Incidentes de seguridad

&

CSIRT

Seguridad de la información

El objetivo es garantizar los siguiente atributos de la información

- Confidencialidad: Garantiza que la información sólo sea accesible por las personas autorizadas.

- Integridad: Garantiza que la información sólo pueda ser modificada por quien está autorizado a hacerlo

- Disponibilidad: Garantiza que los usuarios autorizados tienen acceso a la información y recursos relacionados cuando lo necesiten.

Vulnerabilidad

Una ***vulnerabilidad*** es una debilidad que pone en riesgo la seguridad de la información pudiendo permitir a un atacante comprometer la integridad, disponibilidad o confidencialidad de la misma.

La ***vulnerabilidad*** puede estar en cualquiera de los siguientes:

- El sistema de información
- Las comunicaciones
- Los sistemas que almacena la información
- Las personas que intervienen

Es deseable necesario encontrar las vulnerabilidades y eliminarlas lo antes posible.

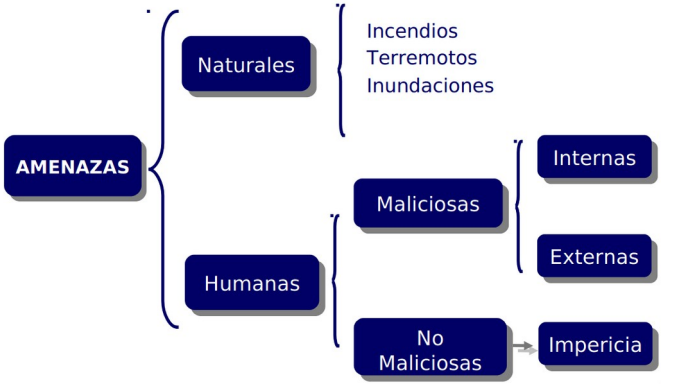
Amenazas

Una ***amenaza*** es toda acción que aprovecha una ***vulnerabilidad*** para atentar contra la seguridad de un sistema de información.

Las ***amenazas*** pueden concretarse a partir de:

- ataques informáticos: ingenieria social, bruteforce, vuln-exploit, etc.
- sucesos físicos: incendios, inundaciones, terremotos.

Desde el punto de vista de una organización, las ***amenazas*** pueden proceder tanto de personal interno como externo.



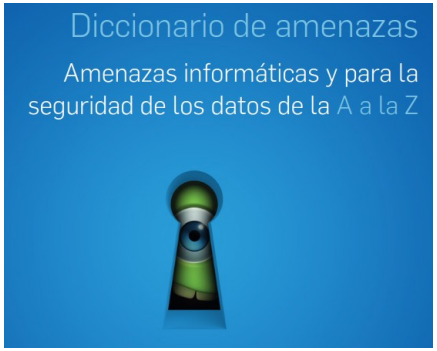
Incidente de seguridad

Un ***incidente de seguridad***, es un evento adverso que afecta los activos de la organización.

Un ***incidente de seguridad*** se produce cuando se concreta una ***amenaza***.

Algunos ejemplos de incidentes de seguridad que pueden afectar a una organización:

- Defacement
- Ransomware
- Robo de contrase
- Fuga de información confidencial
- Compromiso de un hosts, servidor o servicios
- Acceso no autorizado
- etc



CERT / CSIRT

Un CERT o CSIRT, es el equipo dentro de una organización que se encarga de la gestión de incidentes de seguridad

Los incidentes de seguridad de interés son los que afectan a los usuarios y servicios de la organización, así como también los que afectan a terceros pero tienen su origen en la organización.

La gestión de incidentes de seguridad implica:

