid/2019/05/22/5ce5280afdddff7b688b46a2.html

Espionaje, robo de información confidencial

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

Espionaje, robo de información confidencial

Estados Unidos acusa a China de liderar un ciberataque

- El jefe de espionaje James Clapper es el oficial de más alto rango en apuntar a Pekín por haber robado datos personales de más de cuatro millones de usuarios

https://www.elperiodico.com/es/internacional/20150626/estados-unidos-acusa-a-china-de-liderar-un-ciberataque-4306566

Espionaje, robo de información confidencial

Obama ordenó un ataque cibernético contra Irán del que perdió el control

- El programa, bautizado como operación Juegos Olímpicos, fue ideado por Bush
- En verano de 2010 se convirtió en un virus que infectó decenas de miles de ordenadores

DAVID ALANDETE | Washington | 1 JUN 2012 - 20:03 CET 236

https://elpais.com/internacional/2012/06/01/actualidad/1338572841_317814.html

Espionaje, robo de información confidencial

elDiario.es

Hazte socio/a Inicia sesión

Coronavirus Mascarillas Vuelta al cole Memoria histórica José Luis Martínez-Almeida Juan Carlos I + Temas

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 ciberespionaje 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

Espionaje, robo de información confidencial

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

Vigilancia permanente. Edward snowden. Grupo Planeta, 2019.

Espionaje, robo de información confidencial

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

Sabotaje

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

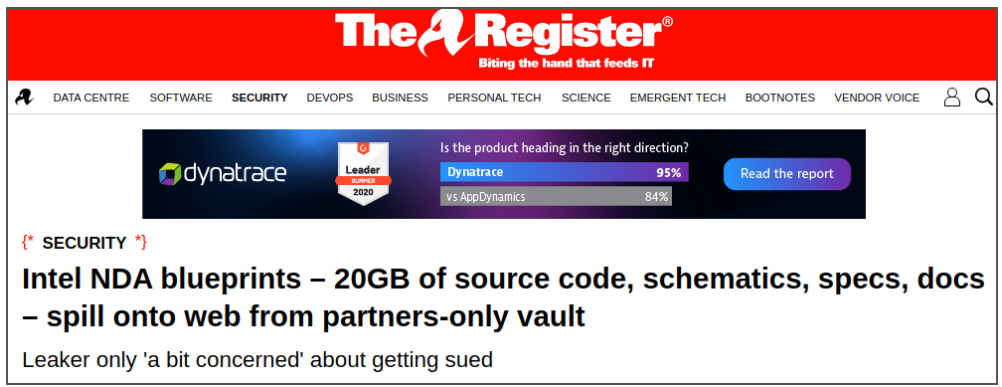
"Sabotaje"

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

"Sabotaje"

https://la9deanon.tumblr.com/post/625357883903754240/half-track-en-avalmadrid

Pérdida propiedad intelectual



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

Pérdida información confidencial

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/

Pérdidas monetarias

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/

Pérdidas monetarias

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

Pérdidas monetarias

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/

Pérdidas de derechos

NAVARRA

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

DIARIO DE NAVARRA

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

Twittear 34

Me gusta 38

Tuenti

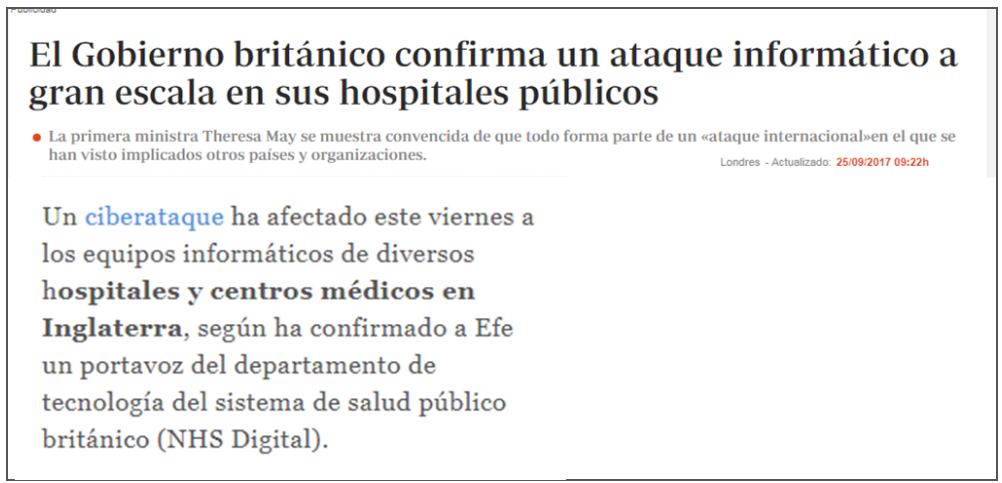
+1 2

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_ilegitimo_historial_una_paciente_70815_2061.html