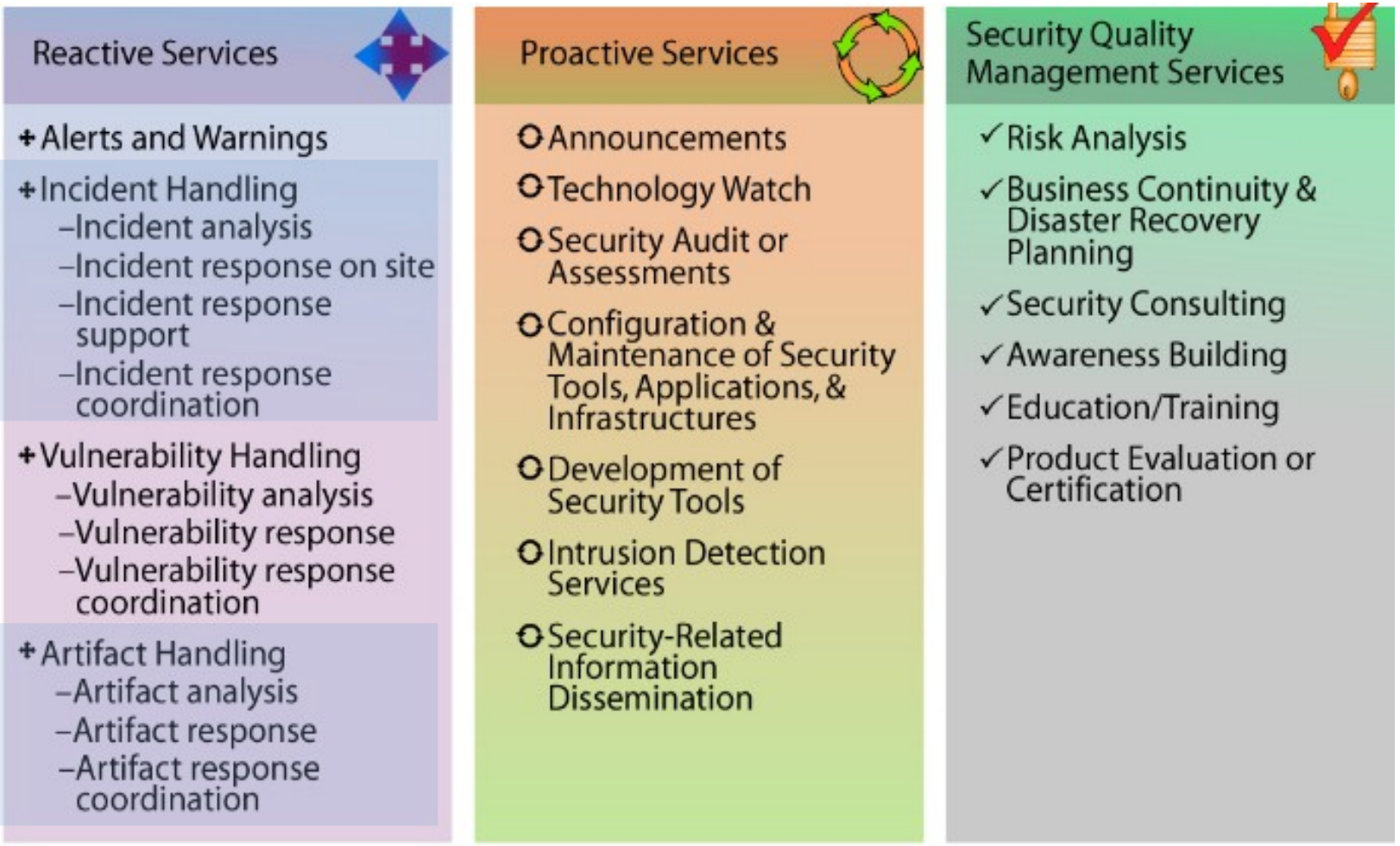
- Disponer de canales para la recepción de incidentes de seguridad
- Analizar los incidentes de seguridad. Investigar aspectos relacionados
- Coordinar acciones para mitigar el incidente
- Brindar recomendaciones para que no vuelva a ocurrir

Otras siglas usadas por CERTs o CSIRTs

No importa si se llama CERT o CSIRT. Lo importante es que gestionan incidentes de seguridad.

- CSIRT Computer Security Incident Response Team
- CSIRC Computer Security Incident Response Capability
- CIRC Computer Incident Response Capability
- CIRT Computer Incident Response Team
- IHT Incident Handling Team
- IRC Incident Response Center or Incident Response Capability
- IRT Incident Response Team
- SERT Security Emergency Response Team
- SIRT Security Incident Response Team

Servicios que un CSIRT puede dar



Handbook for Computer Security Incident Response Teams (CSIRTs): https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Buenas Prácticas

Los miembros de un CSIRT deben manejar con cuidado la información relacionada a los incidentes de seguridad gestionados. Para ello:

- Se mantiene la confidencialidad de la información de modo que solamente el afectado tenga acceso.
- En caso de ser necesario intercambiar información sensible con otros CSIRTs, se utiliza un protocolo conocido como TLP para que el destinatario sepa con quien puede compartir la información.
- Se utiliza criptografía (PGP) para realizar el intercambio de información sensible de forma segura.

Traffic Light Protocol (TLP)

Traffic Light Protocol (TLP) es un esquema creado para fomentar un mejor intercambio de información sensible (pero no clasificada) en el ámbito de la seguridad de la información.

A través de este esquema, de una forma ágil y sencilla, el autor de una información puede indicar hasta dónde puede circular la información más allá del receptor inmediato, y este debe consultar al autor original cuando la información necesite ser distribuida a terceros.

Código	Cuándo utilizarlo	Cómo compartirlo
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.
TLP:AMBER	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.
TLP:WHITE	Se debe utilizar TLP:WHITE cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:WHITE puede ser distribuida sin restricciones, sujeta a controles de Copyright.

Coordinación / TLP
Caso: WannaCry

Ciberataque global [editar]

El 12 de mayo de 2017 entre las 8 y las 17:08 horas UTC[3] se registró un ataque a escala mundial que afectó a las empresas Telefónica[4] [5], Iberdrola y Gas Natural, entre otras compañías en España,[6] así como al servicio de salud británico, como confirmó el Centro Nacional de Inteligencia.[7] [8] [9] [10] [11] La prensa digital informaba aquel día que al menos 141 000 computadores habían sido atacados en todo el mundo.[12] [13] [14]

Subject **[Lac-csirts] WannaCry whitepaper** 15/5/17 10:15

To LAC-CSIRTs lista <lac-csirts >

Segue um whitepaper sobre o WannaCry, produzido pelo ThaiCERT.

Arquivo em anexo.

1 attachment: WannaCry_Ransomware_v1.0.pdf 1,0 MB Save

WannaCry Ransomware

Compiled by ThaiCERT, a member of the Electronic Transactions Development Agency

Version 1.0 (15 May 2017)

TLP:WHITE

PGP

En la operación de un CSIRT, distintas situaciones pueden requerir el intercambio de información de manera segura:

- Compartir datos sensibles entre miembros del equipo
- Entregar informes de pentests realizados.
- Entregar informes de forensias realizadas.

Para ello, es necesario disponer de formas seguras para el intercambio de información. Las posibilidades son:

- Reunión presencial
- Uso de criptografía en las comunicaciones (PGP)