Riesgo para la vida



El Gobierno británico confirma un ataque informático a gran escala en sus hospitales públicos

- La primera ministra Theresa May se muestra convencida de que todo forma parte de un «ataque internacional»en el que se han visto implicados otros países y organizaciones.

Londres - Actualizado: 25/09/2017 09:22h

Un ciberataque ha afectado este viernes a los equipos informáticos de diversos **hospitales y centros médicos en Inglaterra**, según ha confirmado a Efe un portavoz del departamento de tecnología del sistema de salud público británico (NHS Digital).

https://www.abc.es/tecnologia/redes/abci-gobierno-britanico-confirma-ataque-informatico-gran-escala-hospitales-publicos-201705121640_noticia.html

Riesgo para la vida

EL PAÍS INTERNACIONAL

EUROPA EE UU MÉXICO AMÉRICA LATINA ORIENTE PRÓXIMO ASIA ÁFRICA FOTOS OPINIÓN ÚLTIMAS NOTICIAS

Te quedan 9 artículos gratis este mes SUSCRÍBETE

IRLANDA >

Un ciberataque obliga a Irlanda a cerrar el sistema informático de la sanidad pública

El bloqueo obliga a cancelar la mayoría de las citas, pero no afecta al plan de vacunación, según el Gobierno

https://elpais.com/internacional/2021-05-14/un-ataque-cibernetico-en-irlanda-obliga-a-cerrar-el-sistema-informatico-de-la-sanidad-publica.html

Principios de seguridad

- **C**onfidencialidad
- **I**ntegridad
- **D**isponibilidad
- **A**utenticidad
- **N**o 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

Otros principios

- Autorización
- Auditabilidad
- Reclamación de origen
- Reclamación de propiedad
- Anonimato en el uso
- Protección a la réplica
- Confirmación
- Referencia temporal

Autorización

Control de acceso a equipos y servicios

Permite controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema informático, una vez superado el acceso de autenticación de cada usuario

Auditabilidad

Permite monitorizar el uso de los distintos recursos del sistema por parte de los usuarios previamente autenticados y autorizados

Reclamación de origen

Permite probar quién ha sido el creador de determinada información

Reclamación de propiedad

Permite probar que un determinado documento o un contenido digital protegido por derechos de autor pertenece a un determinado usuario u organización que ostenta la titularidad de esos derechos

Anonimato en el uso de servicios

Garantiza el anonimato de los usuarios que acceden a los recursos y consumen determinados tipos de servicios, preservando así su privacidad

Puede entrar en conflicto con otros ya mencionados, como la autenticación o la auditoría del acceso a los recursos

Protección a la replica

Impide la realización de "ataques de repetición" (replay attacks) por parte de usuarios maliciosos, consistentes en la interceptación y posterior reenvío de mensajes para tratar de engañar al sistema y provocar operaciones no deseadas, como realizar varias veces una transacción bancaria

Confirmación de prestación de un servicio

Permite confirmar la realización de una operación o transacción, reflejando los usuarios o entidades que han intervenido en ésta

Referencia temporal

Certificación de fechas

Se demuestra el instante concreto en que se ha enviado un mensaje o se ha realizado una determinada operación, generalmente con una referencia UTC (Universal Time Clock)

Certificación mediante terceros de confianza

Para realizar transacciones electrónicas se requiere garantizar la autenticación de las partes que intervienen, el contenido e integridad de los mensajes o la constatación de la realización de la operación o comunicación en un determinado instante personal

Certificación mediante terceros de confianza

El "tercero de confianza" es un organismo que se encarga de certificar la realización y el contenido de las operaciones y de avalar la identidad de los intervinientes, dotando a éstas de una mayor seguridad jurídica

Ejemplo: Autoridades de Certificación de la firma electrónica como Izenpe

¿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)